Journal of Green Engineering (JGE)

Volume-10, Issue-3, March 2020

Analysis of Energy Efficient Algorithm for Privacy in Mobile Cloud

[1]M. Sankari,[2]P. Ranjana,[3]Y.S Kalaivani

[1]Research Scholar, Department of Computer Science and Engineering, Hindustan Institute of Technology and Science, Chennai, India.E-mail:vpsankarim@gmail.com
[2]Professor, Department of Computer Science and Engineering, Hindustan Institute of Technology and Science, Chennai. India.E-mail:pranjana@hindustanuniv.ac.in
[3]Research Scholar, Department of Computer Science and Engineering, Hindustan Institute of Technology and Science, Chennai, India.E-mail: kalaiys@rediffmail.com

Abstract

For the development of the mobile field, data privacy is the most important challenge while outsourced the data to the cloud storage. The proposed paper discusses about the various energy-efficient algorithms, methodologies, mechanisms, used for securing the mobile's cloud data. It is essential to understand the security of mobile data with ensuring data privacy. The literature survey of energy-efficient security mechanisms focuses on (1) improving the efficiency of mobile devices, (2) reducing the CPU resources, (3) reducing the cost of bandwidth usage and (4) maintaining the authentication in mobile cloud. It recommends ensuring confidentiality, authorization, integrity, data privacy, availability of user's data. The proposed paper aims to provide a descriptive summary of security mechanisms suitable for privacy and explained with the table form. It clearly enforces the security parameters and makes direction for future research in mobile cloud storage.

Keywords: Authentication, Data Privacy, Energy Efficient algorithm, Mobile cloud, Encryption Algorithm.

Journal of Green Engineering, Vol. 10_3, 1123–1138.

Alpha Publishers

1 Introduction

Mobile cloud computing is a combination of cloud computing and mobile computing. Cloud storage is the storage area which we can store, retrieve the data wherever required. It provides various services such as the SaaS, PaaS, and IaaS. It offers the users to utilize the software, hardware, and tools as per the payment basis and storage free service. It allows creating the files, images, photos, videos, and many more. The individual customer, business people, traders, and companies utilize the cloud services. There are various cloud security issues faced by the organization and users. Mobile devices with limited resource constraints, limited battery power, CPU utilization, is an another challenge with the cloud security issues. The combination of mobile and cloud computing is facing various drawbacks such as security, information replication, low reliability and privacy. The user faces major issues of data security for moving the data to the cloud. Some of the major issues handled on the cloud storage.

- Security issues of virtualization/virtual machines.
- Encryption and decryption key management.
- Data Privacy especially customer data.
- Data lost/missing during transmission.
- Fault takes place in physical security like hardware, network, router, wires, and cables.

The analyses of various energy-efficient encryption techniques are used to store the data in the mobile cloud and maintain privacy. In the early stage [1] [2], data are passed to the cloud for encryption. It makes to lose the user's control for protecting data. Later, the partial data are passed to the cloud for encryption. It makes to lose our data by an untrusted third party for their profit. Finally, mobile data are encrypted in mobile and passed the encrypted data to the cloud due to the lack of privacy. The survey papers have explained these kinds of encryption techniques for ensuring privacy. Also, computational overhead is increased. Introducing Light weight Image encryption technique [1] [3] overcomes these issues and provides security/privacy.

2 Literature Survey

Singh et al. [4]noted that the traditional encryption techniques such as AES,RSA,DES and 2-DES were explained about the strength of the techniques and calculation of the execution time.

Modak et al. [5] deeply demonstrated the various scrambling techniques such as XOR, Rubik's, Cubic squares, Scrambling, sudoku and Chaos system. Chaos-based encryption would be high security among all other methods. It is a high sensitivity to initial condition, state ergodicity, and bring long-term unpredictable encryption.

Yamini et al. [6] described the various encryption techniques with security analysis such as correlation, histogram, and time cost of each algorithm. It included the high brute force of searching time, low complexity of execution time. It provides good security.

Ali et al. [7] explained about the RSA algorithm and hash function. It encrypted the data two times which is providing data confidentiality and integrity. First of all, user encrypted the data. The encrypted file is passed to the third-party auditor which is trusted. It ensures confidentiality. The second encryption generated by the third party auditor, which makes the data secure and robust against attacks. It ensures integrity. Data leakage is reduced while transfer encrypted data to the cloud.

Zickau et al. [8] described the user's metadata collected by the method of attribute-based encryption to generate high security. Attributes took over the major role in the encryption technique. It defined the limited access policies to access the data and protect data privacy. Encrypted data are utilized by the authorized users who were satisfied the user's access policies.

Yuan peng xie et al. [9] designed the Hierarchical Attribute-Based Encryption(M-HABE)architecture which is used to generate high security and robust against attacks. It was mainly designed for a multiple user environment. It is the combination of the ciphertext -policy attribute based encryption (CP-ABE) and hierarchical identity based encryption (HIBE).

Rassan et al. [10] introduced a new authentication method by capturing the image in mobile camera rather than the webcam/digital camera. It is used to protect the resources of mobile which is used in the cloud and avoids illegal access. It is used to prevent databases from attacks. It produces 80% accuracy.

Ahmad et al. [11] generated the IdM's(Identity Management) by trusted third party providers in cloud, to control resources by issuing the multiple

tokens. The authorization token was distributed to others which was created by individuals.

Bahrami et al. [12] proposed the new light-weight method which was reduced time complexity in mobile and to improve the speed, throughput, and achieved the superior performance of the method. It was encrypted the data by PRP and passed to different cloud for storage.

Mukesh et al. [13] proposed the database for light-weight encryption method, for fast execution and maintained low complexity in mobile data. The encrypted data are passed to multiple clouds. The Database, keys were managed by a proxy server. Based on the user's query, the data are retrieved through mapping, database, and server.

Bahrami et al. [14] noted that the light-weight method, executed by parallel processing through GPU (Graphics Processing Unit). It improved the speed of the system. It maintained data security and data privacy and executes the huge amount of data in milliseconds. It was used to save energy while outsourced to the cloud.

Arshia et al. [15] noted that the IoT devices have limited resources, low battery power, low speed just like mobile devices which proposed the simple encryption method to store and retrieve the data to ensure privacy. It outsourced the data to third parties who was a semi-trusted. It introduced the new tool 'Contiki' to assess the CPU power consumption of the system. It proves the data security and data privacy.

3 Analysis of Energy Efficient Algorithm for Privacy

The following section are explained the energy efficient algorithm with high security and ensures privacy.

3.1 RSA Algorithm and Hash Function

Ali et al. [7] explained about the RSA algorithm and hash function. It encrypted the data two times which is providing data confidentiality and integrity. First of all, user encrypted the data. The encrypted file is passed to the third-party auditor which is trusted. It ensures confidentiality. The second encryption generated by the third party auditor, which makes the data secure and robust against attacks. It ensures integrity. Data leakage is reduced while transfer encrypted data to the cloud.

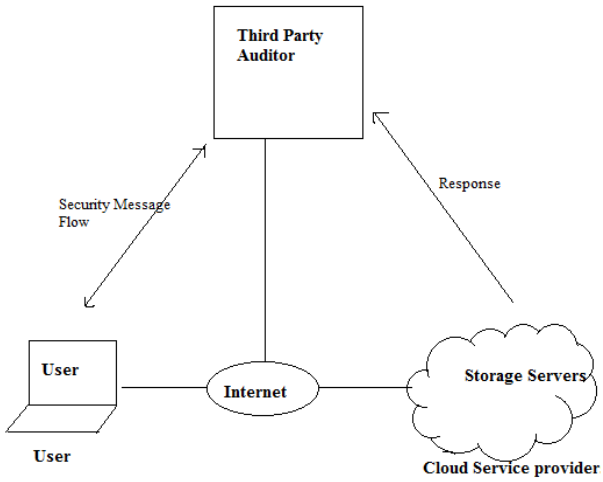

Figure 1. The architecture of RSA and Hash function

The architecture of RSA and hash function was explained in Figure 1. The architecture explained the encrypted data are passes to the third party auditor which is trusted and user are connected to the cloud server through internet. The auditor again encrypted the data for more secure and robust against brute force attacks. It ensures confidentiality and integrity.

3.2 Attribute Based Encryption Mechanism (ABE)

Zickau et al. [8] described the user's metadata collected by the method of attribute-based encryption to generate high security. Attributes took over the major role in the encryption technique. It defined the limited access policies to access the data and protect data privacy. Encrypted data are utilized by the authorized users who were satisfied the user's access policies. It achieved two major goals:(a) user's data history available in the mobile cloud. The basic operation was performed by the users if required. (b) Metadata included key management, distribution handled within the system.

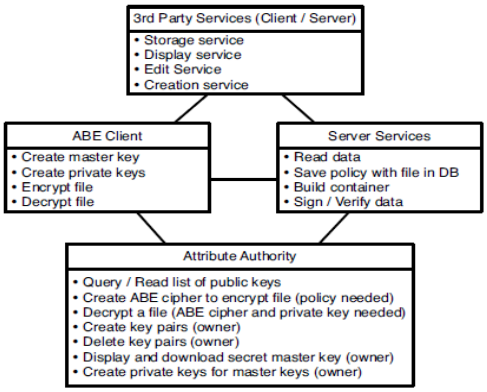

Figure 2. Basic client/Server functionalities with attribute authority

The described attribute authority explained the various functionalities such as ABE client information, third party services, server services, and attribute authority with specific functions such as read the set of lists, create and delete the keys as illustrated in Figure 2.

3.3 Modified Hierarchical Attribute-Based Encryption (M-HABE)

Yuan peng xie et al. [9] designed the Hierarchical Attribute-Based Encryption(M-HABE)architecture which is used to generate high security and robust against attacks. It was mainly designed for a multiple user environment. It is the combination of the ciphertext -policy attribute based encryption (CP-ABE) and hierarchical identity based encryption (HIBE).

The first layer of mobile data was classified based on its model. The second layer encrypted the sensing data by the first layer. The third layer was collected the encrypted data and fulfill the algorithm required to access the ciphertext. Every user has a unique ID, which was identified the internal parties, active within the system.

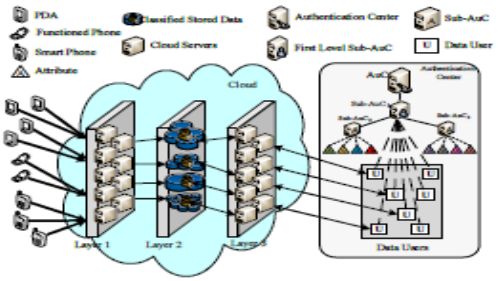

Figure 3. General architecture of M-HABE access control method with three layered structure

The three-layered architecture shown in Figure 3, described the access control of each layer and passed to the user who is authenticated and ensures security.

3.4 Biometric Authentication

Rassan et al. [10] introduced a new authentication method by capturing the image in mobile camera rather than the webcam/digital camera. It is used to protect the resources of mobile which is used in the cloud and avoids illegal access. It is used to prevent databases from attacks. It produces 80% accuracy.

The proposed procedure explains the working process:

1. The fingerprint image is produced by the user through the camera in the enrollment phase to get a fingerprint sample.
2. Pre-processing the sample image. It extracts the features of the image which is converted to grayscale, filtration, effect reduction from RGB image.
3. Further, the featured image is stored in a database.
4. Afterward, the user login with the fingertip image as input and preprocessing used to extract image features.
5. Then compare the features from login user with database verification to identify the user.
6. If the comparison is matched, then the user was accepted. Else, the user was rejected.
7. It was tested with the mobile phone to calculate the processing time for verifying the fingertip user.

3.5 Multi-Token Authorization Strategy

Ahmad et al. [11] generated the IdM's(Identity Management) by trusted third-party providers in the cloud, to control resources by issuing the multiple tokens. The authorization token was distributed to others which were created by individuals. This token consists of two parts. Token1: The token was generated by IdM and passed to the cloud storage and mobile user and the cloud. Token2: The mobile user received the next token after it was generated by the cloud. The token used to avoid unauthorized users to access the cloud. The cloud used it for future reference.

The **stepwise** actions are as follows:

The security arrives from the backchannel communication between the IdM and the cloud. It improved the usage of the mobile battery and prevented the interception by hackers.

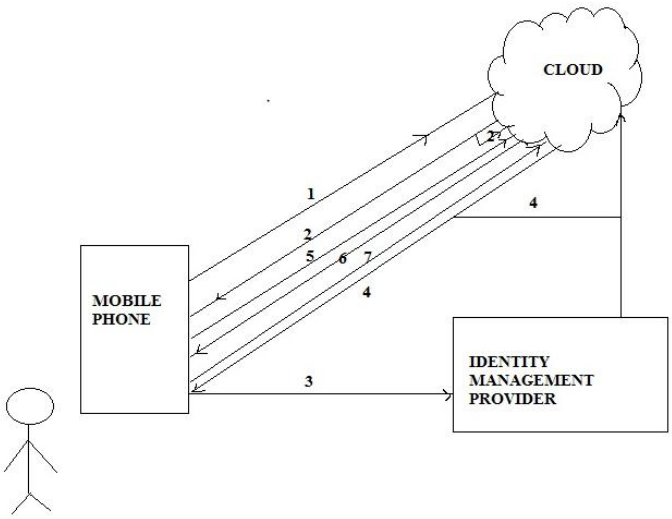

Figure 4. The Architecture of Modified Identity Management System

The architecture explained with the seven steps in Figure 4. The first two steps made the connection and login to the cloud. Then, the third step requested the ID to the Identity management provider(IdM). IdM arose the token and connected to the cloud for storing user information, token Id, and pass it to the mobile user in step 5. Finally, the user and the cloud transferred and stored the data in the last two steps.

3.6 A Light Weight Permutation Based Method

Bahrami et al. [12] proposed the new light-weight method which was reduced time complexity in mobile and to improve the speed, throughput, and achieved the superior performance of the method. It was encrypted the data by PRP and passed to different cloud for storage.

The main purpose was to provide a cost-effective solution, less complexity for mobile users, low computation overheads. It tested the JPEG files with different sizes to ensure energy-efficient. It was stored on multiple cloud computing systems. It ensured privacy also.

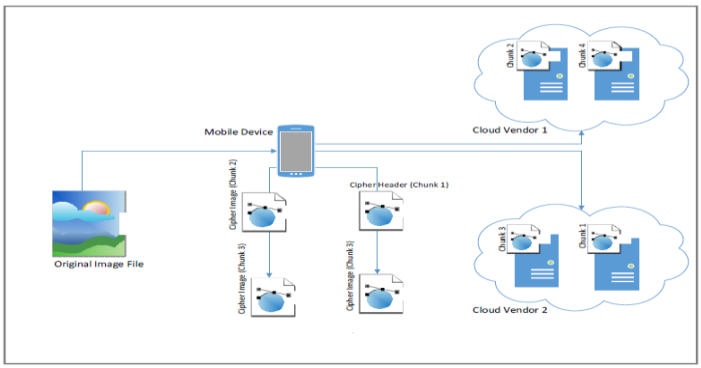

Figure 5. A general view of light weight permutation based method

3.7 Cloud –PDB scheme

Mukesh et al. [13] proposed the database for light-weight encryption method, for fast execution and maintained low complexity in mobile data. The encrypted data are passed to multiple clouds. The Database, keys were managed by a proxy server. Based on the user's query, the data are retrieved through mapping, database, and server. A proxy server was used to store, create, update the data for avoiding complexity.

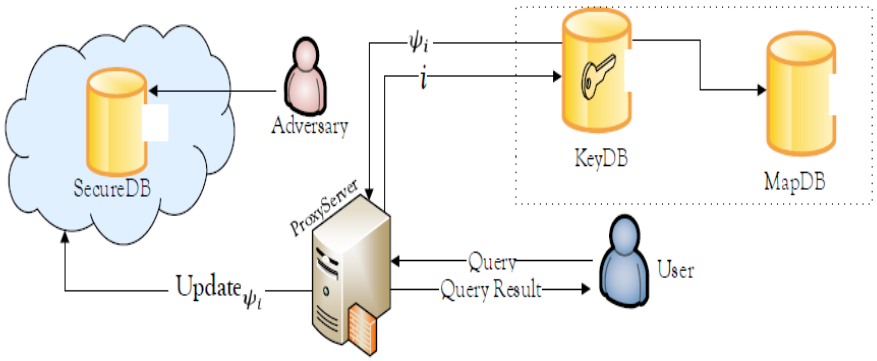

Figure 6. Cloud DPM Scheme

Cloud DPM Scheme implemented based on the proxy server is shown in Figure 6. The Proxy server is managed the keyDB through Map DB. Secure DB updated the data in it based on the users' permission. The user can retrieve the data by its queries.

3.8 *DPM –GPU Method*

Bahrami et al. [14] noted that the light-weight method, executed by parallel processing through GPU (Graphics Processing Unit). It improved the speed of the system. It maintained data security and data privacy and executes the huge amount of data in milliseconds. It was used to save energy while outsourced to the cloud.

3.9 Energy Efficient Data Privacy-IoT Scheme

Arshia et al. [15] noted that the IoT devices have limited resources, low battery power, low speed just like mobile devices which proposed the simple encryption method to store and retrieve the data to ensure privacy. It outsourced the data to third parties who was a semi-trusted. It introduced the new tool 'Contiki' to assess the CPU power consumption of the system. It proves the data security and data privacy.

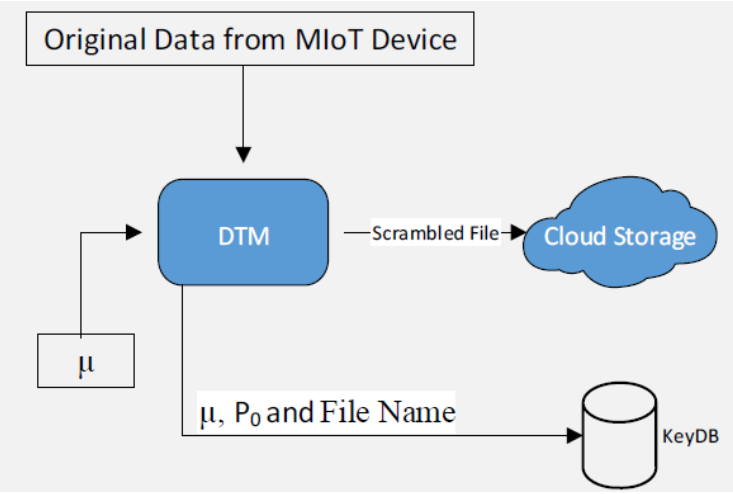

Figure 7. Energy Efficient data Privacy-IoT Scheme

The architecture of IoT-privacy scheme is illustrated in Figure 7. Distributed Trust Management used for IoT devices which is trust-worthy. It collected the data such as P_0,μ acts as keys, and from IoT devices. Encrypted and scrambled data were passed to the cloud.

4 Security Enforcement

The different energy efficient encryption techniques are analysed and explained in Table 1, which ensures high security and privacy. Various techniques such as RSA, ABE, LWE,LWE with DB,LWE with parallel processing are introduced to prove the energy efficient and enforces the data security.

Table 1 Energy Efficient Algorithms for privacy in mobile cloud

S.No	Energy Efficient Techniques	Energy Efficiency	Security Enforcement	Explanation
1	RSA and hash Function [7]	Moderate	Confidentiality Integrity Data Privacy Authentication	Two times encryption makes data robust and ensures data integrity
2	ABE-Model [8]	Moderate	Data Confidentiality Availability Data Privacy	Encryption based on the attribute/s. Randomized keys can find the decryption.
3	M-HABE Model [9]	Moderate	Data Privacy Authentication Confidentiality	Involvement of many layers make a high security.
4	Biometric Authentication [10]	Moderate	Authentication Data Privacy	Success rate of 70-80% accepted for authentication.
5	Multi-Token Authorization [11]	Moderate	User Authorization Data Security Data Privacy	ID management provides token to the users and cloud for easy and safety access. Maintain metadata in mobile device.
6	Lightweight Encryption(LWE) [12]	Low	Data Privacy Confidentiality Integrity	It achieves superior performance than other encryption method (AES, Encoder on JPEG).
7	Cloud -PDB [13]	Low	Data Privacy Data Security	Maintains data in database for fast processing in the mobile.
8	DPM –GPU Method [14]	Low	Data Privacy	Fast processing. Easy to execute the large amount of data.
9	Energy Efficient Data Privacy-IoT Scheme [15]	Low	Data Privacy	Simple Encryption technique used to achieve high security

Table 1 concluded that the light weight encryption algorithm as the energy-efficient, power saving and speed up the process with low complexity.

5 Conclusion

For the analysis of the energy efficient algorithms, there are several methods are discussed with various security parameters to ensure confidentiality, data privacy, authentication, data integrity and authorization in mobile cloud. Encryption takes important role to ensure security. And mainly secure the shared cloud resources in cloud through mobile users. Finally, light weight encryption concluded as the good energy efficient algorithm compared to all other methods to ensure privacy also. For future research work, it will provide opportunities for researchers to extend their work in securing techniques and ensure data robust and scalable. The survey of this paper encourages the future researcher to understand the various methodologies for security and data privacy and make them to do the further research in mobile cloud storage.

References

[1] M. Sankari and P. Ranjana, "PLIE- A Light-weight Image Encryption for data Privacy in mobile cloud storage," International journal of engineering and technology(UAE), vol. 7, no. 4.36, pp. 368-72, 2019.

[2] M. Sankari, P. Ranjana and D. Venkata Subramanian, "Iprivacy-Performance Measurement of Encrypted Image Over Mobile Cloud," International Journal of Recent Technology and Engineering (IJRTE), vol. 8, no. 4, pp. 2919-23, Nov 2019.

[3] M. Sankari and P. Ranjana, "Privacy-Preserving Lightweight Image Encryption in Mobile Cloud," Advances in Intelligent Systems and Computing, bangalore,pp. 403-414, 2019.

[4] G. Singh and Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," International Journal of Computer Applications , vol. 67, no. 19, pp. 33-38, 2013.

[5] P. M. Modak and D. V. Pawar, "A Comprehensive Survey on Image Scrambling Techniques," International Journal of Science and Research (IJSR), vol. 4, no. 12, pp. 814-18, 2015.

[6] Yamini jain et al., "Image Encryption Schemes:A Survey," International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 9, no. 7, pp. 157-192, 2016.

[7] Ali E.Taki et al., "Digital Image Encryption based on RSA Algorithm," IOSR Journal of Electronics and Communiication Engineering(IOSR-JECE), vol. 9, no. 1, pp. 69-73, jan 2014.

[8] S. Zickau, F. Beierle and I. Denisow, "Securing Mobile Cloud Data with Personalized Attribute-Based Meta Information," in 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, San Francisco, CA,pp 205-201, 2015.

[9] Y. Xie, H. Wen, B. Wu, Y. Jiang and J. Meng, "A Modified Hierarchical Attribute-Based Encryption Access Control Method for Mobile Cloud Computing," vol. 7, no. 2, pp. 383-91, 1 april 2014.

[10] A. Rassan and H. AlShaher, "Securing Mobile Cloud Computing Using Biometric Authentication (SMCBA)," in International Conference on Computational Science and Computational Intelligence (CSCI),pp.157-161, 2014.

[11] A. Ahmad, M. M. Hassan and A. Aziz, "A Multi-token Authorization Strategy for Secure Mobile Cloud Computing," in 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, Oxford, pp. 136-141,2014.

[12] M. Bahrami and M. Singhal, "A Light-Weight Permutation Based Method for Data Privacy in Mobile Cloud Computing," in 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), San Francisco, CA.,pp. 189-98, 2015.

[13] M. Bahrami and M. Singhal, "CloudPDB: A light-weight data privacy schema for cloud-based databases," 2016 International Conference on Computing, Networking and Communications (ICNC), pp. 1-5,, 2016.

[14] M. Bahrami, D. Li, M. Singhal and A. Kundu, "An Efficient Parallel Implementation of a Light-weight Data Privacy Method for Mobile Cloud Users," Seventh International Workshop on Data-Intensive Computing in the Clouds (DataCloud), pp. 191-95, 2016.

[15] M. Bahrami, A. Khan and M. Singhal, "An Energy Efficient Data Privacy Scheme for IoT Devices in Mobile Cloud Computing," in IEEE International Conference on Mobile Services (MS), San Francisco, CA,pp. 190-95, 2016.

Biographies

Sankari M , doing her Ph.d in Hindustan Institute of Technology and Science, Chennai, Tamilnadu. She has completed B.E in computer Science and Engineering from Bharat Niketan Engineering College , under Anna University, 2006.She did her Master degree M.E in Computer Science and Engineering from Hindustan Institute of Technology and Science under Anna University,Chennai,2009. She was worked in Engineering College, under Jawaharlal Nehru Technical University, Hyderabad. She has published five international conference papers and three international journals and three national conferences. She conducted presentation Lab and mentors for engineering students. She attended many workshop and handled many research field seminars. She is interested in the field of image processing, cloud storage, security and networks.

Ranjana P is a Professor in Hindustan Institute of Technology and Science, Chennai. She received her Ph.d in computer science from Hindustan University, Chennai,2017. She received M.E in Computer Science and Engineering from Anna university, Chennai,2005. She received MCA from Madurai Kamaraj university, Madurai,1998. She is conducted many conference, seminars and workshops. She is a coordinator of a NBA, NAAC, UGC-CSE and PG students. She has published papers in 25 international Conferences and 50 international journals. Her area of interests includes image processing, cloud, network and security.

YS Kalaivani is a professor in Sindhi College, Bangalore, India. She has completed Bsc Mathematics in Madras University, MCA in Madras University and M.phil in Bharathidasan University. She is doing her Ph.d in Hindustan Institute of Technology and Science, Chennai, Tamilnadu. She has published papers in 5 international Conferences and 5 international journals. Her area of interests includes image processing, hadoop, big data.