International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

An Efficient Secure and Flexible Data Sharing in Cloud Computing using Asymmetric Algorithm

A. Manimaran , K. Somasundaram

Abstract: ***Cloud Security is a technique of safeguarding applications, infrastructures and data involved in cloud computing. Cloud security uses a set of technologies, policies and controls to protect data and application from unauthorized access. RSA encryption and decryption algorithm is presented here for cloud security. The cloud can access the data only after receiving the user's encrypted message using RSA algorithm. However, while transmitting the encrypted message more bandwidth is consumed as the message is transmitted over wireless channel. To minimize the bandwidth, the encrypted message is transmitted into a number of encoded bits and the cloud service provider can append the bits and recover the original message. The performance results for RSA algorithm and the RSA algorithm using Fountain Code are simulated. The results show that the energy, end-to-delay are minimized while using Fountain Code RSA algorithm. In addition, the packet loss ratio decrease and the packet delivery ratio increase.***

Index Terms: Cloud computing, Fountain code RSA Algorithm, Wireless, Encryption, decryption, end-to- delay.

I. INTRODUCTION

Cloud security safeguards online data from unknown persons stealing the data. Techniques of yielding cloud security are obfuscation, penetration testing, firewalls, virtual private network (VPN) and tokenization.Cloud security provides multiple controls within the infrastructure of the network to yield general services such as web-based applications and web-based storage. A private cloud is used for a specific purpose by a single organization or business. The private cloud can be governed by a third-party service provider or a business, or a combination of a business and a third party service. Any application can be executed in a private cloud environment including big data, machine learning applications, databases and websites. Both public and private cloud environment being together acts as a separate environment and called as hybrid cloud. In a hybrid cloud environment, applications and data move between public and private cloud environments yielding enhanced flexibility.

Cloud security faces critical threats such as data violations, data loss, service traffic loss, account hijacking, application program interfaces (APIs) with no security, poor selection of providers for cloud storage, and distributed technology compromising the cloud security.

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author
A. Manimaran*, Research Scholar, Dept. of Computer Science and Engineering, St.Peter's Institute of Higher Education and Research, St. Peter University, Avadi, Chennai, India.
K. Somasundaram, Professor, Dept. of Computer Science and Engineering, Chennai Institute of Technology, Chennai, India.

Also Cloud Security is prone to Distributed denial of service (DDoS) attacks. These attacks block a service through eliminating the service with data. Therefore, users cannot access the bank or email accounts. The cloud security enables the user to store the data on the cloud for safety purpose. Several users believe that their data is secure on their cloud. Once the data is stored in the cloud, it is secured by cloud sevice providers that have effective security measures. On-premise data's face security threats and vary on the type of attack. Data storage systems are exposed to possibility of attacks by malicious applications and malware and on-site data by security threats.

The cloud security is essential for cloud storage providers. The cloud storage providers not only fulfill their customer's requirements; but should also follow some regulatory needs to store sensitive data like health information and credit card numbers. User's data is kept safe by auditing cloud provider's security systems and procedures. Safeguarding the data in cloud is equal to protecting cloud itself. Cloud accessing from stored data on mobile devices or careless login credentials must be avoided. Data saved on another country's cloud can differ in privacy measures and regulations.

By selecting a cloud provider, it is essential to select a firm which safeguard against malicious threat using security clearances and background checks. Majority of the people think that hackers are the main threat to cloud security in-spite employees being the important threat. These employees being malicious insiders, also access sensitive company data unknowingly like using a personal, without the security of the company's own network. Cloud security offers many benefits such as centralized security, reduced cost and administration, cloud DDoS protection, eliability and high availability. Here for encrypting and decrypting the data in the cloud, RSA encryption and decryption is presented. But when a cloud user transmits an encrypted message to the cloud service provider, more bandwidth is consumed as the message is transmitted over the wireless channel. To overcome this problem, the Fountain Code RSA algorithm is introduced. In Fountain Code RSA algorithm, the message is transmitted into an unlimited number of encoded bits, so the cloud service provider can append the encoded bits and recover the transmitted message.

II. LITERATURE SURVEY

The most popular systems to protect the data from unauthorized user is cloud storage. The cloud storage encryption is safe & cannot be hacked. However, some authorities may guide cloud storage providers to show confidential data or user secrets in the cloud.

The design is created for novel cloud storage encryption system, which permit cloud storage providers from persuading false user secrets to prevent user reclusiveness [1].

The cloud database model is the new system, which can assist various Internet-based applications. However, the cloud database system needs the solution of data secrecy problems. Adaptive encryption architecture behaves an alternative to the trade-off between the required information confidentiality level & data base structure flexibility at design time, for cloud databases. The performance and feasibility of an adaption encryption structure is shown by a software prototype in [2].

The performed a method of multi-authority proxy re-encryption based on cipher text-policy attribute-based encryption (MPRE-CPABE) used for cloud storage schemes. The method needs data owner to distribute every file into two blocks that is one small block and one big block. To the large one is encrypt that utilized the little block. The private key is the name of big one. Then, uploaded the encrypted large block to the cloud storage method although the moved uploaded large block of file. Therefore, in the file, unauthorized users' not obtain the full data in an easy manner. [3]

The presented a system of encrypted data sharing for safe cloud storage system, which depends on the conditional proxy broadcast re-encryption technology. The encrypted data sharing system simply not attain transmit data sharing system through taking merits of transmit encryption, also attain dynamic sharing system which enables combining a user to and from the sharing sets, that a user is extracting. However, by utilizing proxy re-encryption technology, the encrypted data sharing system allows proxy to share directly encrypted data to aim users. However, the data owner involvement is not required when keeping data privacy. Therefore, the sharing performance is enhanced. [4]

In encrypted cloud data for ranked explores, the effective device of Order preserving Encryption (OPE) to the relevancy scores encrypt of reversed index. Once utilizing deterministic Order Preserving Encryption (OPE), the cipher texts will show the relevance scores distribution. So that, the probabilistic OPE is presented that named as One-to-Many OPE. For searchable encryption applications, the probabilistic encryption can flatten the plaintexts distribution. Several attack in One-to-Many OPE is performed by working the ordered cipher texts differences. [5]

The technology of Attribute based Encryption (ABE) is utilised to implement fine-grained access operate method that gives one better approach to overcome the security problems. In ABE system, the cipher text size and computation cost grow with the access policy. Outsourced ABE (OABE) and fine-grained access control scheme can minimize the calculation cost. Cost Minimization enables users to encrypt the data are stored in cloud through outsourcing weighty calculation to cloud service provider (CSP). Nevertheless, in the cloud, that more encrypted files are kept. So that cloud is too high, the cloud contains will effective query process. To overcome this issue, the named of cryptographic primitive is attribute based encryption method by outsourcing key-issuing & outsourcing decryption to establish keyword search function (KSF-OABE). [6]

Graph encryption approach is analyzed for an essential query type, which named as top-k Nearest Keyword (kNk) searches. Many indexes are designed to the required data is store for answer queries and assurance that private data concerning the graph. For e.g., keywords, vertex identifiers and edges are excluded/encrypted. Their graph encryption system, that verified efficient and security through experiment on the real life datasets and theoretical proofs respectively. [7]

Public key encryption by equality test (PKR-ET) enable to carry out equivalence test among encrypted the two message based on separate public keys. For the encryption public k, an attribute-hiding predicate encryption is a model, which supports both fine-grained access control and attribute-hiding approach. Initially establish the attribute-hiding predicate encryption model and equality test (AH-PE-ET) through adding the concept of PE and PKE-ET. Then concrete AH-PE-ET system is performed. [8]

Identity-based encryption (IBE) is an attractive cryptographic primitive because of its unnecessary certificate managements. However, in Identity-based encryption (IBE) the user cancelling is one of the major problems. To attain revocation, one possible approach is used to update user's decryption keys. Nevertheless, to prevent the requirement of confidential channels, public keys time are required to permit this update to occur. Identity based encryption approach frequently affects from two issues. 1) The user's preserve the linearly developing decryption keys. 2) Still, previous cipher texts can access by the revoked user to revocation. [9]

In cloud storage, the primary issue is privacy concerns and data security. In multi-user setting, based on the homomorphic encryption, that performed the key word search and provable public key encryption. The suggested technique allows the server in DGHV Homomorphic encryption to provide an reversed encryption index structure with no involving query trapdoor to efficiency improve the search. [10]

In cloud computing, the cipher text policy attribute based encryption (CPABE) analyzes the challenges faced in safe data sharing and developed encryption algorithm for it. Normally, the shared data files must have multilevel hierarchy characteristic, especially in military area. However, the shared files hierarchy structure is explored in CP-ABE. In cloud computing, that utilized an efficient method of file hierarchy attribute-based encryption. The layer access structure is incorporated into individual access structure and by incorporated access structure, that encrypted the hierarchy file. [11]

Cloud computing gives a convenient and flexible way of sharing the data that brings several benefits for both individuals and society. Identity-based encryption is a crypto graphics to produce a data sharing method. Still, not static the data access control. Revocable-storage identity-based encryption (RS-IBE) gives the forward or backward security of cipher text by initializing the user revocation functionalities and to update cipher text simultaneously.

[12] Nowadays, a set of enlarged Proxy Re-Encryptions (PRE) such as Conditional Proxy Re-Encryptions (CPRE), Broadcast PRE (BPRE) and identity based PRE (IPRE) is presented used for bendable applications. By adding BPRE, IPRE, and CPRE, versatile primitive is performed concerned by Conditional identity-based broadcast PRE (CIBPRE) and validates its semantic security. The CIBPRE permits a sender to encrypt a message to many receivers by specifying these identities. Then the receivers and senders assign a Re-encryption key to proxy. [13]

By the data owners, that accept attribute-based encryption to secret data storage and for achieve access control. Constrained computing power with users is used to delegate the decryption task mask to the cloud server and to calculating cost reduce. [14]

By searchable symmetric encryption (SSE), that analyzed the issues of data privacy. From the features of scheme robustness, that showed data privacy issues and similarity application. The data privacy leaks automatically and the server-side ranking is discovered depending on the order-preserving encryption (OPE). For leakage is remove, that done two-round searchable encryption (TRSE) method which top-k multi-keyword retrieval is permit . In two-round searchable encryption (TRSE), that utilized the method of vector space and homomorphism encryption. [15]

III. METHODOLOGY

A cryptosystem, the basic algorithm is RSA algorithm. These cryptographic algorithms provide security services or application specific public key encryption and is utilized broadly to safeguard sensitive data, especially once it is transmitted entire an insecure network. Another name of public key cryptography is asymmetric cryptography and utilises two unlike mathematically connected keys such as private key and public key. In a network, that private key is secretly maintained but in public key is maintained the distributed to all. The message is encrypted by both of the keys are private and public keys; the same way in RSA cryptography the opposite key from the one of the private and public keys utilized to message is encrypt is employed to decrypt a message. RSA assures integrity, authenticity, confidentiality and non-repudiation of data storage and electronic communication.

The private and public key creation algorithm is difficult of RSA cryptography. Two big prime numbers, p and q, are generated by the Rabin-Miller primality test algorithm. A modulus, n is computed through the product of p and q. This number is utilized through the private and the public keys and gives the relation among them. The modulus's length expressed in bits is named as key length. The public key includes a public exponent e set as 65537 and the modulus n. The public exponent e is a prime number that not should be very big. The public exponent e is not to be necessarily a selected prime number, as the public key is distributed to everyone. The private key includes the private exponent d and the modulus n. The private exponent d is computed utilizing the Extended Euclidean algorithm to identify the multiplicative inverse with respect to the totient of n. Figure. 1 shows the flow chart of the RSA algorithm. In cloud environment, the public key is shared to all and the private key is kept secret to user who transmits the data.

To access the data from the cloud, that the cloud user send request to the cloud service provider. The cloud service provider generates RSA keys with choosing two prime numbers p and q. The modulus is n=p*q. The totient is n $\phi(n)=(p-1)*(q-1)$. The cloud service provider chooses a prime number for its RSA public key e and computes its RSA private key utilising the Extended Euclidean algorithm. The cloud user needs to send an encrypted message P to cloud service provider, thus the cloud user obtains the cloud service provider's RSA public key (n, e). The encrypted plaintext message into ciphertext, C, of user's cloud are as follows:

$$C=P^{e} \bmod n$$

In RSA algorithm, the cipher text may be a sequence of numbers or a sequence of text. Transmitting this cipher text consumes more bandwidth as the cipher text is transmitted over wireless channel. So the cipher text is transformed into a number of encoded bits using fountain codes and then transmitted.

Proposed technique, Fountain code is a technique that transforms encoded data into an unlimited number of encoded bits such that the original data can be recovered from any subset of encoded bits of data of size equal or larger than the source data. The Encoded bits of cipher text are*C1, C2, C3.*

When the cloud service provider receives the encoded bits of cipher text, the cloud service provider appends the encoded bits of cipher text, decrypts and recovers plain text using its RSA private key are as follows

$$P=C^{d} \bmod n$$

Where$d=e^{-1} \bmod \phi(n)$ and $\phi(n) = (p-1)*(q-1)$ and $n=pq$

After recovering the plain text, the cloud service provider sends data to cloud user by encrypting the data by it is a private key. The user of cloud decrypts the data sent by the cloud service provider. The flow diagram of the fountain code RSA algorithm is shown in figure1.

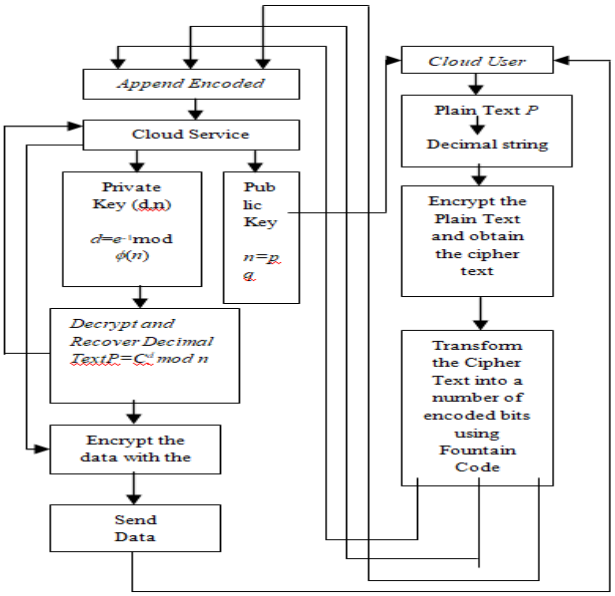

Figure.1 Flow Diagram of Fountain Code RSA Algorithm

IV.RESULTS AND DISCUSSION

The Fountain code RSA algorithm is implemented to reduce the channel band width by transmitting the data into a number of encoded bits. The performance parameters of the algorithm are compared with traditional RSA algorithm. The Fountain Code RSA algorithm performance is evaluated by following parameters such as Packet Loss Ratio, Packet Delivery Ratio, Throughput, Residual Energy and End-to-End Delay

Packet Loss Ratio

Figure 2shows the Packet Loss Ratio for Fountain Code RSA algorithm compared to RSA algorithm. In RSA algorithm, once the duration increases to packet transmit, that the packet loss ratio is increases. However, in Fountain Code RSA algorithm, once the duration increases to packet transmit, that the packet loss ratio is decreases. The maximum packet loss ratio in RSA algorithm is 470%. The maximum packet loss ratio in Fountain Code RSA algorithm is 101%

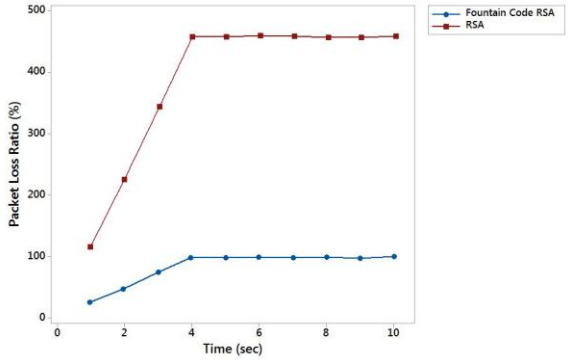

Figure 2. Packet Loss Ratio

Packet Delivery Ratio

Figure 3shows the Throughput for Fountain code RSA algorithm compared to RSA algorithm. In RSA algorithm, once the duration increases to packet transmit, that decreases the packet delievery ratio. However, in Fountain Code RSA algorithm, once the duration increases to packet transmit, that increases the packet delievery ratio. The maximum packet delivery ratio in RSA algorithm is 55% and the maximum packet delivery ratio in Fountain code RSA algorithm is 63%

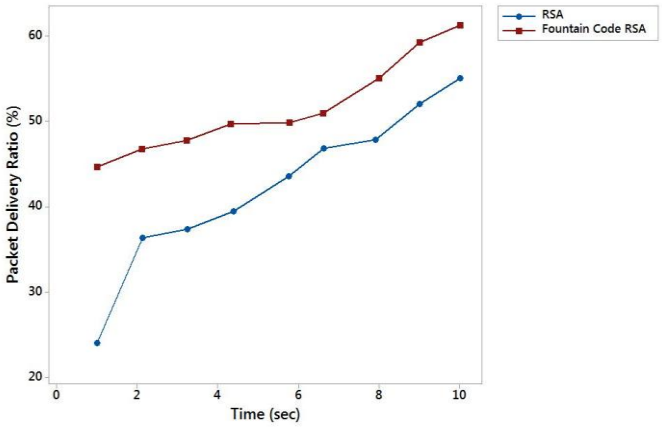

Figure 3. Packet Delivery Ratio

Throughput

Figure 4 represents the Throughput for Fountain Code RSA algorithm compared to RSA algorithm. In RSA algorithm, the throughput is decreases once the required time increases to packet transmit. However, in Fountain Code RSA algorithm, the throughput is increases once the required time increases to packet transmit. The maximum throughput in RSA algorithm is 118 Kbps and the maximum throughput in Fountain Code RSA algorithm is 138 Kbps.

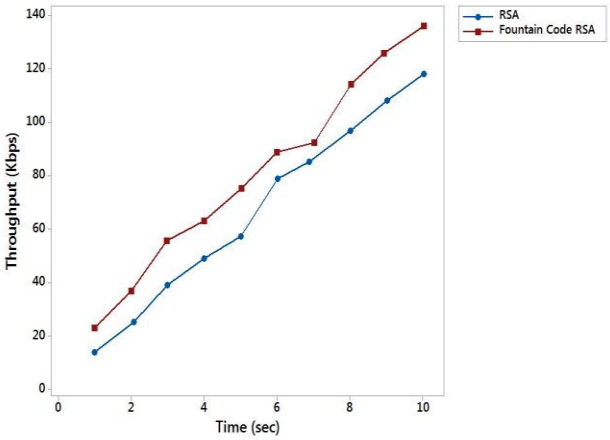

Figure 4. Throughput

Residual Energy

Figure 5 represents the Energy Consumption for Fountain Code RSA algorithm compared to RSA algorithm. The RSA algorithm consumes more energy once the duration increases to packet transmit. However, the Fountain Code RSA algorithm consumes minimum energy once the duration increases to transmit the packet.

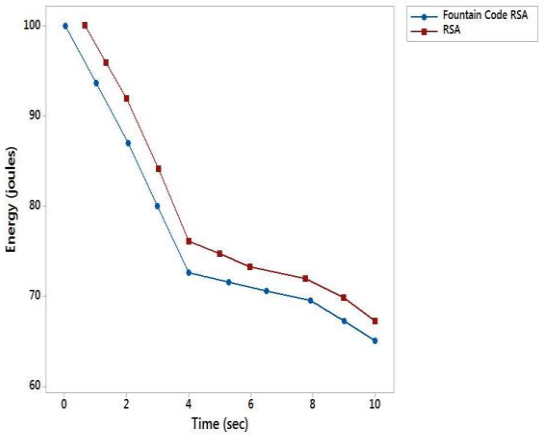

Figure 5. Residual Energy

End-to-End Delay

Figure 6 represents the End-to-End Delay for Fountain Code RSA algorithm compared to RSA algorithm. The RSA algorithm consumes more delay once the duration increases to packet transmit. However, the Fountain Code RSA algorithm consumes less delay once the duration increases to transmit the packet. The RSA algorithm consumes a maximum delay of 2.2 ms and the Fountain code RSA algorithm consumes a maximum delay of 1.7 ms

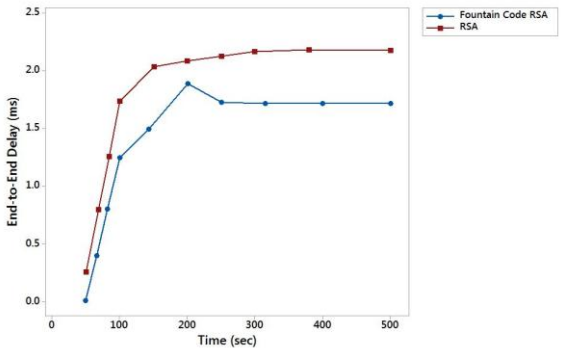

Figure 6. End-to-End Delay

V.CONCLUSION

Generally, RSA Encryption and Decryption algorithm is utilized to provide cloud security. But in RSA, while transmitting the encrypted message, more bandwidth is consumed. Hence to reduce the channel bandwidth, the encrypted message is transmitted into an unlimited number of encoded bits using Fountain Code. The simulation results show an outstanding performance while using Fountain Code RSA algorithm than the traditional RSA algorithm used for cloud security. Packet Loss Ratio, Packet Delivery Ratio, Throughput, Residual Energy and End-to-End Delay shows an outstanding performance while using Fountain code than in using the traditional method. Also the energy consumed in Fountain Code RSA algorithm is less when compared to traditional RSA algorithm. Thus, the Fountain code RSA can be a best alternative to cloud security techniques used at present.

REFERENCES

1. P. Chi and C. Lei, "Audit-Free Cloud Storage via Deniable Attribute-based Encryption," IEEE Trans. Cloud Comput., vol. 7161, no. c, pp. 1–14, 2015.
2. L. Ferretti, F. Pierazzi, M. Colajanni, and M. Marchetti, "Performance and cost evaluation of an adaptive encryption architecture for cloud databases," IEEE Trans. Cloud Comput., vol. 7161, no. c, pp. 1–15, 2014.
3. X. Xu, J. Zhou, X. Wang, and Y. Zhang, "Multi-authority proxy re-encryption based on CPABE for cloud storage systems," J. Syst. Eng. Electron., vol. 27, no. 1, pp. 211–223, 2016.
4. L. Jiang, D. Guo, and S. Member, "Dynamic Encrypted Data Sharing Scheme Based on Conditional Proxy Broadcast Re-Encryption for Cloud Storage," IEEE Access, vol. 14, no. 8, pp. 1–9, 2017.
5. K. Li, W. Zhang, C. Yang, and N. Yu, "Security Analysis on One-to-Many Order Preserving Encryption Based Cloud data Search," IEEE Trans. Inf. Forensics Secur., vol. 6013, no. c, pp. 1–9, 2015.
6. J. Li, X. Lin, Y. Zhang, and J. Han, "KSF-OABE : Outsourced Attribute-Based Encryption with Keyword Search Function for Cloud Storage," IEEE Trans. Serv. Comput., vol. 1374, no. c, pp. 1–12, 2016.
7. C. Liu, S. Member, L. Zhu, J. Chen, and S. Member, "Graph Encryption for Top-K Nearest Keyword Search Queries on Cloud," IEEE Trans. Sustain. Comput., vol. 3782, no. c, pp. 1–11, 2017.
8. J. Sun, Y. Bao, X. Nie, and H. Xiong, "Attribute-hiding Predicate Encryption with Equality Test in Cloud Computing," IEEE Access, vol. PP, no. c, p. 1, 2018.
9. Y. Sun, W. Susilo, S. Member, F. Zhang, and A. Fu, "CCA-secure Revocable Identity-based Encryption with Ciphertext Evolution in the Cloud," IEEE Access, vol. PP, no. c, p. 1, 2018.
10. D. N. Wu, Q. Q. Gan, and X. M. Wang, "Verifiable Public Key Encryption with Keyword Search based on Homomorphic Encryption in Multi-user Setting," IEEE Access, vol. 3536, no. c, pp. 1–9, 2018.
11. S. Wang, J. Zhou, J. K. Liu, J. Yu, and J. Chen, "An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing," Trans. Inf. Forensics Secur., vol. 6013, no. c, pp. 1–13, 2016.
12. R. I. Encryption, J. Wei, W. Liu, and X. Hu, "Transactions on Cloud Computing Secure Data Sharing in Cloud Computing Using," Trans. Cloud Comput., vol. 14, no. 8, pp. 1–13, 2016.
13. P. Xu, T. Jiao, and Q. Wu, "Conditional Identity-based Broadcast Proxy Re-Encryption and Its Application to Cloud Email," IEEE Trans. Comput., vol. 9340, no. c, pp. 1–14, 2015.
14. J. Xu, Q. Wen, W. Li, and Z. Jin, "Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing," IEEE Trans. PARALLEL Distrib. Syst., vol. 9219, no. c, pp. 1–11, 2015.
15. J. Yu, P. Lu, Y. Zhu, G. Xue, and M. Li, "Towards Secure Multi-Keyword Top- k Retrieval over Encrypted Cloud Data ∗," IEEE Trans. DEPEDABLE Secur. Comput., vol. 10, no. 61170238, pp. 1–30, 2013.

AUTHORS PROFILE

Mr A.MANIMARAN is a Research Scholar in **JAYA Engineering College** in the Department of Computer Science and Engineering. He holds his M.E in System Engineering and Operation Research, College of Engineering, Anna University, Chennai and is currently pursuing his research in **St.Peter's Institute of Higher Education and Research** ,St.Peter's University, Chennai. he has 16 years of Academic experience and 3 years of Research experience. He has published in National and International journals.

Dr.K.Somasundaram is having industry and teaching experience about 24 years. He served in various positions in industry and Teaching. He is currently serving as Professor in Computer Science and Engineering department at Chennai Institute of Technology, Chennai. He published about 85 papers in International journals and presented 32 papers in refereed national & International Conferences. There are 8 scholars are completed their research under his guidance and 4 PhD scholars are doing their research. He guided more than 23 M.E., Thesis. He is a member of IE(India), IETE,CSI, ISTE and CEng(IEI). His area of interest includes Data Mining and Data Analytics, Wireless Sensor Networks, Grid/Cloud computing.