International Conference on Recent Trends in Data Science and its Applications
DOI: rp-9788770040723.083

A Secured Photo Sharing framework Using Blockchain Technology for cross-social Platforms

Vijay A
Department ofInformation Technology
M.Kumarasamy College ofEngineering
Karur, India
vijaya.it@mkce.ac.in

Arun S
Department ofInformation Technology
M.Kumarasamy College ofEngineering
Karur, India
arunraj170320@gmail.com

Dhinakaran R S
Department ofInformation Technology
M.Kumarasamy College ofEngineering
Karur, India
dhinakaran2001s@gmail.com

Kavinkumar M
Department of Information Technology
M.Kumarasamy College of Engineering
Karur, India
mkavinkumar2001@gmail.com

Raghu K V
Department of Information Technology
M.Kumarasamy College of Engineering
Karur, India raghukvr905@gmail.com

***Abstract*—Online Social Networks (OSN) have grown in popularity as a result, for the previous few years of the quick development of mobile applications and the explosive expansion of online engagement. As technology and the Internet become more accessible, so has the ease with which users can upload and share photos on Social Networking Sites (SNS). Therefore, it is necessary to safeguard the confidentiality of the same. On the other hand, those methods lose their utility as soon as someone posts the images on other platforms, this unauthorised disclosure of the user's private information causes negative effects and endangers the user's safety. In order to present effective spreading control for cross-social network picture sharing, Photo Chain, a blockchain-based framework, has been created with the goal of protected photo sharing. Combining blockchain, Gaussian Blur for face masking, Pre-Hash Algorithm for photo integrity verification, and Access Control, sharing, and access without having to worry about potential harm to user's interests. To maximize the adaptability of re- posters without jeopardizing the privacy of the former, a vivid privacy policy generating algorithm has been created. The concept also incorporates robust photo ownership identification technologies to stop illicit reprinting. The project culminates with the execution of a prototype and setup in a nearby simulated social setting. The extensive tests and safety measures investigation demonstrate the suggested framework's competence, security, and efficiency.**

Keywords—Block Chain, Cross Social Network, Photo Sharing, Security, Pre-Hashing Algorithm, Gaussian Blur Algorithm, Privacy Preserving.

I. INTRODUCTION

A digital communication tool is social media. Users may participate in conversations, share information, andproduce material for the internet via social medias. Some of the examples for social media can take include social networking sites, photo and video sharing websites, blogs, instant messaging, podcasts, widgets, virtual reality, and other platforms.

Fig. 1.1. Social Media

Most of us today use social media sites like Instagram, Twitter, Snapchat, You Tube, and Meta to communicate with potential virtual mates. These devices leverage online social media networks to alert users of news about their friends, favourite celebrities, and significant global events. Social media is now widely used by many people as part of their daily lives. Numerous billions of people use social media to communicate and share information. Social networking offers you the freedom to connect with loved ones, learn new things, pursue new interests, and seek entertainment.

Frequently used social media platforms and tools: Blogs: A forum for casual conversations and talks about a specific topic or point of view.

Meta: The primary social network in the world, with regularly active users creating private accounts, adding other users as friends, and exchanging communications like status updates to communicate current information. The brand-generated pages can be liked by meta users.

Twitter: A social networking or microblogging platform that enables quick status updates to be exchanged between users and organizations (140- character limit).

YouTube/Video: Uploading videos and browsing websites.

Instagram: An app that allows users to add digital filters, frames, and other creative effects to photos they want to post on social media.

LinkedIn: A topic where a group of professionals with comparable interests can share data and participate in discussions.

II. RELATED WORKS

- KambizGhazinour, John Ponchak [1] This study aims to reduce the security risk for common users by developing a GUI-based metadata reader and editor. The underlying risk, which is concealed in all shared media, can be brought out in the open and reduced by bringing the capacity to examine and modify metadata to various platforms.R. Regin, B. Sneha [2] It displays an adaptive concealing policy indication mechanism that, when shared with several clients, offers a policy to the client. Based on their level of trust in the recipient, this policy aids the client in deciding whether or not to share an image.

- PrashantAbhang, S.B.Rathod [3] The main concept was to create a participant-free tagging technique that would enable the automatic association of a user's account with a specific person's face. In this instance, adversaries were unable to use malicious tagging assaults to share photographs on social media.

- Lei Xu, Ting Bao [4] It is implemented a fine-grained confidentiality managing of photo sharing by means of image processing algorithms. A notion for access controlling in photo sharing in which a image is broken up as several layers that are containing single blurred face. A viewer's final image is created by superimposing specific layers in accordance with their privacy settings. For photo sharing in OSNs, Edwin et al. developed a multi-party admittance architecture that enables access control granularity to be gradually tweaked from photo-level to face-level.

- Mary Jean Amon, RakibulHasan [5] I-Pic and COIN are privacy-preserving sharing systems that let users publish privacy options so that nearby photographers can learn about and respect their preferences. They alert registered users whenever another person nearby takes a picture and tell them whenever another user does so. So, in the current study, we also investigate how often, infrequently, or never people exchange photographs.

- PooryaAghdaie, BaariaChaudhary [6] Genuine facial pictures from two separate people are used to create a morphing image. The final morphed image may be compared to both genuine persons because it has traits from each, allowing for verification. Two methods are used to create morphed photos. In the first method, a morphing image is produced by alpha blending two real facial photographs.

- HarshaliChandel ,Dr. A. M. Bagade [7] Social networking sites (SNSs) are a limitless form of communication that allow people to stay in touch across borders. SNSs are more than just a web application; they are a component of human civilization. SNS use has outpaced conventional forms of communication in practically every industry, including that of news organizations, large and small businesses, governments, and well-known individuals. The abundance of technology and services has made it easier to share information with friends and family, including news, photographs, personal preferences, and information.

- VatsavaiSrija& T SaiDurga [8] Utilizing the K- Nearest Neighbours technique, we are studying the face matching notion. In our project, we are employing the Ball-Tree technique, one of the many sub-methods in the KNN algorithms. Binary Tree Method is another name for the Ball-Tree algorithm. Each node in this technique generates a D-dimensional hypersphere that contains a subset of the searchable points. The prediction parameters are saved in a CLF file when the B-Tree is constructed.

III. PROPOSED METHODOLOGY

With the help of fairness and without any potential risk to the user's safety, Photo Chain, a combined block- chain, Gaussian Blur for face masking, Pre-Hash Algorithm for photo integrity verification, and Access Control, Mechanism realises secured data sharing, retrieval, and access.

Algorithms and Techniques used

- Smart Contract
- Gaussian Blur
- Pre-Hash Algorithm
- Access Control Mechanisms
- Hash-Key to verify the integrity in photo shared

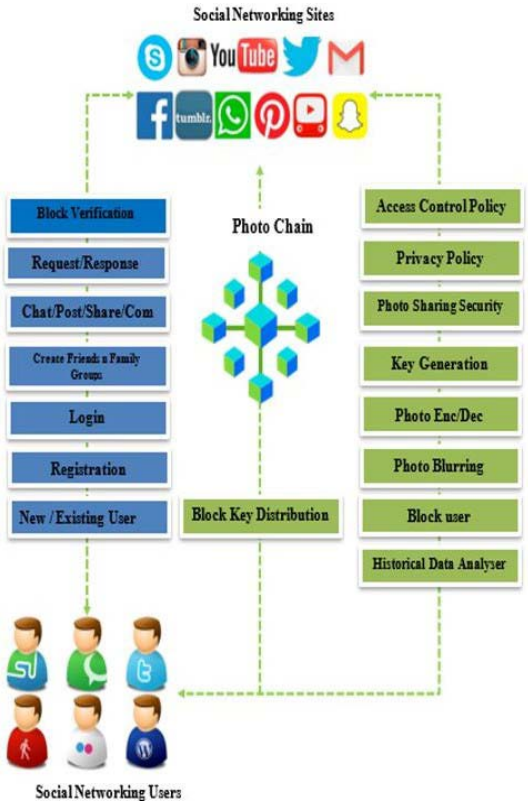


Fig. 3.1. Proposed Architecture

1. SN Web App

The development of SNS as a platform that people may use to connect with others who share their interest, abilities, environments, and real-life connections is taking place. SNS come with a range of formats and facets

2. End user C-panel

2.1. Register

Users of the App must first register their data in order to access and share pictures on the website. In order to access the current and contact information shared by friends, one must first log into the application. They can upload the image as either private or public. Wherein others have the ability to make friend requests, accept them, and intend to reveal secret representations of the medium.

2.2. Login

The user will exhibit many social network functions, including editing his profile and performing the actions of

DOI: rp-9788770040723.083
viewing and adding friends, searching for other users, and seeing user profiles.

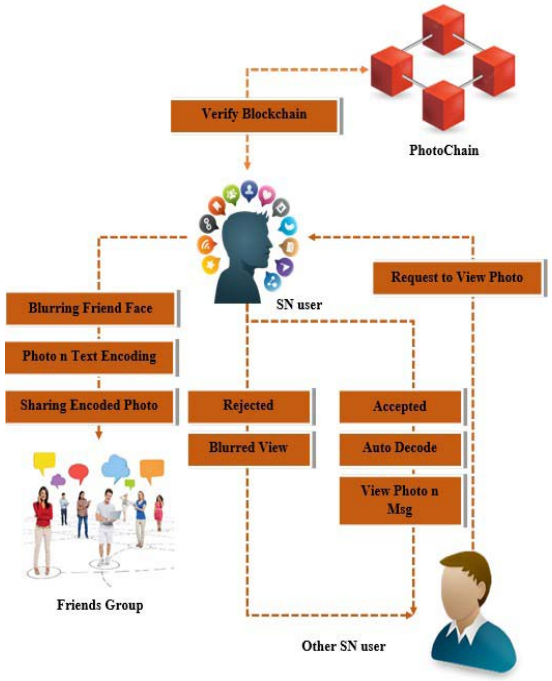


Fig. 3.2. System Flow

2.3. Add Friends /Family Groups

The log-in/log-out button for the social platform is called Friend Request. A greeting and the profile picture are made public after logging in. The proposed prototype has three operating modes: setting up, sleeping, and functioning.

In order to organize the area by selecting the "Pick-Friends" button, a user must physically locate the group of "close friends" from the list on the social networking platform.

2.4. Share/Post/Comment/Chat

Users that post photos can limit their sharing to their friend’s in-lists. The projected plan complies with the co-owner’s disclosure guiding principle and the list of communications of owner’s privacy process.

2.5. Policy mining

Users can choose whether to make an uploaded image public or private; only eligible users who have permission to see public photographs can then access these images; otherwise, they will be hidden. The owner of the content should make available the key forthat image if people wish to see private content. Since representations in the same class are also anticipated in a comparable level of confidentiality fortification, policy mining is conducted inside the same class.

2.6. Policy prediction

This process generates a vast number of application policies while returning to the user the most promising applicants. In terms of offering the anticipated guiding principle of a recently uploaded photo for personal reference, this represents a step towards selecting the best candidate method.

2.7. Request/Response

There are two ways to react to a friend's request: either click the buttons labelled "confirm" or "not now" to decline the invitation.

3. Photo Privacy

3.1. Key Generation

During this process, the personal information of the photo is protected using the selected protection tool and a secret key (or set of keys) given by the sender. The proper management of all the encryption keys used in the system is a relevant difficulty in addition to offering an appropriate security level and an effective implementation. A centralised strategy has been suggested in which the trusted Key Server stores all of the keys.

To produce unique keys for each image and region within it, the server must be able to detect images in a unique way. As previously noted, the encrypted image's metadata contains this particular ID. The encrypted image's metadata contains this particular ID. The hash of the image could be used as ID as an alternative strategy. The drawback of utilising the hash as the ID is that it must be performed in the mobile application, which could be costly depending on the size of the image and could result in security issues if hash collisions are discovered. More significantly, the key server would have the ability to examine some usage patterns and identify instances where two users encrypt the same image.

3.2. Photo and Message Encode/Decode

Image and Message Encoding

Form-sampling, residual, and down-sampling layers make up the encoder network. Fig. 2 depicts the encoder network's organisational structure. Numerous skip connections are used in the reset to combine shallow and deep features at various stages of convolution. The shallow feature is with numerous low level competent particulars about the framework and colour on the image that can be used to create steganographic images. The findings of constructing an encoder network havingtopology alike to the U-Net have shown how the skip connection can effectively reduce steganographic image distortion and improve visual quality.

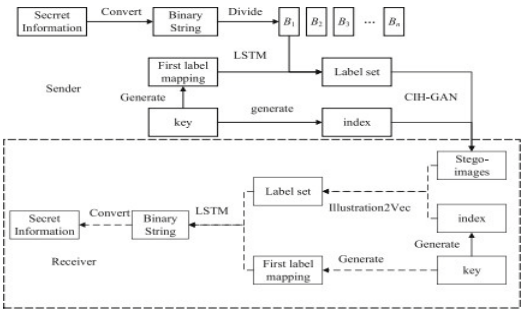


Fig. 3.3 Image and Message Encode and Decode

DOI: rp-9788770040723.083

a. original image

Image and Message Decoding

The decoding network, made up of 6 layer complete Convolutional Network (CN) that pulls out secret colour image-S' from the steganographic image-C'. The encoder and decoder networks from the previous part make form the generator in the proposed model HIGAN. Past studies have shown that both three-channel colour and single-channel grayscale secret images can be successfully recovered using the decoder network's architecture. Following each of the 3 convolutional layers having stride-1 and padding-1, the Batch Normalization method and Real Activation Function are used. However, Sigmoid Activation Function was employed subsequent to the ending layers. The decoding network eventually discloses the hidden image-S.

b. generated image

Here, the CNN parameters includes,

Designing: The nature of the shared images, the intended use case, and the system's performance needs will all have an impact on how the CNN architecture for a blockchain-based secure photo sharing framework for cross-social networks is designed.

Image Pre-processing: The images is necessary to guarantee that they are in a format that the CNN can use. The pictures may need to be resized, their pixel values normalized, and they may need to be converted to grayscale or RGB format, among other things.

Network Architecture: Given that it will have to analyse a lot of images in real time, the CNN architecture needs to be effective and scalable. Additionally, the architecture ought to be able to handle various picture sizes and aspect ratios.

Hyperparameters: It has a number of convolutional and pooling layers to acquire features from images and fully connected layers to categorise the images, is a well-known architecture for image classification.

The CNN should include security measures like encryption and secure authentication since the framework is built on blockchain technology to make sure that only authorised users can access the shared pictures.

3.3. Photo Blurring

A Gaussian function, commonly referred to as Gaussian smoothing, blurs an image. It is a typical effect in graphics software, usually intended to decrease detail and visual noise. Unlike the bokeh- effect due to the out-of-focus of lens / shadow on the object as a result of standard lighting. The proposed technique produce the smooth blur appearing same as translucent screen.

4. Privacy Violation

A policy's current state Individual users are in charge of the privacy policy's current state. The policy should take into account the person's exposure needs as well as their privacy demands. Defend or post If the policy is satisfied, the co-owner receives the notification. The photo is only posted once the owner has permission to upload it; otherwise, it is not.

5. Photo Chain Integration

Based on blockchain technology, the decentralized SN data sharing and storage system Photo Chain decouples user data and programs to return ownership of the data to the users.

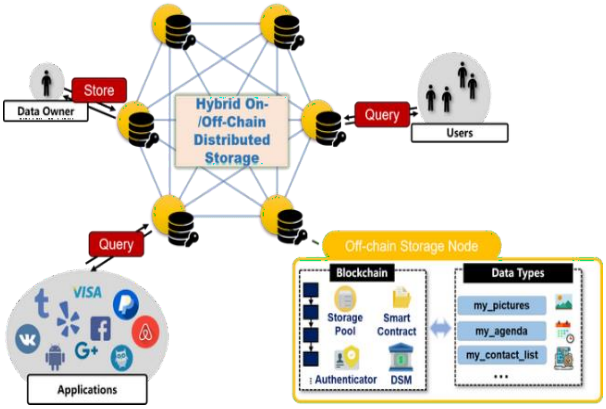
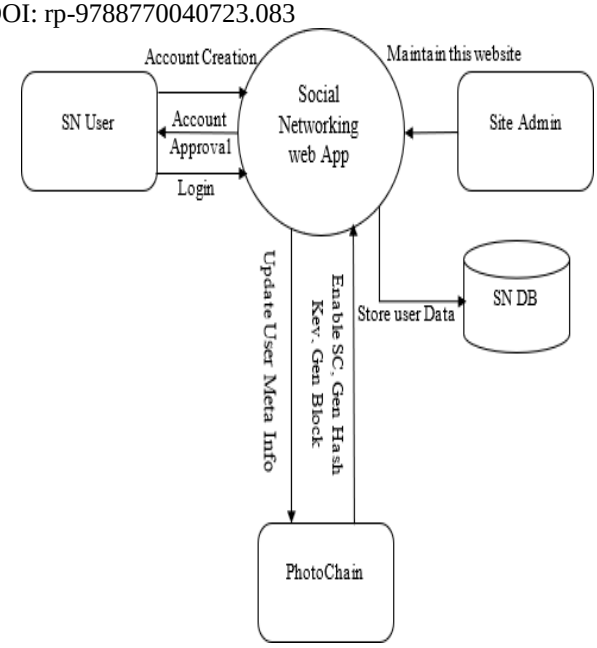


Fig. 3.4. Photo Chain Integration

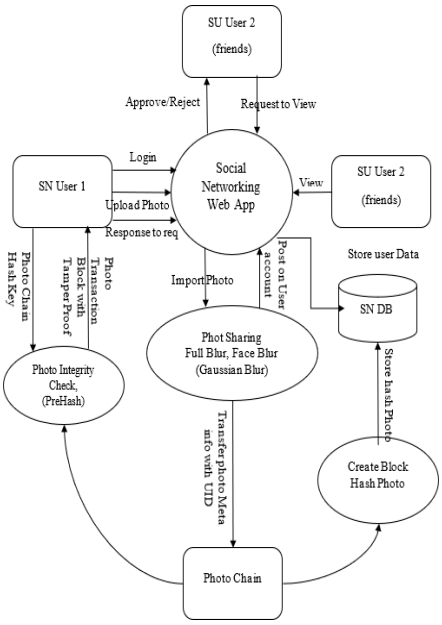
We employ Personal Data Store to increase off-chain storage for internet data. With the use of a distinctive identity assignment (i.e., Web-ID) and certificateless cryptography, we also established an identity establishment mechanism that can support Web ID- based authentication functions. In order to automatically store and securely distribute social data, we design a general framework that uses smart contracts.

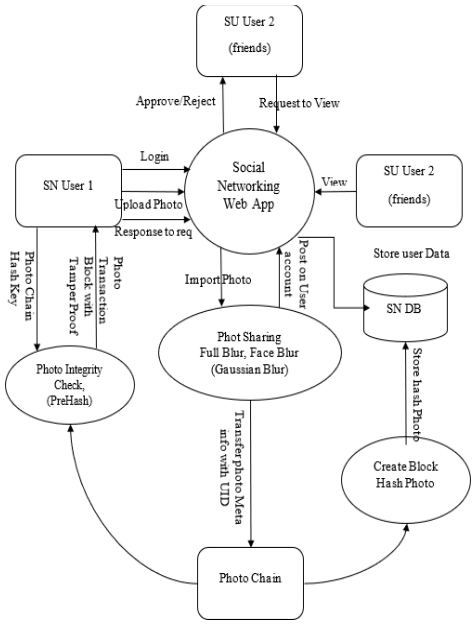
Level – 0

DOI: rp-9788770040723.083



Level – 1





Level – 2

IV. IMPLEMENTATION

- The framework's architecture should be created in a way that enables users to safely store and exchange photos across various social networks. It ought to be built on a blockchain network that offers a decentralised and impenetrable picture storage system.
- For instance, a smart contract can be created to limit who has access to shared photos.
- Integrate social networks: The framework needs to be linked with various social media platforms, including Twitter, Instagram, and Facebook. The social networks' APIs can be used to accomplish this.
- Implement a secure authentication method: A secure authentication method should be used to guarantee that only authorised users can access the shared photos. Digital signatures and public-key encryption can be used together to accomplish this.
- Implement encryption and decryption mechanisms: Encryption and decryption mechanisms should be used to ensure the privacy and confidentiality of the shared pictures. Algorithms like RSA or AES can be used for this.

Overall, a combination of technologies including blockchain, smart contract, encryption, and decentralised storage systems is needed to implement a blockchain-based secure picture sharing framework for cross-social network use. To enable users to safely keep and share their photos across various social networks, the framework should be created with security and privacy in mind.

V. CONCLUSION

Due to the widespread use of smart mobile devices with high-resolution cameras and user-friendly social networks programs, sharing photos has become an easy and popular hobby. Yet, the majority of photo sharing sites don't have a reliable method for safeguarding users' privacy. In this

project, we created, put into practise, and assessed Photo Chain, an expanded control framework for blockchain-enabled, privacy-preserving photo sharing across several social networks. By regulating the actions of the users after them in a dissemination chain, it aids social networking users in maintaining the privacy criteria assigned to their uploaded photos. Without interfering with the display phase, it ties the access control policies to the images in the interim. Photo Chain may therefore enable social networking users to conceal private areas from prying eyes across many social networks. Photo Chain not only protects the shared photos so that no unauthorized users can access them, but also enables users to blur their image search so that the search can also be shared to a cross social networking site obliviously without leakage on the query contents or results. Additionally, Photo Chain not only safeguards user privacy but also minimises system overhead. Results of the evaluation showed that it is effective the idea of photo chain, which offers privacy, confidentiality, and integrity. The suggested plan prevents unwanted users from accessing the private information while also ensuring that legitimate users continue to share information without interruption.

In future work, we will further develop our system by taking into account more user-related attributes and security levels of various groups in order to provide access control with a finer grained. We plan to investigate how the most recent technological advancements, including federated learning, can protect user privacy in Cross SNs in the future.

TABLE 1: RESULTS OF ACCESSING THE PHOTOS

Groups	Can't view	Viewable	Download	Re - upload
Friends	5.6%	90.4%	76.4%	23.2%
Strangers	50.5%	50.4%	43.6%	8.1%
Others	75.2%	22.8%	11.3%	2.3%

REFERENCES

[1] Lihong Tang1, "Faces are Protected as Privacy: An Automatic Tagging Framework Against Unpermitted Photo Sharing in Social Media" Digital Object Identifier 10.1109/ACCESS.2019.2921029date of current version date of current version June 2019.

[2] Aniello Castiglione, Bonaventura D'Alessio, "Steganography and Secure Communication on Online Social Networks and Online Photo Sharing", UniversitàdegliStudi di SalernoI-84084 Fisciano (SA).

[3] Y. Edwin, and F. Song, "Poster: PhotoLock: Autonomous Privacy-preserving Photo Sharing in Online Social Networks", University of Oklahoma, PhD Thesis,2018.

[4] R.L. Fogues, P.K.Murukannaiah, J.M. Such,and M.P. Singh,"Sharing policies in multiuser privacy scenarios: Incorporating context, preferences, and arguments in decision making," ACM Transactions on Computer- Human Interaction, vol. 24, no. 1, p. 5, 2017.

[5] P. Ilia, I. Polakis, E. Athanasopoulos, F. Maggi, and S. Ioannidis, "Face/off: Preventing privacy leakage from photos in social networks", Proc. Of ACM CCS 2015.

[6] J. He, B. Liu, D. Kong, X. Bao, N. Wang, H. Jin, and G. Kesidis, "Puppies: Transformation-supported personalized privacy preserving partial image sharing", In: Proc. of IEEE/IFIP DSN 2016.

[7] H. Hu, G. J. Ahn, and J. Jorgensen, "Multiparty access control for onlinesocial networks: model and mechanisms", IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 7, pp.1614 - 1627, 2013.

[8] Dhanabalan, S. S., Sitharthan, R., Madurakavi, K., Thirumurugan, A., Rajesh, M., Avaninathan, S. R., & Carrasco, M. F. (2022). Flexible compact system for wearable health monitoring applications. Computers and Electrical Engineering, 102, 108130.

[9] Y. Fenghua Li, and Zhe Sun "An Extended Control Framework for Privacy-Preserving Photo Sharing across Different Social Networks",International Conference on Computing 2019.

[10] P. Forero, A. Cano, and G.B.Giannakis "Consensus- based distributed support vector machines",Mach Learn J, Res, vol. 99, pp. 1663–1707, August 2010.

[11] K.Xu, "My Privacy My Decision: Control of Photo Sharing on Online Social Networks", IEEE Transactions on Dependable and Secure Computing, 2017.

[12] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, "Distributed optimization and statistical learning via the alternating direction method of multipliers", Found. Trends Mach. Learn., vol. 3, no. 1, pp. 1–122, Jan.2011.

[13] Gomathy, V., Janarthanan, K., Al-Turjman, F., Sitharthan, R., Rajesh, M., Vengatesan, K., &Reshma, T. P. (2021). Investigating the spread of coronavirus disease via edge-AI and air pollution correlation. ACM Transactions on Internet Technology, 21(4), 1-10.

[14] A. Kapadia, F. Adu-Oppong, C. K. Gardiner, andP. P. Tsang, "Social circles: Tackling privacy in social networks", in Proc. Sympsable Privacy Security, 2008.

[15] R. Trenholm, "Most Facebook Photos are Taken While Were Drunk, Survey Says", Accessed: Jun. 8, 2019.[Online].Available: https://www.cnet.com/news/most-facebook photos-are- taken-while-were- drunk-survey-says.