

Key-cipher policy attribute-based encryption mechanism for access control of multimedia data in cloud storages

Kavyasri Madakaripura Nagaraju, Ramesh Boraiah

Department of Computer Science and Engineering, Malnad College of Engineering, Karnataka, India

Article Info

Article history:

Received Sep 29, 2021

Revised Jul 5, 2022

Accepted Aug 1, 2022

Keywords:

Access policy

Attribute revocation

Data owner

Key-cipher-policy based ABE

Secure access

ABSTRACT

Cloud technology is advancing at a rapid pace. Many applications and multimedia data are hosted in the cloud, Security, confidentiality, and efficiency are the key drawbacks of cloud computing. There are a variety of access control systems on the market to secure the data and applications on the cloud. But key generation time is a major flaw both in multi-authority and single authority systems. Cipher policy attribute-based encryption (CP-ABE) is one of many cryptographic algorithms available for ensuring user confidentiality which provides fine-grained access control. It also addresses a number of issues related attribute revocation, key generation time, and issues in handling a large number of attributes. We present a mechanism called key-cipher-policy-based ABE (KCP) in this article, which is a hybrid approach and combines CP-ABE and KP ABE approaches which result in handling a wide range of attributes, an efficient key generation process, and addresses challenges in attribute revocation.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Kavyasri Madakaripura Nagaraju

Department of Computer Science and Engineering, Malnad College of Engineering

Hassan, Karnataka, India

Email: kavyasrimn88@gmail.com

1. INTRODUCTION

Cloud computing as a technology makes a big shift from the traditional thinking to the usage of information technology (IT) resources. Cloud service providers supply a variety of services through the internet for a fee. This is a combination of parallel and distributed computing technologies where work is performed simultaneously on several units. The user will rent resources from the cloud services provider, who will not have to worry about maintenance and can focus on the task at hand. As technology progresses, multimedia is becoming increasingly important in the present environment. Multimedia is a powerful communication tool. Multimedia includes video, animation, music, and other mediums. Multimedia can be preserved on storage devices, but with the advent of cloud computing, more enterprises are turning to storage services. Storage-as-a-service is the most popular types of cloud computing. A cloud service provider delivers cloud-based services. Multimedia data stored on a data storage in the cloud. When storing and accessing multimedia data, the data storage server has privacy and security difficulties. We're focusing on work-related security concerns as well as issues with attribute revocation in conjunction with secure access control. We must protect the majority of data stored in cloud storage because it is highly sensitive. Secure attribute revocation is also required to protect the security of the user's data. A primary challenge is secure access to multimedia data housed in cloud data centers.

When it comes to security, data encryption is the most effective way to safeguard sensitive data from unauthorised access. Earlier public key encryption often called as identity encryption, requires that encrypted data be encrypted by a single user. However, it lacks advanced data interchange capabilities. To overcome this

problem, the attribute based encryption (ABE) algorithm was developed of the identity based encryption concept, in which a set of descriptive attributes rather than a single string is utilized to define the user's identity. In comparison to identity-based encryption, ABE enables flexible one-to many encryption instead of one-to-one encryption. Schemes [1]-[5] uses attribute based encryption but they lacks in providing efficient encryption and decryption time. Schemes it is thought to be a possible answer to the problem of fine-grained, safe, and secure data exchange as well as decentralised access. Cipher policy attribute based encryption (CP-ABE) is one of the most efficient cryptographic methods for providing fine-grained access control to cloud data, but it has shortcomings in key generation efficiency, scalability, attribute revocation flexibility, and access to a wide variety of attributes. Schemes [6]-[18] proposes schemes using CP-ABE but they do not support wide range of attributes. We present a novel key-cipher-policy (KCP) strategy, which combines the traditional CP-ABE and traditional KP-ABE approaches, to provide efficient encryption for secure access to multimedia data at cloud storage facilities. It makes key generation more efficient. Analyze the results for multimodal content such as text, image, audio, and video, compare them to existing schemes, and show that our technique is efficient.

2. RELATED WORK

An attribute-based encryption technique was presented by Boneh and Franklin [19] (ABE). This system adds an access policy to the ciphertext or for the key which is used for decryption instead of encrypting to specific users. Cryptography will make data access self-enforcing as a result of encryption. Waters proposed a CP-ABE method based on matrix structure [20]. The time required for encryption and decryption, as well as the sizes of the private key and ciphertext, rise linearly with the number of attributes.

Sangeetha and Karthik [21] proposed hybrid key-attribute based encryption. This paper will go over the access structure tree and also user attributes. This solves the shortcoming of KP-ABE while also shortening the time required for encryption and produce keys. This concept suits earlier procedures, however, it does not produce adequate results with modern systems. Huanh and Su put forth an identity-based access control solution for digital content on CP-ABE [22]. To share the digital files to several users, this method takes less storage space. This architecture works well when compared to a conventional access control list. This model includes minimum security features.

Vignesh [23] introduced a hybrid attribute-based encryption system that uses expressive policies with dynamic attributes for encryption of data. In his study, he blends attribute-based encryption ciphertext policy, symmetric AES encryption, and a location-based approach. This architecture provides location-based secure collaboration and can be used to provide end-to-end secure attribute-based communications and identity management.

3. KEY CIPHER POLICY BASED ABE

KP-ABE provides efficient ways of access control but it has less flexibility and scalability features. On the other hand CP-ABE provides efficient encryption and key generation but not efficient access control. We developed a model in which two ABE techniques, KP-ABE and CP-ABE, were merged to achieve secure and fine grained access control while also reducing the time required to generate a key and also encryption time. The model is known as key-cipher-policy-ABE [24]. There are four algorithms in key-cipher-policy ABE.

- Setup (P_{KC}, M_{KC}): Let us assume the bilinear group of the prime of order P is believed to be G_p . g bet on the G_p Generator. Consider the following: $G_i \times G_j \rightarrow G_p$ denotes a bilinear map, and K , a security parameter, denotes group size. It employs two hash functions: $H_{KC}: 0,1^* \rightarrow G_i$ and $H_{1KC}: G_j \rightarrow 0,1 \log p$. It makes public the parameter $Pk(e_{KC}, g, G_p, Y, T_{iKC} | i_u)$ and employs the master key Mk_{KC} as: $(y, t_i | i_u)$.
- key generation: It creates the private keys or users by executing $KeyGen(Mk_{KC}, Sk_{KC})$. This algorithm receives the message(M_{KC}) and the attributes sets (S_{KC}). These are considered to be the input and it outputs a secret key that holds attributes in S (set of attributes). Input: public key(Pk_{kc}), message (Mk_{KC}), attribute-associated access structure ($T_{a_{kc}}$).

It selects two input, and random exponents, $r_i \in \mathbb{Z}_p^*$ and $r_j \in \mathbb{Z}_p^*$ where r_i and r_j are unique secret keys to the user U_i and U_j respectively $\in S_{abe}$. then it provides the private key to the user.

$$Sk_{ut} = (Dk_c = g(\alpha + r_i)/\beta, \quad \forall \lambda_j \in Sk_c) \quad (1)$$

$$Dj_{kc} = g^{r_i} \cdot H'_{kc}(\lambda_j r_j) \quad (2)$$

- Data encryption: In the provided tree access structure, an encryption method is utilised to encrypt messages depending on the user attributes (T_{kc}). Let us refer to T_{kc} 's leaf nodes as K_{kc} . The data owner computes $S_{y_{kc}}=(e(g), H_{kc}(y))$ for all $y \in Y$ in the access tree's leaf node, and then computes $H1_{kc}(S_{y_{kc}})$.

The encryption process encrypts the message M using the tree access structure T_{KC} and user attributes. The process begins by selecting a polynomial $q_{x_{kc}}$ for each node in the tree T_{kc} , which includes leaves; every node in the tree is represented as x_{kc} . Beginning with the node assumed to be the root R_{KC} , polynomials are chosen using a top-down approach. Set the degree dx_{kc} of the polynomial $q_{x_{kc}}$ to be less than the threshold value of kx_{KC} . $dx_{KC} = kx_{KC}-1$ for each x_{KC} node in the tree starting with R_{KC} , the method chooses a random attribute set S , Zp , and sets $qR_{KC}(0) = S$. Then, to fully define the polynomial qR_{KC} , it randomly selects dR_{KC} and other points from qR , polynomial. For each other node x_{KC} , it sets $q_{x_{KC}}(0) = q_{KC}parent(x_{KC})(index)$.

$$CT_{kc} = T \tag{3}$$

$$C'_{kc} = Me(g, g') \text{ as } \tag{4}$$

$$C_{kc} = HskC, \forall y \in Y \tag{5}$$

$$C_{y_{KC}} = g \cdot q_{y_{KC}}(0) \tag{6}$$

$$C'_{y_{KC}} = HKC(att(y)) \cdot q_{y_{KC}}(0) \tag{7}$$

- Decryption: A recursive decryption process is used. The recursive algorithm first runs Decrypt (CT_{KC} , Sk_{KC} , x). It accepts ciphertext $CT_{KC} = (T_{KC}, C'_{KC}, C_{KC}, Y: C_{y_{KC}}, C'_{y_{KC}})$ and a private key Sk_{KC} which is associated with an attributes set S and a T_{KC} node x_{KC} as input. If node x_{KC} is regarded as a leafy node, then $i=att(x_{KC})$, and if $I \in S_{KC}$, then (8).

$$\begin{aligned} \text{Decrypt}(CT_{kc}, Sk_{kc}, x_{kc}) &= \frac{ekc(D_{kc}, C_{x_{kc}})}{eabe(D'_{kc}, C'_{x_{kc}})} \\ &= \frac{ekc(gr. Hkc(i)ri, hq_{x_{kc}}(0))}{ekc(gri, Hkc(i)q_{x_{kc}}(0))} \\ &= ekc(g, g).rq_{x_{kc}}(0) \dots \dots \dots \end{aligned} \tag{8}$$

4. RESULTS AND DISCUSSION

We employ a simulator in our study to implement key cipher policybased ABE. We compared the time required by our approach for key generation, encryption, and decryption to that of hybrid attribute based encryption (HABE) [25] and shown in Figure 1. The KC-ABE key generation time is not directly proportional to the number of at tributes as shown in Figure 1(a). The decryption algorithm is applied on a set of cipher texts for which encryption is done with policy tress of varying sizes produced at random. Beginning with root nodes, the trees are built by periodically linking the child to a randomly picked node till enough leaf nodes are generated. A random threshold was set for each internal node.

A key is picked consistently and randomly from the keys which are accessible and that fulfil the policy's parameters for each run. This is accomplished by iteratively considering attribute subsets random on the tree's leaves. The access tree influences decryption time. The number of attributes included in the private key determines the encryption time as shown in Figure 1(b). The number of attributes accessible also influences the length of time it takes to decrypt as in Figure 1(c).

We examine the algorithms' performance. Our PC configuration is an 11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz 1.38 GHz with 4 GB RAM and a 64-bit OS system. In simulation, we utilise a key size of 128 bits. Analysis of encryption time and decryption time for multimedia data is done as shown in Figure 2. For the text file as shown in Figure 2(a), It demonstrates that encryption exhibits a linear curve as the load grows, however decryption takes less time than encryption. The encryption and decryption times for image files increase approximately linear, and the approach works well for image files as shown in Figure 2(b). The encryption and decryption time curves for audio files in Figure 2(c) indicate that the encryption curve increases linearly with file size and decryption takes longer than the encryption time curves. The time required to encrypt and decrypt a video file increases linearly with the increase in file size as in Figure 2(d).

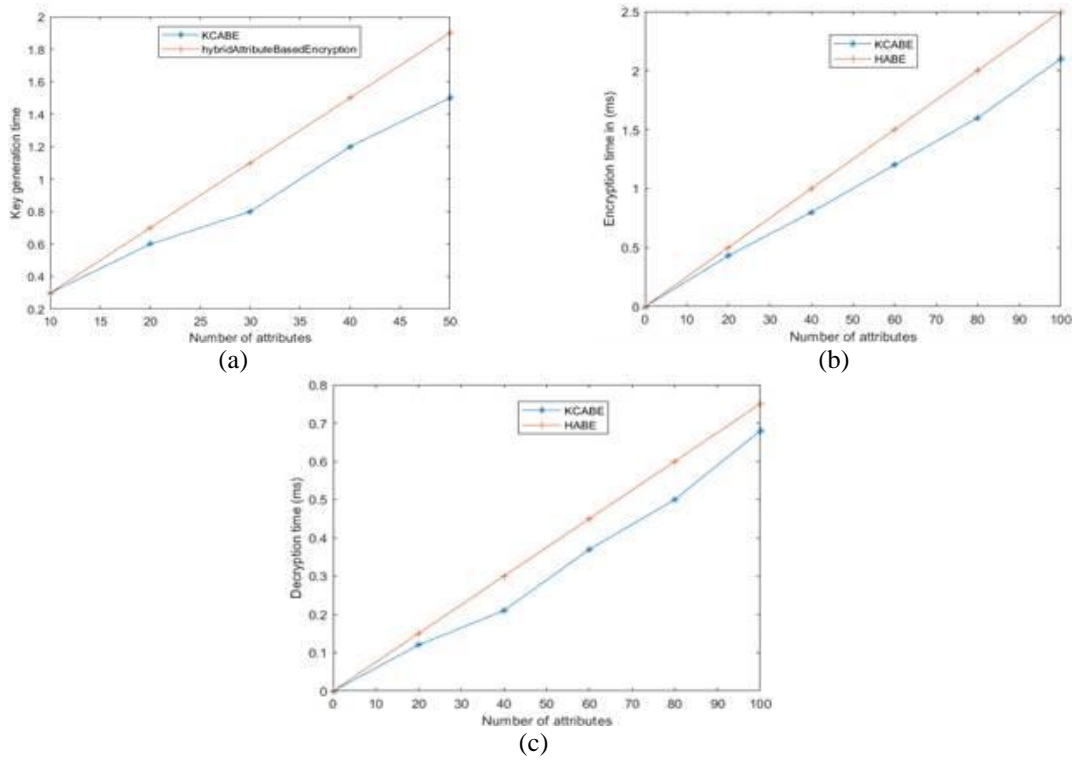


Figure 1. Comparison of performance of key-cipher-policy based ABE with respect with hybrid attribute based encryption: (a) key generation time, (b) encryption time, and (c) decryption time

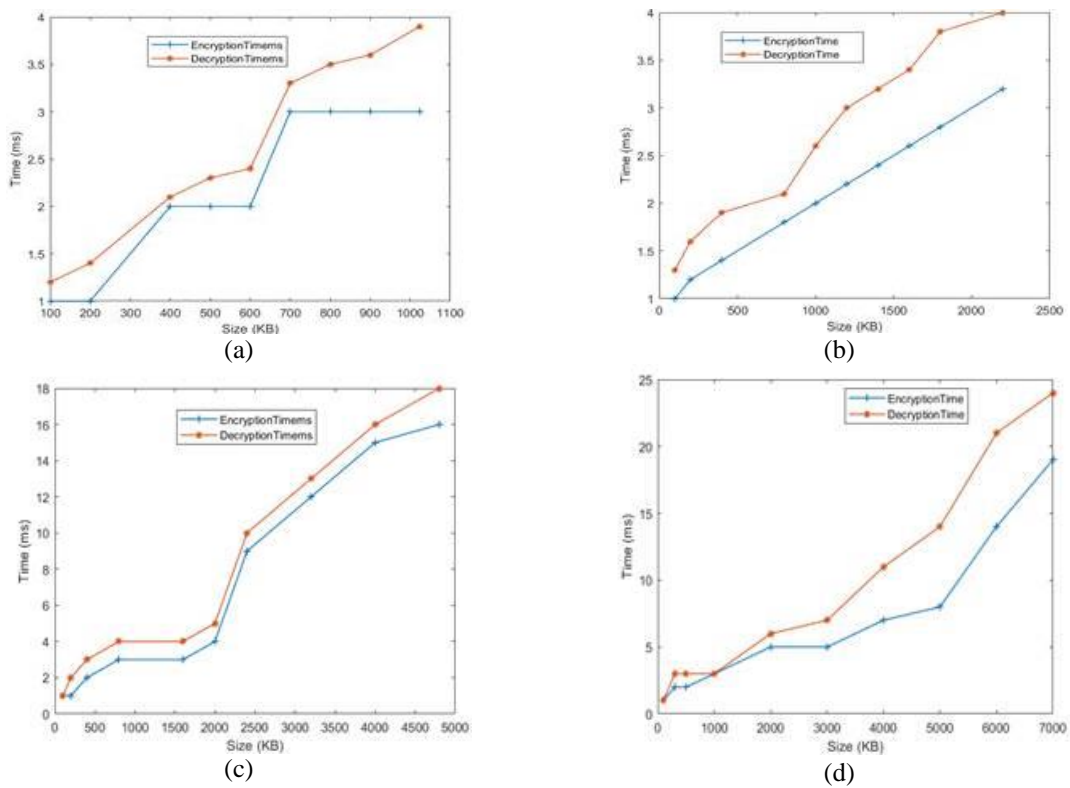


Figure 2. Analysis of encryption and decryption time for multimedia data: (a) encryption and decryption time for text file, (b) encryption and decryption time for image file, (c) encryption and decryption time for audio file, and (d) encryption and decryption time for video file

5. CONCLUSION

Our effort focused on the implementation and execution of the KCP algorithm. The scheme is applied, and the results are compared to similar procedures. It demonstrates that the new strategy outperforms the existing system. The encryption and decryption time with text, audio, image, and video data is also analysed and proven to be efficient. We can keep multimedia data private and confidential as compared to existing methods. We employed a hybrid technique in which the KP-ABE and CP-ABE algorithms were merged to allow secure and fine-grained access to multimedia content stored in cloud storage facilities. The suggested system's performance in terms of key generation time, encryption time, and decryption time is examined and shown to be efficient and secure. To address the limitations of flexibility and scalability, key-cipher policy-based ABE can be utilised for attribute revocation in the future.





REFERENCES

- [1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT '05)*, of *Lecture Notes in Computer Science*, vol. 3494, 2005, pp. 457–473, doi: 10.1007/11426639_27.
- [2] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proceedings of the Annual International Cryptology Conference (CRYPTO '01)*, of *Lecture Notes in Computer Science*, vol. 2139, 2001, pp. 213–229, doi: 10.1007/3-540-44647-8_13.
- [3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*, 2006, pp. 89–98, doi: 10.1145/1180405.1180418.
- [4] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, 2007, pp. 456–465, doi: 10.1145/1315245.1315302.
- [5] M. N. Ghuge and P. N. Chatur, "Collaborative key management in ciphertext policy attribute-based encryption for cloud," *Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018) IEEE Xplore Compliant - Part Number*, 2018, pp. 156–158, doi: 10.1109/ICICCT.2018.8473169.
- [6] N. Helil and K. Rahman, "CP-ABE access control scheme for sensitive data set constraint with hidden access policy and constraint policy," *Security and Communication Networks*, vol. 2017, p. 13, 2017, doi: 10.1155/2017/2713595.
- [7] K. Edemacu, B. Jang, and J. W. Kim, "CESCR: CP-ABE for efficient and secure sharing of data in collaborative ehealth with revocation and no dummy attribute," *PLOS ONE*, vol. 16, no. 5, p. e0250992, 2021, doi: 10.1371/journal.pone.0250992.
- [8] S. Wang, K. Liang, J. K. Liu, J. Chen, J. Yu, and W. Xie, "Attribute-based data sharing scheme revised in cloud computing," *IEEE Transactions of Information forensics and security*, vol. 11, no. 8, 2016, doi: 10.1109/TIFS.2016.2549004.
- [9] B. Waters "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," *In International workshop on public key cryptography*, Taormina, Italy, 6–9 March, pp. 53–70, 2011, doi: 10.1007/978-3-642-19379-8_4.
- [10] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT '05)*, vol. 3494, 2005, pp. 457–473, Springer, doi: 10.1007/11426639_27.
- [11] K. Xue, W. Chen, W. Li, J. Hong, and P. Hong, "Combining data owner-side and cloud-side access control for encrypted cloud storage," *IEEE Transactions on Information Forensics And Security*, vol. 13, no. 8, 2018, doi: 10.1109/TIFS.2018.2809679.
- [12] P. P. Kumar, P. S. Kumar, and P. J. A. Alphonse, "An efficient ciphertext policy attribute based encryption for big data access control in cloud computing," *Ninth International Conference on Advanced Computing (ICoAC)*, pp. 114–120, 2017, doi: 10.1109/ICoAC.2017.8441507.
- [13] J. Lai, R. H. Deng, and Y. Li, "Fully secure ciphertext-policy hiding CP-ABE," in *Proceedings of the International Conference on Information Security Practice and Experience*, pp. 24–39, Springer, Berlin, Germany, 2011.
- [14] L. Sun and C. Xu, "Hidden policy ciphertext-policy attribute-based encryption with conjunctive keyword search," 3rd *IEEE International Conference on Computer and Communications*, 2017, pp. 1439–1443, doi: 10.1109/CompComm.2017.8322780.
- [15] D. Amesh and R. Priya, "Multiauthority scheme based CPABE with attribute revocation for cloud data storage," *International Conference on Microelectronics, Computing and Communications, IEEE (MicroCom)*, 2016, pp. 1–4, doi: 10.1109/MicroCom.2016.7522518.
- [16] G. S. Tamizharasi, B. Balamurugan, and H. A. Gaffar, "Privacy preserving ciphertext policy attribute based encryption scheme with efficient and constant ciphertextsize," *IEEE, International Conference on Inventive Computation Technologies (ICICT)*, vol. 3, 2016, pp. 1–5, doi: 10.1109/INVENTIVE.2016.7830099.
- [17] U. C. Yadav, "Ciphertext-policy attribute-based encryption with hiding access structure," *IEEE International Advance Computing Conference (IACC)*, pp. 6–10, 2015, doi: 10.1109/IADCC.2015.7154664.
- [18] W.-B. Huang and W.-T. Su, "Identity based access control for digital content based on ciphertext-policy attribute-based encryption," *International Conference on Information Networking (ICOIN)*, 2015, pp. 87–91.
- [19] D. Boneh, and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proceedings of the Annual International Cryptology Conference (CRYPTO '01)*, vol. 2139, pp. 213–229, 2001, doi: 10.1007/3-540-44647-8_13.
- [20] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *proc 14th Int. Conf. Theory Public Key Cryptography Conf. Theory Cryptograph*, 2012, pp. 53–70, doi: 10.1007/978-3-642-19379-8_4.
- [21] M. Sangeetha and P. V. Karthik, "To provide a secured access control using combined hybrid key-ciphertext attribute-based encryption (KC-ABE)," *International Conference on Intelligent Techniques in Control, Optimization and Signal Processing*. IEEE, 2017, pp. 1–4, doi: 10.1109/ITCOSP.2017.8303116.
- [22] W.-B. Huanh and W.-T. Su, "Identity-based access control for digital content based on ciphertext-policy attribute-based encryption," *International Conference on Information Networking (ICOIN)* 2015, pp. 87–91.
- [23] M. Vignesh, "Exploration of attribute based encryption schemes on cloud computing," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 5, 2020, doi: 10.35940/ijrte.E6764.018520.





- [24] M. N. Kavyasri and B. Ramesh, "Key-Cipher-Policy based ABE with efficient encryption of multimedia data at data centers of cloud," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 11, no. 1, pp. 73–76, May 2022, doi: 10.35940/ijrte.c6486.0511122.
- [25] Y. Xie, H. Wen, B. Wu, Y. Jiang, and J. Meng, "A modified hierarchical attribute-based encryption access control method for mobile cloud computing," *IEEE Transactions on Cloud Computing*, vol. 7, no. 2, 2019, doi: 10.1109/TCC.2015.2513388.

BIOGRAPHIES OF AUTHORS



Kavyasri Madakaripura Nagaraju     is currently working Assistant Professor in the Department of Computer Science and Engineering, Malnad College of Engineering, Hassan. She is currently pursuing her research in Cloud Computing. Her major area of research includes Cloud Computing, soft Computing, Computer Networks. She has presented ten papers in the international journals and conferences. She can be contacted at email: kavyasrimn88@gmail.com.



Dr. Ramesh Boraiah     is currently working as Professor in the Department of Computer Science and Engineering, Malnad College of Engineering, Hassan. He Received his Ph.D. degree in Mobile Adhoc Networks from Computer Science and Engineering from Anna University, Tamilnadu. His research interests include computer networks, multimedia computing, mobile AdHoc networks, cloud computing and network security. He is been awarded as the Best Citizens of India Award 2013 from he international Publishing House. He can be contacted at email: sanchara@gmail.com.