Survey on Attribute-based Encryption in Cloud Computing

P. R. Ancy, Addapalli V. N. Krishna, K. Balachandran, M. Balamurugan, and O. S. Gnana Prakasi

(Corresponding author: P. R. Ancy)

Department of Computer Science, Engineering, Christ University
Bengaluru, Karnataka, India
(Email: ancy.prasadam@res.christuniversity.in)

(Received Feb. 10, 2020; Revised and Accepted June 8, 2020; First Online July 26, 2020)

Abstract

Attribute-Based Encryption (ABE) is an appropriate solution to the access mechanism and security issues in cloud computing. As we know cloud computing is the emerging technique and solution for problems such as storage, security, efficiency, and many more facing today. As cloud computing arises as a new technology many issues and confusion are arising with it mainly regarding the security of the data. The cloud providers are capable of storing enough data, but the user is having doubt about how much security the cloud providers are giving to the data. Due to this reason, many organizations and companies are not willing to move to the cloud environment. So, Attribute-Based Encryption came as a solution to this problem. As per our comprehensive survey that has been done on different ABE schemes, we have included the recent ABE schemes, different access policy, problems, and their solutions for ABE in this paper. Finally, this paper also includes the security comparison and efficiency comparison of different ABE schemes.

Keywords: Access Control; Ciphertext-Policy Attribute-Based Encryption; Multiauthority; Revocation Mechanism

1 Introduction

Security is one of the main aspect of cloud computing. With the development of cloud computing, many data owners store their data in the cloud server for simplifying local IT management and reducing the cost [17]. Cloud storage is one of the major services provided by cloud computing [12]. It enables data owners to remotely host their data by outsourcing them to cloud servers, which brings great convenience for both individuals and enterprises to share data over the Internet [16, 24, 25]. As today every organization is moving to cloud for different services their main concern is on how much secure is their data in the cloud provider's environment. Therefore this is the main area where many types of research are going through. For enhancing security in cloud storage many methods are introduced and one among them is ABE (Attribute-Based Encryption) [4]. ABE is a type of public-key encryption in which the sender encrypts the message using receiver's public key and the receiver decrypt the message using the private key. The main key point of ABE is outsourcing which means the data is encrypted within the source or sender's environment and sends it to the service provider's environment for storing it.

In ABE encryption and decryption are done using a set of attributes and access policy. Attributes are the secret key of a user and the ciphertext is dependent upon attributes. Like traditional identity-based encryption, the sender in an ABE system only needs to know the receiver's description in order to determine their public key [2]. The decryption of the ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext.

There are two types of access structure monotonic access structure and non-monotonic access structure. Monotonic access structure support "AND " and "OR" between attributes and non-monotonic access structure support "NOT" with "AND" and "OR" between attributes. [10] proposed a method that can convert any monotone circuit to an equivalent access tree. There are two types of ABE, Key Policy Attribute-Based Encryption (KP-ABE) and Ciphertext Policy Attribute-Based Encryption (CP-ABE). In KP-ABE data is encrypted using attributes and decrypted using access policy and in CP-ABE data is encrypted using access policy and decrypted using attributes. About the number of authorities, a system has there are two types of system single authority system and multiauthority system. In the case of revocation, there are attribute revocation and user revocation. Attribute revocation is changing the user's attributes because of the expiring of attributes, revoke of attributes or need of adding new attributes. And in the case of user revocation, the system should satisfy both forward and backward security. In forward security, revoked users should not access new ciphertext using an old secret key and in backward security newly joined users not give the privilege to access the previous ciphertext.

2 Related Work

A new scheme is suggested [3] that can withstand any number of corrupt authorities. The author applies this technique to attain a multi-authority form of identical access control Attribute-Based Encryption. According to this scheme each user has to prove his set of attributes to the third party to obtain a secret key. The user can use this secret key to decrypt the message. The main challenge of single authority Attribute-Based Encryption is preventing collusion. This problem is addressed in this paper by introducing the multiauthority scheme. A scheme is intrduced by [1] for the identification of encrypted information with complex access control called CP-ABE. According to the work, the author proposed that even if the storage server is untrusted, the information could be kept confidential. And also, this method is secure against collusion attacks. In this paper, the author used the concept of attributes.

The characteristics are used to define the credentials of a user, and information is determined by a party encryption policy for who can decrypt. A new security model of honest but curious servers to identify possible attacks [27]. This scheme allows the authority to cancel any characteristic at any period by inserting a minimum load on the user. This method applies to Key Policy ABE. The author addresses the attribute revocation issue in the attribute-based system. [11] addressed some challenging issues in different scenarios and different policy updates. Ciphertext-Policy ABE is a promising solution for these issues like access policy and data storage. Some problems can occur to these types of framework that is revocation problem. In this article, the author develops an access control policy that has an effective revocation capability that is user and attribute.

An access policy is efficient to promise safety in cloud data [26]. Data storing in insecure cloud third parity become an issue in deciding access policy. For this ciphertext-policy, ABE is an adequate scheme because the owner is deciding policy. But it is difficult to introduce due to revocation issue. For this reason, the author introduces an effective revocation access policy that applies to multiple authority scheme. Also, this system can achieve both backward and forward safety. [6] suggests access structures can represent by the monotonic or non-monotonic way. One of the best techniques to store data with encryption is ABE. In this article, the author addresses the key escrow problem and find a perfect solution to solve it. The author resolves this key escrow problem by introducing 2pc protocols in the system. A new multilevel secret sharing system is introduced by [13] expanding the Shamir's to the global threshold that is exclusively higher than the compartment's number of thresholds. The article also shows how to use the polynomial interpolation-based threshold secret sharing systems. Proposes two effective systems that linearly proportion the number of public shares to the number of respondents.

A novel multi secret-sharing system based on Hermite interpolation is implemented [21]. According to the threshold as well as value and number of secrets the proposed scheme is dynamic to the changes. This scheme has a key feature of multi-usability. The article also provides multi-user function over elliptic curves by solving the discrete logarithm issue. This assumes that n members and the dealer is not one of them. He will unbiassed set the system up and issues the standards. The members will give their shares to a combiner, who is any one of the members for reconstructing the secret. By extending the Key-Policy ABE with attribute privacy preservation in cloud storage [8] proposes an Effective Attribute-based Access Control with Authorized Search system. It is further effective than current solutions on calculation and storing expenses. The aim is to suggest Key Policy-ABE with partly concealed characteristics constructed on the search for sensitive keywords and to demonstrate that the system is safe under the q-2 decisional bilinear DH supposition. [14] defines a threshold version of the Localized Multi-secret Sharing Scheme (LMSS). The author provides lower limits on The decryption share size of localized multi-secret sharing systems in a particular background and gives clear development of systems. The author also analyses various methods to relax the model providing trade-offs among the shared scope and between the number of safety assurances given by this system to allow the development of a small number of shared systems.

3 Attribute-based Encryption

The concept of ABE is first introduced by Sahai and Waters on the paper called Fuzzy Identity-Based Encryption [19]. In ABE data is encrypted using a set of attributes. ABE is a scheme in which each user is identified by a set of attributes, and some function of those attributes is used to determine decryption ability for each ciphertext [3]. Attribute-Based Encryption (ABE) is a type of public-key encryption. Using this public-key encryption, the message is encrypted and decrypted using a public key and private key respectively for a specific receiver. In attribute-based encryption, it contains a set of attributes where secret key and ciphertext are attributes dependent. Here a user can decrypt the ciphertext only when the attributes of the ciphertext match the attributes of the user key. The user encrypts the data using an access policy or access structure. An example of access policy is Area=Italy AND age <30 AND Business=Researcher. There are two types of access structure monotonic and non-monotonic. Two kinds of ABE exist they are Key-Policy ABE and Ciphertext-Policy ABE. Due to some issues in Key-Policy ABE such as access policy is storing in a third party so it may have a chance that he can change access policy so we are mainly focusing on Ciphertext-Policy ABE.

3.1 Key Policy Attribute-based Encryption

In KP-ABE secret keys for users are generated based on access structure and encryption of data is done based on a set of attributes. The decryption of the message is done when user attributes satisfy the access structure. The most common access structure used is a tree-based access structure. The main issue in Key-Policy ABE is access policy are storing in a third party so it may have a chance that he can change access policy. In this paper, we are mainly focusing on ciphertext policy attribute-based encryption.

3.2 Ciphertext Policy Attribute-based Encryption

In CP-ABE data is encrypted using access trees and a set of attributes is used for generating user's secret keys. There are two types of system models for the CP-ABE scheme, single authority and multi-authority. In single authority systems in Figure 1 there is only one attribute authority called central authority and all attributes of the system are managed by this central authority. In the case of a multi-authority system in Figure 2, there are multiple attribute authority and attributes that are shared across these authorities. The main entities of system architecture are:

Attribute Authority: The entity which checks the validity of user attributes ana sets up parameters and secret key. It is responsible for key updating and revocation process.

Data Owners: The entity that wants to store data safely on cloud storage. This is achieved by outsourcing data that is sending encrypted data to the cloud. The data owner is the one who defines access policy to the data.

Data Users: The entity which has a set of attributes and secret key to access the ciphertext.

Cloud Servers: The entity which has the charge of storing encrypted data from data owners.

In the framework, five algorithms are used:

Setup: The attribute authority generates the parameters for Public Key (PK) and Secret Key (SK).

KeyGeneration: The attribute authority generates Public Key and Secret Key based on the parameters and attribute set.

Encryption: The message is encrypted using a Public Key and access structure.

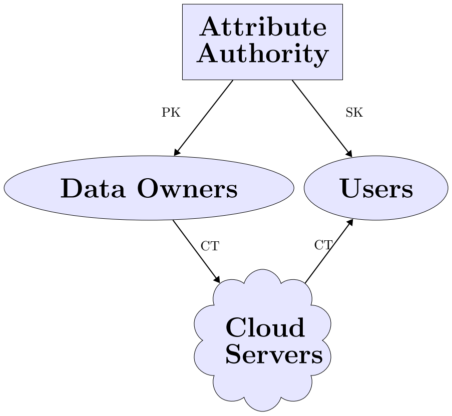

Figure 1: Single authority system

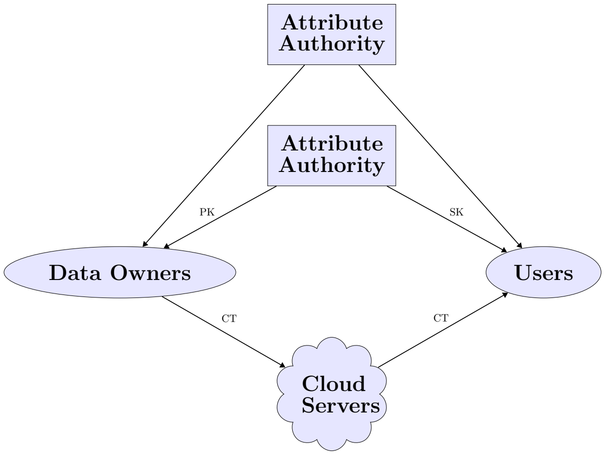

Figure 2: Multi-authority system

Decryption: The ciphertext is decrypted by data users using the secret key.

Delegation: The updating and revocation process are handled by taking the private key and regenerate a new key.

3.2.1 CP-ABE schemes

In this section, we are discussing recent CP-ABE schemes and the different access policies. A directly revocable attribute-based encryption (DR-CP-ABE) scheme [22] is introduced by constructing a complete subtree for access structure and is solved by the subset cover method. For data confidentiality and to keep the privacy of signcryptor [18] a ciphertext-policy attribute-based signcryption (CP-ABSC) is used with an access policy of monotone span programs. Using this method, they achieved shorter ciphertext size when compared to the schemes which already exists. A new system architecture was introduced by [15] for securely sharing data to a cloud by a user of limited resources. Using a linear secret sharing scheme it achieves high- efficiency, fine-grainedness, and data confidentiality. Managing access policy in a cloud storage system is an importing task [23] and a scalable ciphertext-policy attribute-based encryption (SCP-ABE) is introduced for that.

The most common access policy used is a monotonic access structure but here a different access policy called blocked linear secret sharing scheme (BLSSS) is used. A matrix is used to describe a tree circuit of access structure due to this special scheme scalability is achieved. Another recent ABE scheme is the ciphertext-policy attribute-based hierarchical document collection encryption (CP-ABHE) scheme [5] which access trees are combined according to attribute sets. This scheme uses an access tree that contains only "AND" gate and so it is called monotone access structure. Security of outsourced data is the main concern of personal health records in the cloud [7] and a hierarchical CP-ABE scheme with multiple authorities was introduced. As hierarchical files are sharing the author used a layered model of access structure. Access structures are combined to form a single one as this paper is dealing with the sharing of hierarchical files.

An ABE scheme that is applicable for resource-constrained mobile devices [9] is a lightweight attribute-based encryption (LBE) scheme. This paper introduced a scheme that is applicable to cyber-physical systems and based on monotone access structure. This means AND gate are used as access policy. Another one scheme for mobile cloud is decentralized multi-authority attribute-based encryption [20] scheme which is an appropriate solution of key escrow problem and is based on a monotone access policy. For preserving the privacy of the user, a CP-ABE scheme with hidden access policy [28] is introduced called hidden access policy CP-ABE (HP-CP-ABE) scheme is introduced. This scheme improves data confidentiality and protects the user's privacy. This is achieved by an access policy of a monotonic access structure with the "AND" gate.

3.2.2 Challenges

In this section, we are discussing different challenges and proposed solutions. The main problem of the existing ABE scheme is the lack of user revocation mechanism [22] and one solution for this is by introducing one more entity in the system architecture called user revocation centre (URC). URC is maintaining a revocation list and all revocation tasks are outsource to this third-party organization. Lack of scheme which achieves security goals such as data confidentiality, privacy, fine-grainedness [15, 18] of cloud data sharing still unresolved. Managing access policy [23] is a critical issue of the ABE scheme. The existing policy managing schemes have high computation complexity and communication overhead. One solution for this is using a blocked linear secret sharing scheme (BLSSS) in which a matrix is used to describe tree-circuit. Another one main challenge concerning limited resource devices and mobile cloud [9, 20] is to reduce computation and communication overhead.

Even though many ABE schemes are introduced for this challenge anyone can find out a better scheme that can achieve low processing time, which takes limited storage space, limited resources and limited energy. One major challenge addressed by [28] is protecting user's personal privacy. This is an important issue that has to address at present. Along with this one should concentrate on developing a scheme that is efficient in communication and computation cost. Some issues addressed by the author are data confidentiality, efficient decryption test, efficiencies such as parameter size and time complexity of algorithm. Scalable user revocation [24] is an important issue. Here one can develop an ABE scheme that provides both forward security and backward security. The above discussed are the major challenges faced by the recent ABE schemes.

3.2.3 Security

The different frameworks used to prove the system security is discussed in this section. The security of an ABE scheme can be proven using dual system encryption in the standard model [22]. This scheme is indistinguishable under chosen-plaintext attacks. Most of the ABE schemes prove their security under decisional bilinear Diffie-Hellman exponent (dBDHE) [5, 7, 9, 18, 20, 28]. For some schemes, security analysis is done with random oracles [18, 23]. Some paper proves the security of the scheme against chosen-ciphertext attacks [15]. Security can also be proven against a collusion attack [23]. One of the main security issue is Key escrow problem. Existing multi-authority attribute-based encryption schemes however still require a trusted central authority to publish system parameters and to generate user secret keys. They give to the trusted central authority enough privileges to access the plaintext information meant for the user, a problem referred to as key escrow issue [20]. This scheme solves the key escrow problem by removing the central authority, without making use of any global user identity.

3.3 Comparison

In this section, we compare the various existing CP-ABE schemes and is given in the following Table 1. we compare different scheme against the access structure used, the number of authorities, revocation mechanism is addressed or not and the security assumption followed by the scheme.

3.4 Conclusion

In this paper, we have done a comprehensive survey of recent CP-ABE schemes along with the access policy used by these schemes. We also discussed the major challenges faced by CP-ABE schemes and the existing solution for that issue. One who wants to work on this can take any mentioned issue and can develop a better CP-ABE scheme. The security analysis model of different schemes also discussed. Finally, we compare different

Table 1: Comparison of CP-ABE schemes

Scheme	Access structure	Authority	Revocation mechanism	Security assumption
Fu, J., and Wang, N. [5]	Tree	Single	No	DBDH
Gadge.,Snehlata et al [6]	Tree	Single	Yes	-
Guo, R., et al [7]	Tree	Multiple	Yes	DBDH
Hao, Liu., et al [8]	Tree	Single	No	DBDH
He, Q., et al [9]	LSSS	Single	Yes	DBDH
Hur, Junbeom., et al [11]	Tree	Single	Yes	-
Li, J., et al [15]	LSSS	Single	No	CCA
Liu.,Fan., et al [17]	LSSS	Single	No	DBDHE
Rao, Y. S. [18]	Tree	Single	Yes	DBDH
Arthur Sandor, V. K., et al [20]	LSSS	Multiple	No	DBDH
Wang, H., et al [22]	LSSS	Single	Yes	CPA
Wang, J., et al [23]	BLSSS	Single	Yes	DBDH
Wei, J., et al [24]	LSSS	Multiple	Yes	DBDH
Yang, Kan., et al [26]	LSSS	Multiple	Yes	BDHE
Zhang, L., et al [28]	Tree	Single	No	DBDH

schemes against the access structure used, the number of authorities, revocation mechanism is addressed or not and the security assumption followed by the scheme.

References

[1] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE symposium on security and privacy (SP'07)*, IEEE, pp. 321–334, 2007.

[2] Z. Cao, L. Liu, and Z. Guo, "Ruminations on attributebased encryption," *International Journal of Electronics and Information Engineering*, vol. 8, no. 1, pp. 9–19, 2018.

[3] M. Chase, "Multi-authority attribute based encryption," in *Theory of Cryptography Conference*, Springer, pp. 515–534, 2007.

[4] P. S. Chung, C. W. Liu, and M. S. Hwang, "A study of attribute-based proxy re-encryption scheme in cloud environments", *International Journal of Network Security*, vol. 16, no. 1, pp. 1-13, 2014.

[5] J. Fu and N. Wang, "A practical attribute-based document collection hierarchical encryption scheme in cloud computing," *IEEE Access*, vol. 7, pp. 36 218–36 232, 2019.

[6] M. S. V. Gadge, "Analysis and security based on attribute based encryption for data sharing," *International Journal of Emerging Research in Management & Technology*, pp. 2278–9359, 2014.

[7] R. Guo, X. Li, D. Zheng, and Y. Zhang, "An attribute-based encryption scheme with multiple authorities on hierarchical personal health record in cloud," *The Journal of Supercomputing*, pp. 1–20, 2018.

[8] J. Hao, J. Liu, H. Wang, L. Liu, M. Xian, and X. Shen, "Efficient attribute-based access control with authorized search in cloud storage," *IEEE Access*, 2019.

[9] Q. He, N. Zhang, Y. Wei, and Y. Zhang, "Lightweight attribute based encryption scheme for mobile cloud assisted cyber-physical systems," *Computer Networks*, vol. 140, pp. 163–173, 2018.

[10] P. Hu and H. Gao, "A key-policy attribute-based encryption scheme for general circuit from bilinear maps," *International Journal of Network Security*, vol. 19, no. 5, pp. 704–710, 2017.

[11] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1214–1221, 2010.

[12] M. S. Hwang, T. H. Sun, C. C. Lee, "Achieving dynamic data guarantee and data confidentiality of public auditing in cloud storage service," *Journal of Circuits, Systems, and Computers*, vol. 26, no. 5, 2017.

[13] P. S. Kumar, R. R. Kurra, A. N. Tentu, and G. Padmavathi, "Multi-level secret sharing scheme for mobile ad-hoc networks," *International Journal of Advanced Networking and Applications*, vol. 6, no. 2, pp. 22–53, 2014.

[14] T. M. Laing, K. M. Martin, M. B. Paterson, and D. R. Stinson, "Localised multisecret sharing," *Cryptography and Communications*, vol. 9, no. 5, pp. 581–597, 2017.

[15] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," *Computers & Security*, vol. 72, pp. 1–12, 2018.

[16] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of attribute-based access control with user revocation in cloud data storage," *International Journal of Network Security*, vol. 18, no. 5, pp. 900–916, 2016.

[17] Z. Liu and Y. Fan, "Provably secure searchable attribute-based authenticated encryption scheme," *International Journal of Network Security*, vol. 21, no. 2, pp. 177–190, 2019.

[18] Y. S. Rao, "A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing," *Future Generation Computer Systems*, vol. 67, pp. 133–151, 2017.

[19] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 2005, pp. 457–473.

[20] V. K. A. Sandor, Y. Lin, X. Li, F. Lin, and S. Zhang, "Efficient decentralized multi-authority attribute based encryption for mobile cloud data storage," *Journal of Network and Computer Applications*, vol. 129, pp. 25–36, 2019.

[21] M. H. Tadayon, H. Khanmohammadi, and M. S. Haghighi, "Dynamic and verifiable multi-secret sharing scheme based on hermite interpolation and bilinear maps," *IET Information Security*, vol. 9, no. 4, pp. 234–239, 2014.

[22] H. Wang, Z. Zheng, L. Wu, and P. Li, "New directly revocable attribute-based encryption scheme and its application in cloud storage environment," *Cluster Computing*, vol. 20, no. 3, pp. 2385–2392, 2017.

[23] J. Wang, C. Huang, N. N. Xiong, and J. Wang, "Blocked linear secret sharing scheme for scalable attribute based encryption in manageable cloud storage system," *Information Sciences*, vol. 424, pp. 1–26, 2018.

[24] J. Wei, W. Liu, and X. Hu, "Secure and efficient attribute-based access control for multiauthority cloud storage," *International Journal of Network Security*, vol. 12, no. 2, pp. 1731–1742, 2016.

[25] C. Yang, Q. Chen, Y. Liu, "Fine-grained outsourced data deletion scheme in cloud computing," *International Journal of Electronics and Information Engineering*, vol. 11, no. 2, pp. 81–98, 2019.

[26] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," *IIEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 7, pp. 1735–1744, 2013.

[27] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, pp. 261–270, 2010.

[28] L. Zhang, Y. Cui, and Y. Mu, "Improving security and privacy attribute based data sharing in cloud computing," *IEEE Systems Journal*, 2019.

Biography

Ancy P. R. is currently pursuing her PhD in Computer Science and Engineering from CHRIST(Deemed to be University), Bangalore, India. She has received her M.Tech in Computer Science and Engineering from Marian Engineering College, India. She has worked as Assistant Professor for over three years.Her research interest includes Network Security, Cryptography and Cloud Computing.

Addepalli V. N. Krishna is working as Professor in Computer Science and Engineering department at CHRIST(Deemed to be University), Bangalore, India. He received Ph.D in 2010 at Department of Computer Science and engineering, Acharya Nagarjuna University, AP, India and M. Tech degree in 2001 from department of Computer Science and Engineering, Birla Institute of Technology, Mesra, Ranchi, India. He is having 25 years of teaching experience at undergraduate and postgraduate engineering level. His research interests includes Security algorithm design in wireless sensor networks, Advanced key management algorithms for computer security and protocol design for network security.

K. Balachandran is working as H.O.D and Professor in Computer Science and Engineering department at CHRIST(Deemed to be University), Bangalore, India. He received Ph.D in 2015 at Department of Computer Science and engineering, Anna University, India.He pursued his BSc and MCA from Bharathidasan University, MSc Physics from Annamalai University, MTech (IT) from Allahabad Agricultural University and MPhil from Alagappa University. He has worked as a scientific officer for two decades with the Department Atomic Energy, India. Many of his research papers have won the best paper award at national and international conferences. His area of research includes Data Science, Networks, Big data Analytics and Computer Architecture.

Balamurugan M. is working as Associate Professor in Computer Science and Engineering department at CHRIST(Deemed to be University), Bangalore, India. He received Ph.D in 2013 at Department of Computer Science and engineering, Anna University, India. He is having 13 years of teaching experience at undergraduate and postgraduate engineering level. His area of research includes Machine Learning, Big data Analytics and Data mining.

O. S. Gnana Prakasi is working as Assistant Professor in Computer Science and Engineering department at CHRIST(Deemed to be University), Bangalore, India. She received Ph.D. in 2017 from Anna University, India. She received her B.Tech. degree in Information Technology and M.E. degree in Software Engineering from Anna University. Her research interest includes, Mobile Ad hoc Networks, IoT, Software Engineering and Machine Learning.