Real-Time Image Privacy Preservation using AES with Salt key and Gaussian Blur Algorithms with the application of Data Perturbation in Cloud

S. Sambath Kumar, S. Devi

Abstract*: Rapid increase in image data produced by individuals and companies provoke privacy hitches such as unauthorized revelation of personal data and person's individuality stealing, but it can be used to protect privacy of the user and also personal information. Data provider and Cloud Administrator are two types of users who have privilege and access. However, there is absence of research examining the effectiveness of implementing techniques to images as a technology that protects privacy. The Advanced Encryption Standard (AES) algorithm is selected for the login authentication process, which ensures the protection of information from unauthorized access and is proposed to create a random key generation. Data perturbation is used to add noise in databases, and Gaussian blur is done to introduce some degree of degradation in the original image. The obtained test results show that an AES with salt key can be randomly generated. In this process, security authentication is reinforced in the ciphertext changes that make up the key words for each encryption process. The result shows that the model is relatively fast with a time average of 0.034 s occupying less than 100kB of memory space.

Keywords* : *Lung Cancer Detection, CT Scan Image, Cancer, Image Processing.

I. INTRODUCTION

Cloud computing combines conventional computing and networking approaches altogether in order to execute a specific task. Due to advancement in technologies, service providers and users are going towards the cloud. Today different enterprises are using their own cloud services to the end users for the purpose of providing network connection and availability of superior services. Although cloud computing has more advantages than conventional storage mechanisms; security concern is an obstacle for choosing it. Lot of research work has been executed in this area. Cloud infrastructure has two modes one is public and the other is private. Personal mode provides services to smaller group of people and is dedicated to a company hosted. And it has minimized security issues. Public mode is hosted by the cloud provider where the security is an important issue. With the emergence of technologies, many companies have invested in cloud and large users located at various geographical areas share data at high speeds. But the cloud environment has security compromises in its system performance, reliability and security. Privacy issues usually arise in online social networks (OSNs), where the individual's information can be scrutinized from their own images [1, 2, 3]. The outsourcing of computing image feature extraction by data providers to cloud discloses the owner's data namely personal, locality, financial status and also sensitive data. The attacker can subtract the content of the from the benchmark image and there is a possibility to retrieve a portion of the image. From the survey, it was found that no previous studies have examined the performance of perturbing digital database particularly image data. A usual way to protect content of the image is to blur a owner's faces in an image [1, 4 5, 6, 7] so that the identity of the person is protected even if the image is shared with unwanted viewers [1]. Various characters such as objects in the image, the background structure [9, 10] in an image discloses owner's information other than identity. One of the broadly used method to protect important content in an image is to soften it and degrade using Gaussian blur [8, 11]. Current approaches are insufficient to ensure image data security, especially for end users. Our goal is to examine the effectiveness of AES with salt, perturbation and blurring as a means of protecting privacy against human recognition.

II. LITERATURE REVIEW

A novel visual cryptography scheme [12] shares two binary confidential images of two rectangular stock images with no pixel expansion. The main challenge to overcome it is about data security in a distributed environment. The idea is to create a database that protects privacy, such as updating data sharing functions, restricting access and sharing of data, and delivering data to a central company, thus supporting database sharing and proprietary data. Data confidentiality is achieved by keeping compatible relationships in a distributed environment. Portable capability can be combined with cloud computing services to provide secured services to customers. Also, privacy [13] is a major concern in collective ubiquitous computing, as it may prevent data sharing about a wide variety of data. Security Multiparty Accounting Algorithm that allows the client to register using encrypted identifiers [14].

Revised Manuscript Received on January 5, 2020

***** Correspondence Author

S. Sambath Kumar*, Department of Computer Science and Engineering, PRIST Deemed to be University, Thanjavur, India. Email: ssampathk8@gmail.com

S.Devi, Deparment of Electronics and Communication Engineering, PRIST Deemed to be University, Thanjavur, India. Email:devi.bharath@gmail.com

The protocol is more practical than previous secure enrollment models in data access requirements for communicating with third parties. Although certainly possible, the basic mechanism of the number of records is the speed of measurement. This method introduced an additional version of the proposed protocol, in which data holders incorporate Q-anonymous features of their client into their encrypted data submissions. These characteristics facilitate highly efficient enrollment and support the proper protection of the fact that every company is less affiliated with gay men in the union of all executive consumers. Beyond a hypothetical measure of the problem, the method provides a broad test score. Privacy-Protecting Algorithm [15], [16] to securely integrate personal data from different data providers. Two information-based authentication and transfer programs [17] are used to protect health information sharing and privacy in health social networks (HSN). HSN users are labeled with decent dignified attributes and it aids more efficient computation, supporting a proper security that each record is connected to not less than k individuals in the union of all administration consumers. OSNs [19] have accelerated the emergence of large amounts of personal information on the Internet. The attribute-based exchange program allows an HSN user to hide health information in a web text associated with a personalized access policy which is defined by the target properties. Users who meet the access policy only can encrypt web text. Two attribute-based authentication and transfer programs effectively address pseudo-attack, attribute-trace attack, alert attack, and joint attack through security analysis. The concern of usage limit refers to restricting data after publication. The widespread growth in the number of users engaging in sharing contents, data publishing is becoming an increasingly important issue. This problem is best solved by providing a reliable hardware environment for each user, but unfortunately its cost is high. OSN [18], [21] have found difficulties in using a particular context and specific image sharing. In previous OSNs, the owner of the uploaded image could access the content, but other users with the same content could not set the fate. DECENT, [20] is a framework for OSNs that utilizes hash tables to accumulate data of the user, and includes cryptographic safeguards for prudence and integrity along with rapid recovery. DECENT makes that data / social associations are not available to fraudulent users for their copying and verifying it. Separate social networking content makes that OSNs [22] provide which decoupling users control with their own social information only have access to a third party. Geo-Aware Social Networks [23] impose privacy concerns beyond location-based services. Content published on it is associated frequently with citations to multiple users without the awareness of the publisher about the privacy of those users.

III. METHODOLOGY

This section gives the methodology used in the proposed system for the real-time image privacy preservation using AES Algorithm with salt and gaussian blur algorithm with the application of data perturbation in cloud based environment. Figure 1 shows the **b**lock diagram showing application of the above three techniques in privacy preservation of image data.

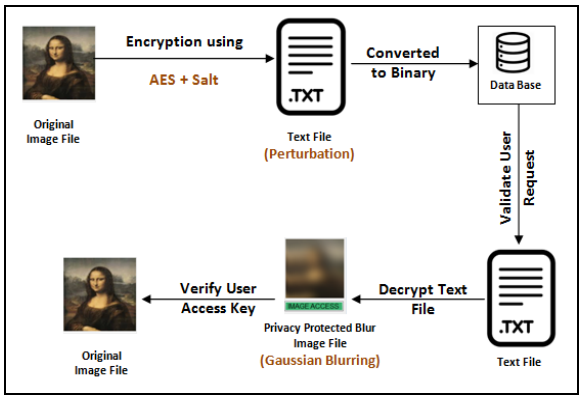


Figure 1. Block Diagram of proposed system in Privacy Preservation of image data

A. Data Perturbation

Organizations store huge data, most of which are personal or confidential data and those data must be secured from illegal parties and also from those who are having permission to access it. The interest in this concern is relating to control access to private database to authenticate legal users. Data perturbation protects private data with random noise added in cryptographic properties of plaintext thereby allowing legal users to access important statistical attributes from the database. This protects the unique secret of a record. It is a technique for maintaining data privacy. This technique changes the value of the data record without changing the underlying object of the data. It uses two techniques: data distribution and data distortion by generating decision tree classifications to include noise or any other data in the original data for classification before data release. This can be further reconstructed by registered owners who know the sample data used for the conversion [4], [5]. The perturbation technique is shown in Figure 2.

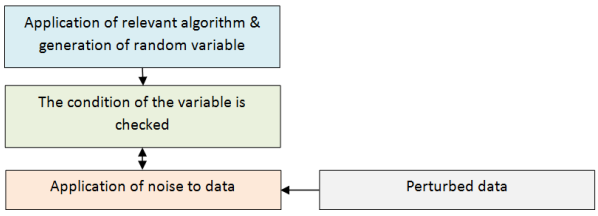


Figure 2 Implementation of perturbation technique

B. Advanced encryption standard (AES)

AES is a balanced cryptographic algorithm that is secure enough to protect data and can encrypt and decrypt data with key lengths of 128, 192, and 256 bits [5] and it . The AES encryption algorithm has the process of transforming the bytes that consists of Sub-Bytes, Shift-Rows, Mix-columns, and Add-Round-Key as transformation bytes [5]. In the case of decryption, the reverse cipher transformation is executed in the opposite direction using Inv-Sub-Bytes, Inv-Mix-Columns, and Add-Round-Key. In AES algorithm confidentiality is provided by block cipher modes (ECB, OFB, CBC, CFB, CTR & XTS).

Randomly encrypted modes use the initiation vector (IV) and by this it is possible to create unique ciphers even if the same empty text is encrypted several times [20]. Salt is implemented with AES to overcome the following shortcomings:

(1) The attacker can quickly detect the password using the birthday conflict method. It becomes much easier if a large number of passwords are stored in the database.

(2) An attacker can break a password in a few seconds using a predetermined number of hashes.

To remove these flaws, it is possible to combine the salt password before performing the hash function. Salt is a fixed length random number and different for each entry saved. It is saved after the password hash in plain text (original content).

C. Gaussian Blurring

The process of blurring an image via a Gaussian function is called Gaussian blurring. The main idea of this technique is to update the value of one pixel with the average of neighboring pixels.

Instead of calculating the average of all neighboring pixels, the weighted average is calculated. When this value is combined with the corresponding blurred pixel, the average weight of each pixel shows the largest value. Ideally, the Gaussian blurring method helps to find the weight of each neighboring pixel. The two-dimensional Gaussian functions are shown in Figure 1. The blurred pixel has a peak value compared to other neighboring weighted average pixels [11] - [12].

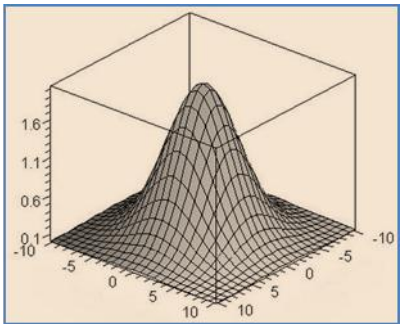


Figure 3. The graphical representation of the 2-dimensional Gaussian function [12].

The weight of the main pixel and the other weight of the base pixels can be calculated by Equation (1) in the Gaussian equation [11], [12]. The parameters of this equation are explained as follows:

$$F(x,y)=1/(2\Pi v^2)\exp((^{x2}+^{y2})/2v^2) \quad (1)$$

Where ν is blur factor, e is euler number, x and y represents the horizontal vertical distance to centre pixel respectively. If the blur factor increases, the image becomes more blur. According to equation 1, the x and y distances are zero for the central pixel. As the distance from the central pixel increases, the value of x2 + y2 increases and the weight decreases. If this formula is used for two dimensions, the bell-shaped distribution originates from the focal point and forms the homomorphic circular surfaces. These distribution values are used to make the change. That matrix is used to the original film. Each new value of the pixels can be calculated by averaging the self and neighboring pixels. The central pixel takes on a higher average weight. Nevertheless, the weight of neighboring pixels is directly proportional to the distance to the center. This process protects blurred coating, borders and edges [11]. The Gauss blur is applied to rows and columns. Thus, there is no need to pass every pixel. In this case the time complexity is given by equation 2[11]:

$$O(rows * cols * kernelheight + rows * cols * kernelwidth) \quad (2)$$

The Gaussian blurring mechanism for an image can be seen in Figure 2. The general purpose of this function is: to reduce image noise and image margins [12]. This is to ensure that bad high-frequency information does not appear in the image, which affects the indistinguishable causes of different signals. Gaussian blur is a suitable solution for images that do not have sharp edges.

IV. PROPOSED SYSTEM

This section gives the description of the proposed system. And the entire system of operation is shown in Figure 4.

A. Data Provider (DP)

The steps for the Data provider are shown below:

- Data provider upload image
- Then Encrypted using secret key
- Encrypted file is converted to binary
- The binary file is stored in Database of the cloud server

The data provider has an account registered prior to access the cloud server. Then DP can login to the account from anywhere using username and password and also DP can upload or download files. In the case of uploading, the content is encrypted with AES and salt key encryption method before being stored in the database.

B. Data User (DU)

The steps for the Cloud Users are shown below:

- Request access to cloud server for image file
- Cloud server send access request to data provider
- Cloud server enable registration of the Data user
- After enabling the Data user, Binary image file is sent to Data user
- Data user decrypt the Binary image file using secret key
- Data user obtains the privacy protected image file (blur image)
- Cloud server send OTP by email for accessing the image

DU is a user who can able to access data from the cloud server. DU must also get registered as DP in the cloud and can send requests to DP. The DP if it is genuine accepts the requests from DU and then shares a key with DU to access the data. DU after getting the key from the DP can access the data from the cloud.

C. Authorization Verification:

Authentication is the process of verifying a user's right to access something. The proposed model verifies the data user's privilege to access image data file in cloud environment. Both the DU and DP are verified whether they are meeting the data policies. After that cloud administrator approves the DU and DP.

All the sensitive data namely user email id and password are encrypted using AES with salt algorithm and stored into data base. Both the DU and DP are validated through one time verification code (OTVC) sent to their registered email ids. Depending on the verification, cloud administrator activates an account, ban illegal users, Monitor the user access. The uploaded image document to the cloud server by DP is converted to .txt file by the perturbation approach then that text file is encrypted with secret key set by the data provider. Each file has unique file id then that perturbated file is converted to binary file and stored into database. If DU want to access the uploaded file by the DP, DU must send access request to the DP, then DP validate the request and enable access to corresponding DU. If the DP enable access to DU, the cloud server send Access Key (One Time Password) to DU for viewing original image uploaded by the DP. Until then, DU cannot able to view the original image.

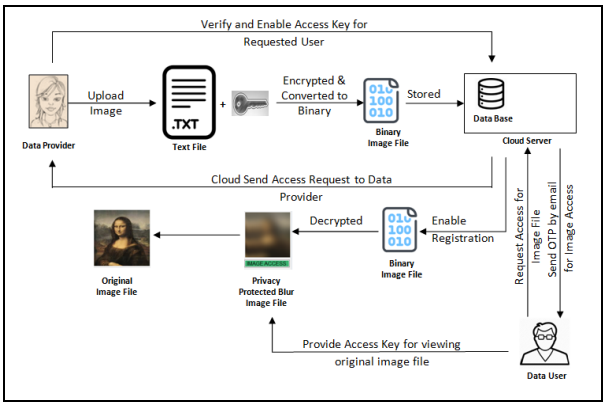


Figure 4. Operation of the Proposed System

V. RESULTS AND DISCUSSION

The above operation is executed C-sharp and dotnet with backend tool using SQL server. It uses public IP configured system/server and the results are obtained. Figure 5 represents the access request intimation email sent to data provider, Figure 6 shows the account activation OTP sent by cloud administrator, Figure 7 shows the account created by data provider, Figure 8 shows the login by data user, Figure 9 represents the file access request by data user to data provider, Figure 10 shows the file access granted by data provider, Figure 11 shows the image uploaded by data provider has converted to ".txt" file, Figure 12 shows the access grant permission by data provider , Figure 13 shows the data protection through perturbation, Figure 14 shows the login by cloud administrator, Figure 15 shows the cloud admin-account activation panel, Figure 16 shows the cloud admin-account de-activation panel, Figure 17 shows the image data perturbation.

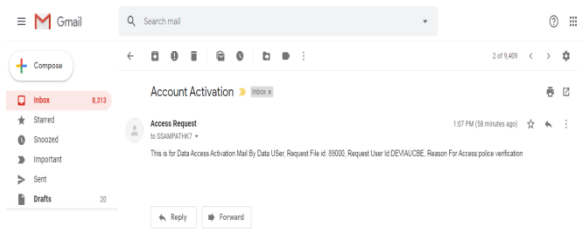


Figure 5. Access Request Intimation email sent to Data Provider

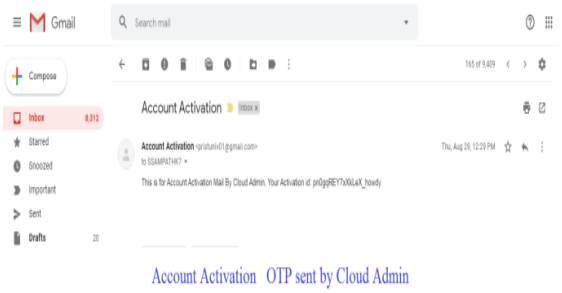


Figure 6. Account Activation OTP sent by Cloud Administrator

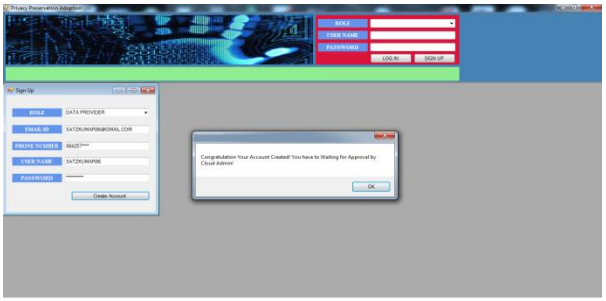


Figure 7. Account Created by Data Provider

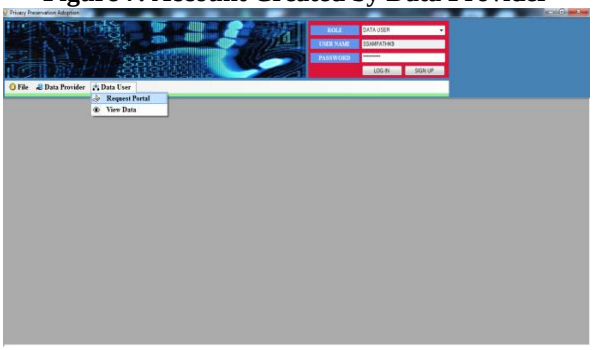


Figure 8. Login by Data User

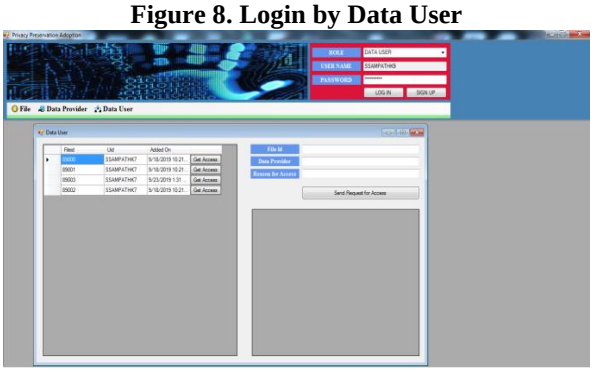


Figure 9. File Access Request by Data User to Data Provider

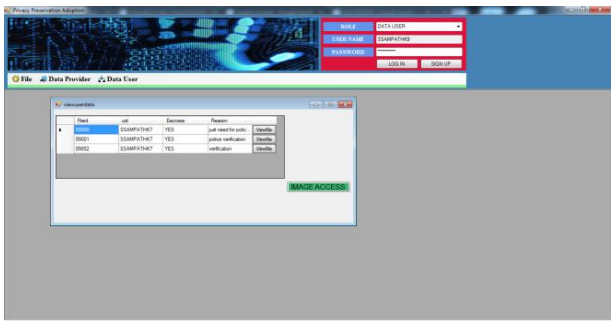


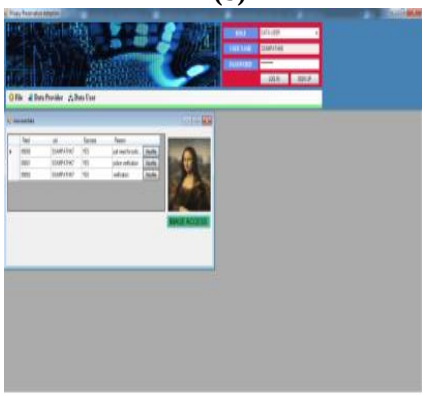
Figure 10. File Access Granted by Data Provider

Figure 11. Image Uploaded by Data Provider has converted to ".txt" File

Figure 12. Access Grant Permission by Data Provider

(a)

(b)



(c)

Figure 13 Data Protection through Perturbation

Figure 14. Login by Cloud Administrator

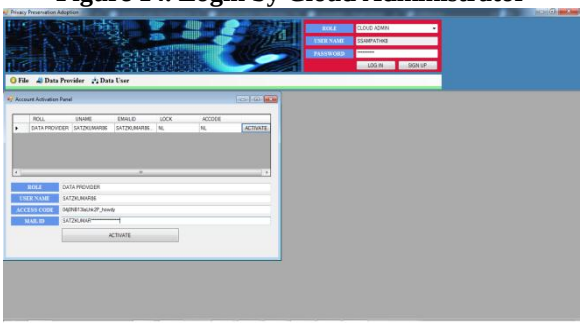


Figure 15. Cloud Admin- Account Activation Panel

Figure 16. Cloud Admin- Account De-Activation Panel

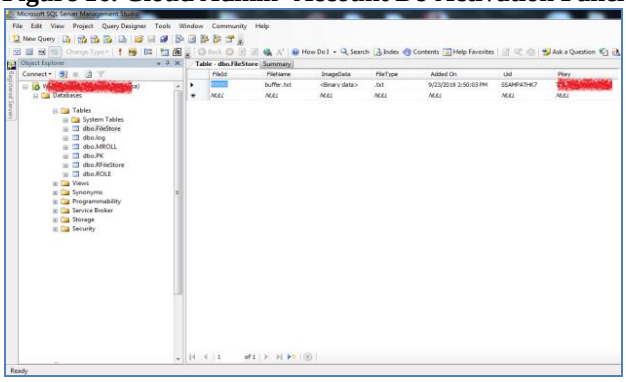


Figure 17. Image Data Perturbation

The sample of four test images is taken for the study. Their extension, dimension is shown in Table 1. After perturbation, the size of the file, the type of the file, and its execution time in milliseconds are shown in Table 1. Figure 18 shows the comparison of file size (kB), perturbed file size (kB) and execution time (ms) of the four sample test images taken for study. The results show that the average execution time is 0.034 seconds. Also the storage space occupied by the software of the proposed system is less than 100kB. This is the major advantage of the proposed system and till now it is not achieved by any other models in the existing literature.

Table 1. Execution Time of the Test images

File Name	Test image1	Test image2	Test image3	Test image4
File Size	36.3kB	37.1kB	15.0kB	10.5kB
File Extension	.jpg	.jpg	.jpg	.jpg
File Dimension	738x415	452x678	214x170	143x178
Perturbated File Name	Buffer	Buffer	Buffer	Buffer
Perturbated File Type	.txt	.txt	.txt	.txt
Perturbated File Size	37 kB	38 kB	16 kB	11 kB
Perturbated File Execution Time (ms)	39.1016	33.7738	28.8865	34.3017

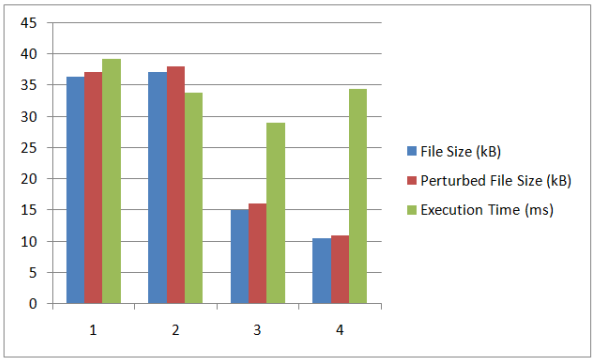


Figure 18. Comparison of File size (kB), Perturbed File size (kB) and Execution Time (ms) of the four Test Images

VI. CONCLUSION

Rapid increase in image data produced by individuals and companies provoke privacy hitches such as unauthorized revelation of personal data and person's individuality stealing, but it can be used to protect privacy of the user and also personal information. Data provider and Cloud Administrator are two types of users who have privilege and access. The Advanced Encryption Standard (AES) algorithm with salt key is selected for the login authentication process, which ensures the protection of information from unauthorized access and is proposed to create a random key generation. Data perturbation is used to add noise in databases, and Gaussian blur is done to introduce some degree of degradation in the original image. In this process, security authentication is reinforced in the ciphertext changes that make up the key words for each encryption process. The result shows that the model is relatively fast with a time average of 0.034 s occupying less than 100kB of memory space.

REFERENCES

1. S. Hill, Z. Zhou, L. Saul, and H. Shacham, "On the (in) effectiveness of mosaicing and blurring as tools for document redaction," Proceedings on Privacy Enhancing Technologies, vol. 4, 2016, pp. 403–417.
2. R. Hoyle, R. Templeman, S. Armes, D. Anthony, D. Crandall, and A. Kapadia, "Privacy behaviors of lifeloggers using wearable cameras," In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, 2014, pp. 571–582.
3. P. Ilia, I. Polakis, E. Athanasopoulos, F. Maggi, and S. Ioannidis, "Face/off: Preventing privacy leakage from photos in social networks," In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 781–792.
4. M. Korayem, R. Templeman, D. Chen, D. Crandall, and A. Kapadia. (2016) "Enhancing lifelogging privacy by detecting screens". In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, pp. 4309–4314. ACM, 2016.
5. K. Xu, Y. Guo, L. Guo, Y. Fang, and X. Li, "My privacy my decision: Control of photo sharing on online social networks," IEEE Transactions on Dependable and Secure Computing. vol. 14, no. 2, 2017, pp. 199-210.
6. K. Lander, V. Bruce, and H. Hill, "Evaluating the effectiveness of pixelation and blurring on masking the identity of familiar faces" Applied Cognitive Psychology, vol. 15, no. 1, 2001, pp. 101–116.
7. Li, Q. Li, and W. Gao, "Privacycamera: Cooperative privacy-aware photographing with mobile phones," In Sensing, Communication, and Networking (SECON)" 13th Annual IEEE International Conference on, pages 1–9. IEEE, 2016.
8. R. McPherson, R. Shokri, and V. Shmatikov, "Defeating image obfuscation with deep learning"' arXiv preprint arXiv:1609.00408, 2016.
9. A.C. Squicciarini, D. Lin, S. Sundareswaran, and J. Wede, "Privacy policy inference of user-uploaded images on content sharing sites," IEEE transactions on knowledge and data engineering, vol. 27, no. 1, 2015, pp. 193–206.
10. N. Vishwamitra, Y. Li, K. Wang, H. Hu, K. Caine, and G.-J. Ahn, "Towards pii-based multiparty access control for photo sharing in online social networks,". In Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies. ACM, 2017.
11. K. Xu, Y. Guo, L. Guo, Y. Fang, and X. Li, "My privacy my decision: Control of photo sharing on online social networks," IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 2, 2017, pp. 199-210.
12. Elisa Bertino, Federica Paci, and Rodolfo Ferrini, "Privacy-preserving Digital Identity Management for Cloud Computing," IEEE Computer Society Technical Committee on Data Engineering, vol. 32, no. 1, 2009, pp. 109-115.
13. Ali Inan, "A Hybrid Approach to Private Record Matching", IEEE transaction on Dependable and secure routing, vol. 9, no. 5, 2012, pp. 684-698.
14. Noman Mohammed, Benjamin Fung C. M., Ke Wangy, and Patrick Hungz C. K, "Privacy-Preserving Data Mashup" ACM journal, vol. 4, no. 7: 2009, pp. 467-474.
15. Zhiguo Wan, Kai Xing, Yunhao Liu, "Priv-Code: Preserving Privacy against Traffic Analysis through Network Coding for Multihop Wireless Networks" IEEE INFOCOM, vol. 12, no. 4, 2012, pp. 73-81.
16. Sonia Jahid, Shirin Nilizadeh, Prateek Mittal, Nikita Borisov, and Apu Kapadia, "DECENT: A Decentralized Architecture for Enforcing Privacy in Online Social Networks," In:IEEEInternational Conferenceon Pervasive Computing and Communications Workshops,;PERCOM'12. 2012, pp. 326–332.
17. Sören Preibusch, Alastair R., and Beresford, "Privacy-Preserving Friendship Relations for Mobile Social Networking," Workshop on the Future of Social Networking, 2009, pp. 1-8.
18. Amin Tootoonchian, Stefan Saroiu, and Yashar Ganjali, "Lockr: Better Privacy for Social Networks," ACM journal, vol. 2, no. 7: 2009, pp. 234-244.
19. Ilavarasan1 K.G. and Malavika R, "A multiple level visual Cryptography scheme for biometric Privacy without pixel expansion," International Journal of Communications and Engineering, vol. 4, no. 4, 2012, 809-819.
20. Murat Kantarcioglu, Ali Inan, Wei Jiang, and Bradley Malin. (2009) "Formal anonymity models for efficient privacy - preserving joins" Elsevier Science Direction Data & Knowledge Engineering, vol. 19, no. 1, 2009, pp. 1009-1019.
21. Murat Kantarcioglu, Ali Inan, Wei Jiang, and Bradley Malin, "Formal anonymity models for efficient privacy - preserving joins," Elsevier Science Direction Data & Knowledge Engineering, vol. 19, no. 1, 2009, pp. 1009-1019.
22. Deshmukh M., Ghatol A. P, "Different types of Data Privacy Preserving Repository and Schemes," International Journal of Computer Science and Applications, vol. 6, no. 2, 2013, pp. 313-318.

23. Xiaohui Liang, Mrinmoy Barua, Rongxing Lu, Xiaodong Lin, and Xuemin (Sherman) Shen, "Health Share: Achieving secure and privacy-preserving health information sharing through health social networks" Elsevier Science Direct on Computer Communications, vol. 4, no. 7, 2012, pp. 406-420.
24. Leucio Antonio, Cutillo Refik and Molva Melek ¨Onen, "Privacy Preserving Picture Sharing: Enforcing Usage Control in Distributed On-Line Social Networks" ACM, 2012, vol. 19, no.6, 2012, pp. 509-519.

AUTHORS PROFILE

Prof. S. Sambath Kumar, B.E.,M.Tech.(Ph.D), completed B.E. degree in Computer Science and Engineering in Anna University, Chennai. He obtained M.Tech in Embedded Systems from PRIST University, Thanjavur and Doing Ph.D in Computer Science and Engineering in PRIST University, Thanjavur. He is having more than nine years of service in teaching as Lecturer, Assistant Professor. His area of interest includes Data Mining, Privacy Preservation Data Mining, image processing.

Dr. S. Devi, completed B. E. in Electronics and Communication Engineering in Bharathidasan University, Trichy and M.Tech in Communication Systems in Dr. M.G.R University, and Ph.D in Anna University. She has more than ninteen years of experience. She has published more than twenty papers in reputed peer reviewed Journals, Conferences, and book chapters.