International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-8, June 2020

Access Control Based on Different User Privileges in Social Media

Alina K Jayarajan, Eldo P Elias

Abstract: ***The emergence of social media lead to people around the world is widely using it. There are varieties of applications under this category for diverse purposes. Day by day, the security concerns related to this area is increasing since it is a medium which connect people. At present, the single access policy is present. That is whether a user can access the media content or not. Hence multi access policy can provide more user satisfaction. On the other hand video and image can be encoded into different qualities. Ciphertext Policy Attribute-Based Encryption is used for encrypting keys used in symmetric encryption. Here introducing Linear Secret Sharing Scheme (LSSS) to the scalable social media stream security. The LSSS mechanism is adopted to increase the expressiveness of the monotone access structure. By utilizing an LSS Scheme the access structure becomes more protective. This algorithm is very useful in practice as a ciphertext policy can now be intuitively expressed using a monotone Boolean formula, which has good usability, and the corresponding LSSS for an actual CP-ABE construction can then be generated accordingly using this algorithm.***

Keywords: CP-ABE, LSSS, Media layers, Access structure .

I. INTRODUCTION

Now it is easier to share images and videos through the social media with friends, relatives and colleagues. But content propagation can even be extended to public. Some of the users are showcasing their everyday life to public. Most of the population with contrasting intentions comes together in different social media. So people without knowing proper security mechanisms involved become target to the social media hackers. Social media creators also need to ensure the protection of user data. For this new security mechanisms should be continuously evolved to withstand against modern threats in internet. So it is also necessary to media content up-loader must be aware of the uploaded media that whether it may lead to any security problems. That is any crucial information that may disclosed to unauthorized persons. The media content generator used creates an access control mechanism to restrict the data which is sharing. Hence setting the access privileges enhance the sharing the data with distant layers of security. The protection of data shared in social media is required. So the privacy related problems to be addressed [1].

Revised Manuscript Received on June 30, 2020.
***** Correspondence Author
Alina K Jayarajan*, Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam, Kerala, India.
Eldo P Elias, Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam, Kerala, India.

The information distributed by sender is used by others and they re-share them like theirs and sometime make modifications also. Then when visual data is seen by unauthorized users, they will get some personal information of person who posted [2]. So it may affect a person in virtual and real world as well. There are different methods in artificial intelligence, machine learning and other emerging fields which can mine lot of information from video and image [3]. Hence security in social media should be preserved necessarily and it is one of the major domain to be considered. Posting of images in dark shades and cropping the image to remove sensitive information are done by users [4]. But all these won't solve the issues. Different people have distinct motives while using social media. Sometimes even their profiles are not true. One condition whether the user can access the posted media data can't preserve intention or motive behind social media. In social media different levels of assorted and tangled association between people is existent and flow of information shared by one person through this levels. So conventional access policy to data access is against for the foundation of social media. Actually social media paves for new way of income to lots of people. Marketing, advertising, personal branding, selling, buying etc. occur through this virtual world by less expense of time, energy and money. So this innovation in technology has greater impact on people. The media content which is posted by users on the social media platform contains a lot of private details. When that confidential information reaches the wrong hands, it leads to problems. So it is necessary to provide access control to information based on the attributes possessed by the users. Those attributes also need to be authenticated. The attributes may be courses such as BTech, BSc, MTech, etc, specialization such as computer science and engineering (CSE), information technology (IT), electronics and electrical engineering (EEE), etc. Then form a boolean form An example is (BTech OR MTech) AND CSE. The AND gate becomes root and attributes are at leaf nodes in case of forming an access tree structure. This authorization of attributes is done at the social media server. Hence different users get media content with different quality. The low-quality media content can be widely populated and can give access to all users. So the privacy of contents posted in social media is ensured. This scheme also provides a way for revocation, change and adding of attributes.

A scalable media access control scheme can preserve the principles of social media [5]. The image and video can be encoded into different qualities ranging from higher to lower. Between them different medium qualities also present. Various compression techniques are existing and utilize any of them to get different qualities. So the user with higher access privilege which is decided by media distributor will get original or best quality media content. Then users who lower access privilege will poor quality media content. Or else low-set quality media content can be extensively distributed in social media [6]. Low-set quality content is non-compliant to various machine learning and artificial intelligence techniques to extract information from image and video [7]. Then fraudulent users are not interested to post poor quality images with missing content as theirs [8]. Hence based on different qualities of image or video, the content generator can generate access control with many levels of privileges. The scalable ciphertext policy attribute-based encryption is used to encrypt the symmetric key used in the Advanced Encryption Standard (AES) algorithm. The different streams of media with variety of qualities can be encrypted using AES algorithm. The keys are different to encrypt each distinct quality media stream. The authentication based on the attributes users can be done using attribute based encryption. Then there is need to ensure various levels of privileges. So the media consumers will receive the keys to decrypt the media stream based on their access privilege. The access key is distributed to the users and cancelled based on changes in their attributes possessed by them. The access structure is formed at the content distributor. It is developed on the basis of people who can access the video or image. The access structure is updated by distributor periodically. It is stored on the social media server. The authentication of attributes and distribution of keys are done at server side.

By handling a LSS Scheme the access structure becomes more protective. A secret-sharing scheme is an approach by which a distributor distributes shares to parties such that only legitimate subsets of parties can reorganize the secret. Linear Secret Sharing Scheme (LSSS) matrices are frequently adopted for operating monotone access structures in highly expressive Cipher text Policy Attribute-Based Encryption (CPABE) schemes. By contrast, LSSS matrices are much lower perceptive to handle when compared with other mechanisms such as Boolean formulas or access trees. To reduce the distance between the practicability of an access structure depiction method and the construction mechanism needed in a concrete CP-ABE construction, Lewko and Waters proposed an algorithm which can convert any monotone Boolean formulas to LSSS matrices. This algorithm is very useful in practice as a cipher text policy can now be intuitively expressed using a monotone Boolean formula, which has good usability, and the corresponding LSSS for an actual CP-ABE construction can then be generated accordingly using this algorithm.

II. RELATED WORK

For preserving the privacy in social media for sharing especially video and audio, many techniques are adopted related to ABE and scalable media format.

A. Scalable Media

The media stream is encoded into various layers. One is fundamental layer which has minimum quality. There are other higher layers above them which have varying degree of qualities. So that lowest layer consists of fewer signals to noise ratio, frame rate, color, resolution etc. [9]. In dimensions the qualities are shown varying on these factors. So it is possible to construct two dimensional, three dimensional or even higher depending upon number of quality parameters. Hence leading layer is send to users maintaining higher access privileges. Fig. 1 shows the scalable media varying in terms of resolution, SNR and frame rate. In two dimensional structures, there are two factors determining quality. M values for one factor and N values for another factor is considered. Then M+N-1 access levels are existing for users. If the media layer is written as m_ij. Then layer with largest i and j have highest media quality content. By considering two layers m_ij and m_pq where i+j = p+q implies that access privilege is same for these layers. The access privileges to different media layers are shown in Fig. 2.

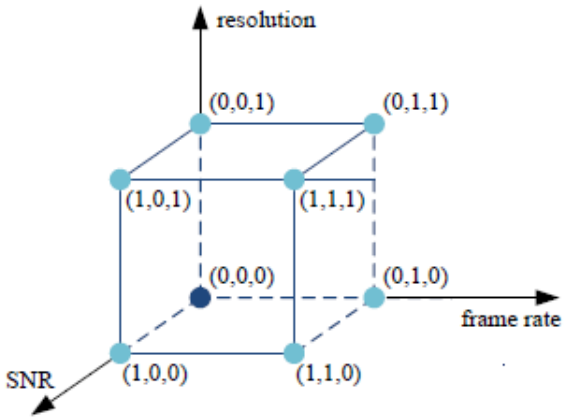

Fig. 1. Scalable Media.

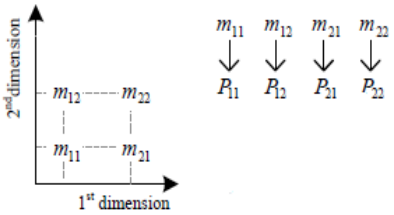

Fig. 2. Access Policies.

B. Architecture

There are three different parties exist in the scenario. So the detailed description of their duties are shown in this section. The media distributor shares video or image in the social media. It is then received by media consumers [5]. The relationship between media distributor and media consumers are varying from strong to weak. The relationship can be friend, friend of friends, no one etc. Usually who can view the media is mentioned by everyone, friends, friends of friends etc. Or it can be social circle such as relatives, school mates, colleagues at work place etc.

In SCP-ABE, attributes such as name of college, place, department in case of college as an scenario.

Here the distributor decides who can view the media content based on the attributes. Hence the users with specific attributes can access media with particular quality. The high quality media content is accessed by people with high access privilege. The access structure in the form of tree is created based on the attributes. The system architecture is shown in Fig. 3.

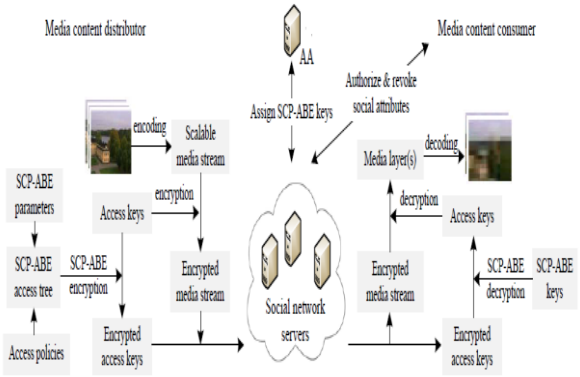

Fig. 3. System Architecture.

The attributes are authenticated by the social media server and attribute authority combined. The media content in the form of ciphertext is stored at server. Because the content distributor not trust the server. So the server cannot directly decrypt it. Then the consumers get key to decrypt the symmetric key used in the media encryption. Thus after decryption, the consumer can view a specific quality according to access privilege. Then ciphertext of symmetric keys are stored in server.

C. SCP-ABE Algorithm

The SCP-ABE algorithm is established on the CP-ABE algorithm. For CP-ABE, input is encrypted based on access policy that is comprised of attributes. The user can decrypt the ciphertext exclusively its attributes satisfy the access policy. Using a similar mechanism, the SCP-ABE algorithm place priority on masterly encrypting multiple dimensional data. In specific, SCP-ABE made up of six algorithms consisting of setup, access tree composition, encryption, SCP-ABE key creation, legation, and decryption [10]. The bilinear map is used as a preliminary in the establishment of this algorithm. Bilinear map satisfies two properties such as bilinearity and non-degeneracy. In the setup phase, the public key and master key are generated using the bilinear group. All users in the system can access the public key. Only attribute authority can access the master key. Then the access tree is constructed based on various access rights. Here the access policy is mentioned in terms of attributes. Whether the attribute is present or not. The media distributor is creating the access tree. The attributes which are used for construction must be verified by the social network server. The access structure changes when there is need to update the access rights to media shared. Then next is encryption, where the data is encrypted using the public key. For key generation, set of attributes and master key are given as inputs and outputs the secret key. In delegation, when attribute set and secret key are given as input. It outputs a secret key for a subset of attributes. To get the data back to plaintext, it should be decrypted. For decryption, it utilizes secret key and public key. Then decrypt the ciphertext of the data layer. So decryption contingent on attributes that determine access policies.

D. AES Algorithm

The Advanced Encryption Standard (AES) is the symmetric encryption algorithm. The number of rounds is fluctuating based on the length of the key. The key size should be larger to enhance security. Each round involves four processes such as byte substitution, shift rows, mix columns and add round key. In decryption, these processes take place in reverse order. This algorithm is adapted to images as well as videos. AES encryption is more secure than DES (Data Encryption Standard) and triple DES. Then it is also efficient for encrypting bulk volume of social media data mainly comprising of images and video.

The video and image should be encoded into different qualities using different compression techniques. After the encoding of image or video, encrypted using AES algorithm. The key used for encrypting image in AES is encrypted SCP-ABE algorithm [11]. SCP-ABE algorithm is the asymmetric cryptographic algorithm. Here is the combination of symmetric and asymmetric cryptography.

E. Access Privilege Permission

An efficient key management scheme is used to authenticate the attributes of users of the system [12]. Then it can also authorize and cancel the access privilege when the attributes of the user are changed. The realization of SCP-ABE is made by providing the media consumers with access key depending on attributes possessed by them. It is also necessary that not share the social attributes of users with the third party. To keep the social attributes in secret, share the hash values of attributes with attribute authority. To avoid brute force attacks, share one or more secret values by social network server and users. When the attributes of an media consumer changes or the access structure created consumer are updated, then key revocation will take place. When college transfer is given to a student, then the attributes changes. It should detected firstly by social network server and inform it to the social media distributor. So to ensure privacy, the distributor changes the key and encrypt it for that specific consumer. When there is need to update the access structure, then the SCP-ABE keys of all users are changed. Then the former keys are cancelled and distribute new keys.

III. PROPOSED METHODOLOGY

The access structure construction is modified to enhance the security of the system. It represents different access privileges in a single tree. Firstly, attributes of high access privilege users are given at first. As parse from top to bottom of the tree, then the quality received by the users decreases. Hence the lowest layer consists of attributes of the user who has access to the low-quality media content.

This is to generate the LSSS matrix from an access tree structure which can amplify the expressiveness of policies used in access mechanism to media content [13].

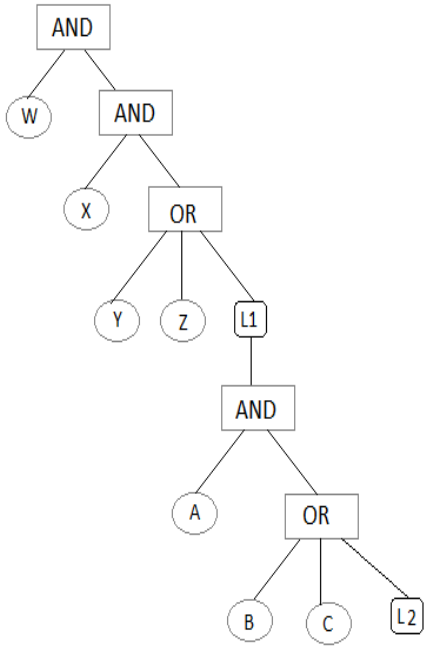

Fig. 4. Access Structure

The tree structure consists of both non-leaf and leaf nodes. Attributes are placed in leaf nodes while threshold gates are placed at non-leaf nodes. The quality of media mentioning attributes is placed at non-leaf nodes or leaf nodes. These attributes are called quality attributes denoted by L1 and L2 in Fig. 4. The highest quality is given at first quality attribute L1 in the tree. Here the lowest quality attribute is at the leaf node which is the last node in the tree. The attributes of media content consumers and quality attributes are represented in different shapes. The boolean formula comprises W AND X AND (Y OR Z) is described at the top of the tree which accesses the quality L1. So the users having attributes W, X, Y or W, X, Z can access the highest quality video or image content. The boolean formula containing A AND (B OR C) can access the media quality L2. So the consumers having attributes A, B or A, C can access low quality L2 as per this access structure Fig. 4. The access tree is scalable, we can add any number access boolean formula to this according to the requirement.

The input to the LSSS matrix is an access tree representing boolean formula that should be monotone access structure. The AND and OR gates are placed at non-leaf nodes. The algorithm provides output as a matrix [14]. The number of leaf nodes representing the attributes of consumers becomes equal to the number of rows in the LSSS matrix. Initialize count c equal to 1 and vector equal to 1 for root node AND gate. When the non-leaf node is AND gate with vector v, then the right child becomes vector v concatenated with 1. The left child 0 concatenated with -1. Here the number of 0 is equal to c. After that increment the value of c by 1. In the case of the OR gate, no need to change the value of v. Thus give the same vector to both left and right child. The counter remains unchanged.

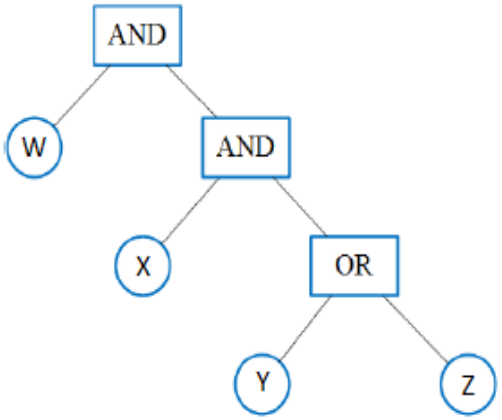

Fig. 5. Access Tree.

Then Fig. 5 shows the access tree for the boolean structure of consumers with high access privileges. Their boolean formula W AND X AND (Y OR Z) is represented here. That access tree is labeled according to the above-mentioned algorithm in Fig. 6 to get the output as the LSSS matrix. Each media consumer has access to one media layer. That is there is no access to the different qualities of image or video even though the user has higher access privilege. For each boolean structure in the access, the tree creates a different LSSS matrix.

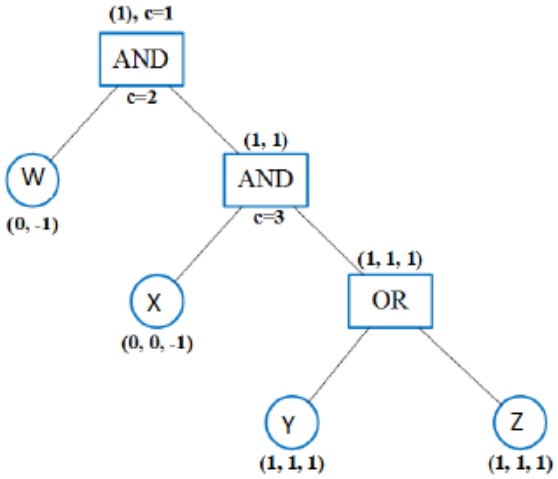

Fig. 6. Label the Access Tree.

In our example, the first boolean formula in the access structure is used. The vector formed at each attribute is placed in the row one after another. If the size of the vector is smaller, then pad with zeros to make all the rows have equal length. So the first row represents the vector of attribute W and so on.

The LSSS matrix is shown in fig. 7 with four rows for attributes W, X, Y, and Z. To find whether the attributes specified in a set satisfies the LSSS matrix when the rows of given attributes in the LSSS matrix contain (1, 0, 0, 0,..., 0) in their span. Fig. 8 shows how to calculate the span of attributes such as W, X, and Z. The V_1, V_2 and V_3 represents the vectors of given attributes of consumers such as W, X, and Z. Then C_1, C_2 and C_3 are some constants which can be arbitrarily chosen for the attributes.

Using the equation and solving it given in fig. 8. provides the output (1, 0, 0) which satisfies the condition. Hence the media consumers possessing the attributes W, X, and Z can access the high-quality media layer which is represented by quality attribute L1.

$$A = \begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \begin{matrix} \rho(1) = W \\ \rho(2) = X \\ \rho(3) = Y \\ \rho(4) = Z \end{matrix}$$

Fig. 7. LSSS Matrix.

$$C_1 V_1 + C_2 V_2 + C_3 V_3$$

$$= 1 \begin{bmatrix} 0 \\ -1 \\ 0 \end{bmatrix} + 1 \begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix} + 1 \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

Fig. 8. Span of LSSS Matrix.

IV. RESULT AND PERFORMANCE ANALYSIS

The performance of the system is evaluated in terms of security and efficiency. The security ensures the media is received to right people with authorized attributes. The efficiency is necessary to optimize the use of resources in practical applications.

A. Security Analysis

There are two measures to demonstrate the security of the system. That is security and reliability of access rights permission. Hence the decryption occurs only if the user gets corresponding access key and the consumers with specific attributes or access rights will get a corresponding access key [15].

The single access structure consists of different access rights for users. It consists of multiple access privileges. So the users with attributes are verified from the access structure and can decrypt media content if it matches with attributes specified by the media distributor. It follows the security of the SCP-ABE algorithm. It actually utilizes elliptic curve groups and cryptographic hash functions. LSSS is used to define and implement access rights. It also decreases overhead created by expressing access permissions.

The access permission of media server and consumers are reliable. The users with specific attributes attain the corresponding SCP-ABE key. The consumers cannot collude to obtain the media content which is not reserved for them. The SCP-ABE key revocation mechanism can deal with changes in the attributes of users. The new attributes of a user can be authorized and regenerate the access keys for them. Then also prevent the social media server from accessing media content [16].

B. Efficiency Analysis

The efficiency of the system can be estimated from the cost of access policy permission and its authorization. The implementation of operations is done on Lenovo G50 with Intel(R) Core(TM) i3-4030U CPU @ 1.90GHz CPU. The cost for system originate from the AES algorithm for media content and SCP-ABE algorithm for symmetric keys [17]. The cost of encryption of video is much larger than the SCP-ABE algorithm. Hence the cost of SCP-ABE encryption is negligible. Then during the evaluation, the cost of the SCP-ABE algorithm enhances when the number of attributes is larger. The server-side cost increases with a number of media consumers. Fig. 9 shows the computation time occurs when the attributes increase. In the case of the LSSS scheme, the computation overhead increases with the number of attributes. It can express the monotone access structure efficiently

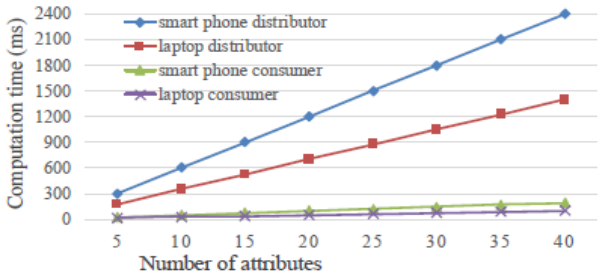

Fig. 9. Time vs Number of Attributes.

V. CONCLUSION

The proposed features in social media security systems enhance the privacy of images or videos shared on social media. The integrity, confidentiality, and availability of information shared in the modern platform are ensured. The access level policy is strictly enforced by media content distributor which decides who can access media content. So the content cannot be obtained by unauthorized persons. The tree access structure is modified. It inflates the parsing through attributes. There are different levels of access permissions are represented in the tree. Then the tree structure is given as input to the LSSS algorithm. The LSSS mechanism is adopted to increase the expressiveness of the monotone access structure. Then by using LSSS, attain smaller ciphertext. Hence LSSS accomplish different access control restrictions created by media content distributor. Each user has access to one of the quality in media content or no access. In some cases, low-quality media content can be widely propagated among all the users in the platform. The security and reliability of the system are analyzed and it is efficient in practical applications.

REFERENCES

1. M. Fire, R. Goldschmidt and Y. Elovici, “Online Social Networks: Threats and Solutions," IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 2019-2036, 2014.
2. L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, A. V. Vasilakos, “Security and privacy for storage and computation in cloud computing," Information Sciences: an International Journal, 258, p.371-386, 2014.

3. R. Shokri, V. Shmatikov, “Privacy-Preserving Deep Learning," Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 1310-1321, 2015.
4. M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, “Deep Learning with Differential Privacy," CCS, pp. 308- 318, 2016.
5. Changsha Ma, Zhisheng Yan and Chang Wen Chen, "Scalable Access Control For Privacy-Aware Media Sharing", IEEE Transactions on Multimedia, 2018.
6. C. K. Mick, R. R. Shea, K. P. Grundy, J. C. Fjelstad, “Method and apparatus for protecting digital rights of copyright holders of publicly distributed multimedia files," U.S. Patent 20080247543 A1, Oct 9, 2008.
7. , S. Dodge and L. Karam, “Understanding How Image Quality Affects Deep Neural Networks," arXiv preprint, arXiv:1604.04004, 2016.
8. S. Karahan, M. Kilinc Yildirum, K. Kirtac, F. S. Rende, G. Butun and H. K. Ekenel, “How Image Degradations Affect Deep CNN-Based Face Recognition?" 2016 International Conference of the Biometrics Special Interest Group (BIOSIG), pp. 1-5, 2016.
9. H. Schwarz, D. Marpe and T. Wiegand, “Overview of the Scalable Video Coding Extension of the H.264/AVC Standard," IEEE Trans. Circuits and Syst. Video Technol., vol.17, no.9, pp.1103-1120, 2007
10. Bethencourt, J.; Sahai, A.; Waters, B., “Ciphertext-Policy Attribute-Based Encryption," IEEE Symposium on Security and Privacy, pp. 321-334, 2007.
11. Jun Zhou et al, “4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks," Inf. Sci. 314: 255-276, 2015.
12. Zheng Yan, et al, “Two Schemes of Privacy-Preserving Trust Evaluation," Future Generation Comp. Syst. 62: 175-189, 2016.
13. A. Beimel, ``Secure schemes for secret sharing and key distribution," Fac. Comput. Sci., Technion-Israel Inst. Technol., Haifa, Israel, 1996
14. A. Lewko and B. Waters, ``Decentralizing attribute-based encryption," in Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Adv. Cryptol.-EUROCRYPT, Tallinn, Estonia, 2011, pp. 568588.
15. S. Canard, J. Devigne, and O. Sanders, ``Delegating a pairing can be both secure and efcient," in Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.,Springer, 2014, pp. 549.565.
16. B. Preneel, “Cryptographic hash functions," European Trans. Telecom.,5 (1994), pp. 431-448, 1994.
17. D. M. Dumbere and N. J. Janwe, “Video encryption using AES algorithm," Second International Conference on Current Trends In Engineering and Technology (ICCTET), pp. 332-337, 2014.

AUTHORS PROFILE

Alina K Jayarajan received Bachelor of Technology in Information Technology from Government Engineering College Idukki in 2017 and currently pursuing Master of Technology in Computer Science and Engineering from Mar Athanasius College of Engineering, Kothamangalam affiliated to APJ Abdul Kalam Technological University. Her research interest is in Computer Networks and Cryptography.

Prof. Eldo P Elias is currently working as assistant professor in the Department of Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam, Kerala, India. He received B-Tech Degree in Computer Science and Engineering in 2003 from Bharathiar University, Coimbatore and M-Tech in Computer and Information Sciences from Cochin University of Science and Technology, Kochi in 2013. He has around 14 years of teaching and research experience in various institutions in India. His research interests include Computer Security, Computer Architecture, Operating Systems and Data Science