A Novel Image-based Homomorphic Approach for Preserving the Privacy of Autonomous Vehicles Connected to the Cloud

Aiman Sultan, Shahzaib Tahir, *Senior Member, IEEE,* Hasan Tahir, *Senior Member, IEEE,* Tayyaba Anwer, Fawad Khan, *Senior Member, IEEE,* Muttukrishnan Rajarajan, *Senior Member, IEEE* and Omer Rana, *Senior Member, IEEE*

***Abstract*—Autonomous vehicles are taking a leap forward by performing operations without human intervention through continuous monitoring of their surroundings using multiple sensors. Images gathered through vehicle mounted cameras can be large, requiring specialized storage such as cloud. However, cloud data centres can be prone to security and privacy challenges. A partial image-based, homomorphic searchable encryption scheme is proposed, which uses pixel-level encryption to identify objects within encrypted images. The scheme provides Object-Trapdoor and Trapdoor-Image indistinguishability – as the trapdoors are probabilistic. The proposed scheme is deployed on a cloud data centre and tested over a real data set. The proposed scheme reduces storage overhead by approximately 20 times, and is 33 times more efficient compared to the generic Paillier homomorphic searchable encryption scheme. Security analysis demonstrates that the scheme maintains high levels of security and privacy.**

***Index Terms*—Paillier homomorphic encryption, partial image encryption, Searchable Encryption.**

I. Introduction

THE necessity for Internet of Things (IoTs) in an industrial setting has seen a significant rise. A self-driving autonomous vehicle demonstrates how real-time inputs generated by cameras, sensors and LIDAR can support vehicles to operate on public roads. Figure 1 shows different sensors in an autonomous car, enabling automated detection of multiple objects such as cars, trucks, traffic signals, animals, lanes, pedestrians etc., and generating a viable response accordingly. However, several obstacles remain to transition from non-autonomous to fully autonomous vehicles, such as the danger of accidents, establishment of road traffic rules, and accountability. The combination of human drivers and self-driving automobiles can pose a risk at certain hazardous angles and lighting conditions where accidents may occur [1]. There are several legal concerns from law enforcement agencies when considering tracking autonomous automobiles or having significant surveillance data [2].

Automated vehicles can generate data in the form of images/ videos via a real-time webcam feed that needs to be stored and processed for further use *e.g.* for surveillance, location tracking, keeping a record of the vehicle movement, and protection of owners, etc. Local storage and management of this data poses a challenge to the vehicle owner(s) and raises concerns regarding the security and privacy of autonomous vehicle data, often requiring third-party storage.

Cloud computing is the provision of on-demand computation and storage resources through the internet on a pay-as-you-go basis. To decrease the expenses of local maintenance, an increasing number of users opt for outsourcing their data to the cloud server. However, outsourcing of data comes with its challenges, the foremost of which is data confidentiality. Moreover, there remains the need to ensure the integrity of data, its authenticity of access control in communication as well as its storage. It implies that data should be secured against unauthentic modification and scheme(s) should be employed to ensure legitimate access control and authorization. One of the major problems for cloud computing is data privacy since the cloud server is not considered a fully trusted entity and is assumed to be *honest but curious* to gain information about the outsourced data. Although end-to-end encryption ensures the security of users' data, it eliminates the ability to carry out searching over it.

While the applicability of the multiple secure and privacy-preserving techniques on cloud services are widely being explored [3] [4], most common techniques being employed are Privacy Enhancement Technologies (PET) [5] and Homomorphic encryption-based searchable schemes [6]. In practice, PETs are expensive, computationally extensive and resource intensive, making them hard to implement, prone to user error and can result in serious bandwidth issues. PETs may also give people a false sense of security, which may encourage them to engage in forms of behaviour deemed unacceptable by regulations and jurisprudence [7] [8].

Homomorphic encryption schemes, on the other hand, enable the users to process and work on the data without decryption, thus saving resources and time in terms of efficiency [9]. Mathematically, it means that the processing is done on plaintext after encryption will yield the same result as

A. Sultan, S. Tahir, T. Anwer, F. Khan are with the Department of Information Security, College of Signals, National University of Sciences and Technology (NUST), Rawalpindi, Pakistan. e-mail: (asultan.msis17mcs@students.mcs.edu.pk; shahzaib.tahir@mcs.edu.pk; tayyabaanwer21@gmail.com; fawadkhan@mcs.edu.pk).

H. Tahir is with the School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Islamabad, Pakistan. e-mail: (hasan.tahir@seecs.edu.pk).

M. Rajarajan is with the School of Mathematics, Computer Science and Engineering, City, University of London, UK. e-mail: (r.muttukrishnan@city.ac.uk).

O. Rana is with the School of Computer Science and Informatics, Cardiff University, UK. e-mail: (ranaof@cardiff.ac.uk).

if the same process was done before on plaintext and then was encrypted afterward. In this way, the underlying plaintext remains unchanged with no threat to its integrity even after performing various operations. This implies that searching can be carried out efficiently and easily over encrypted data and queries generated will yield no beneficial information about the underlying data. Multiple applications for homomorphic-based searchable encryption schemes have been proposed in different domains *i.e.* finance, healthcare, artificial intelligence, blockchain, vehicular ad-hoc networks (VANETS) as well as telemedicine [10]–[13]. While some may propose the capability to search securely over data [14]–[17], many other schemes focus on secure key agreement *i.e.* mutual authentication, data integrity and privacy preservation [18]–[20].

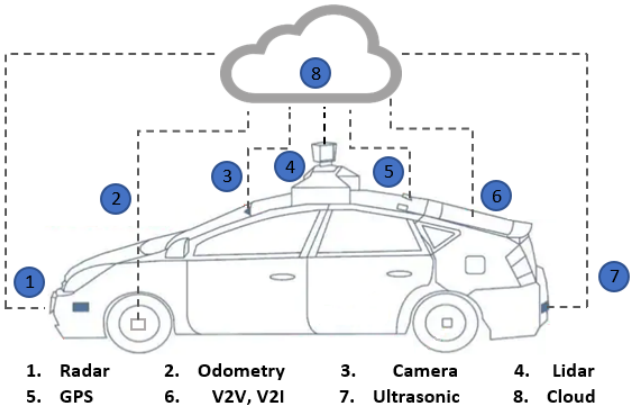

Fig. 1. Autonomous Vehicle Multi-Sensory Inputs and Cloud Connectivity

The data generated by multi-sensor cameras of autonomous vehicles can be so large that local (on-vehicle) storage is not an option. Therfore, data has to be migrated to an external hosting platform, yet be secured so that it is not accessible to unauthorized users. To achieve this, search operations need to be carried out over encrypted images stored on a cloud. In addition, search pattern security should also be ensured so that no information is revealed about the encrypted image data from the search history. A search query should be randomized so that trapdoors are generated probabilistically and no two similar trapdoors are generated even for the same query. Searching over homomorphically encrypted data with privacy-preserving mechanisms through probabilistic trapdoors, along with the requirement of storing large quantities of data from autonomous vehicles, form the two key motivations for this research.

A. Contributions

The following contributions are made in this research:

- The prevalent issue of security and privacy associated with autonomous vehicles connected to the cloud is addressed for the first time through homomorphic-based searchable encryption. A novel partial image-based homomorphic scheme is proposed for preserving the privacy of autonomous vehicles, which carries encrypted searching over encrypted image data (at pixel level) gathered from the camera embodied within an autonomous vehicle. The searching is carried out over probabilistic trapdoors to provide security against search pattern leakage.
- The scheme is deployed and tested in a real cloud environment "Contabo" over a real world data set. The proposed scheme reduces the storage overhead by approximately 20 times and is nearly 33 times more efficient as compared to generic Paillier Homomorphic Encryption based searching scheme. The paper also highlights the practical challenges, lessons learnt and way forward.

The rest of the paper is organized as follows: Related work is discussed in Section II. Section III presents the preliminaries. Section IV discusses the system model. Section V revisits the security definitions. Section VI put forwards the proposed methodology. Security and performance analysis are discussed in Section VII and VIII respectively while Section IX concludes the paper and explores future works.

II. Related Work

Research on image processing algorithms and Searchable Encryption (SE) on encrypted image data has highlighted its high computational and resource requirements. There are different image processing techniques and thus provide a vast ground for image searching mechanisms *i.e.* feature detection, content-based searching and digital watermarking, etc [21]. Research scholars working in the field of image processing have been working on extracting features from heavily encrypted image data sets. Different searchable encryption schemes [22] are employed for encrypted image searching over cloud *i.e.* homomorphic encryption, asymmetric watermarking, zero-knowledge proofs, and zero-knowledge watermarking detection to name a few. Application of existing techniques over encrypted images remains an open challenge for data owners, and many different theoretical proposals, as well as mathematical models have been presented to counter issues in this domain [22] [23].

The initial presentation of searchable encryption over image data was claimed to be carried out by [24] with the help of Scale Invariant Feature Transform (SIFT) and homomorphic encryption. The research lacked the property of privacy preservation and had the drawback of huge overhead on user's end. These vulnerabilities were addressed in [25] using a multi-cloud model incorporating the user's privacy preservation of data while retaining the image's original SIFT features. An image feature extraction scheme for privacy preservation using SIFT (PPSIFT) was proposed in [26] based on the Paillier cryptosystem. The design goals and technological problems of implementing a cloud-based privacy-preserving image processing system were examined in [27]. An approach based on Hahn Moment was put forward by [28] using somewhat homomorphic encryption (SHE) and claimed that its model provided confidentiality and privacy preservation of reconstructed images. Another scheme for images' feature similarity searching over cloud environment was presented in [29]. It tackled both local and global feature extraction/retrieval under Earth mover's distance metric and searchable generation of indices. An alternative technique for privacy preservation of image data based on Linear Binary Pattern (LBP) was

TABLE I
COMPARATIVE ANALYSIS OF IMAGE BASED SEARCHING SCHEMES

Research Paper	Technique Used	Index based	Homomorphic Encryption based	Search Pattern Security	Probabilistic Trapdoor	Privacy Preservation
Secure searching over encrypted images [24]	SIFT	✓				
Multi-cloud model for user's privacy preservation [25]	SIFT	✓	✓			✓
Privacy preserving searching over encrypted images [26]	PPSIFT & RSA		✓		✓	✓
Cloud-based privacy-preserving image processing system [27]	SIFT, HOG & SHE		✓			✓
Privacy-preserving of reconstructed images [28]	Hahn Moment & SHE		✓			✓
Image feature based similarity searching scheme [29]	Earth Mover Distance Metric	✓				
Image features based technique for privacy preservation [30]	Linear Binary Pattern	✓				
Ranked searchable encryption scheme [31]	LSH & kNN	✓				
Privacy-preserving of Image data [32]	K-means for Indices generation	✓				✓
Content Based Image Retrieval (CBIR) scheme [33]	DCT	✓				
Privacy preservation CBIR (PIC) [34]	kNN means & Multilevel Homomorphic Encryption	✓	✓			✓
CBIR over Mobile Cloud Computing [35]	LSH & SIFT	✓				✓
Privacy Preserving Searching over Encrypted Medical Image data [36]	CNN & PHE		✓	✓		✓
Efficient Privacy Preserving Image Similarity Detection [37]	PHE & Euclidean Distance		✓			✓
CBIR scheme over Cloud [38]	Inception with ResNet v2 (SIRS-IR) & Multiple Share Creation (MSC)					✓
Privacy Preserving Image retrieval scheme [39]	4D chaotic map & AES	✓				✓
Privacy preserving medical IR scheme [40]	CNN & Random Number Generator	✓		✓	✓	✓
TCSM [41]	CNN, Proxy re-encryption & Bilinear mapping	✓		✓		✓
FMIR [42]	CNN & Euclidean Distance	✓		✓		✓
TDHPPIR [43]	CNN based Hash	✓				✓
Proposed Scheme	PHE & Partial Image Encryption		✓	✓	✓	✓

put forward in [30] to retrieve features from images after encryption using the Image Plane Encoding algorithm with the most significant bit (MSB) and converting images into matrices. A cloud-assisted efficient and privacy-preserving CBIR (EPCBIR) technique was suggested in [31]. The authors based their scheme on LSH and kNN algorithms for indexing and image feature security respectively. While their scheme provides a ranked-based image searching scheme, it calls for high computational resources. For the encryption and security of images and their pertinent attributes, the approach in [44] employs the same LSH and kNN algorithms as [31].

The authors in [32] put forward a scheme for user privacy in outsourcing image data using K-means for the generation of indices. An encrypted images-based secure retrieval scheme was presented in [33] where index generation and content based searching is carried out at CSP by carrying out Discrete Cosine Transform (DCT). Yuan *et al.* proposed a Secure and Efficient Encrypted Image Search with Access Control (SEISA) in [45]. The scheme, based on Locality-sensitive hashing (LSH) K-nearest neighbors (kNN) algorithms, claims to be lightweight and provisions searching access control for image retrieval over cloud storage. Another scheme for privacy preservation CBIR for large-scale data over the cloud was discussed in PIC [34]. PIC enables users to search over encrypted images with efficient access controls defined by data owners. Encrypted image searching in the mobile cloud domain was discussed in [35].

A Privacy-preserving image search (PPIS) was presented in [36] for large-scale medical image data using a convolutional neural network (CNN). The authors claimed secure search queries and privacy preservation of image data. A novel scheme by Li *et al.* for cloud-connected image data in a multi-user environment, was presented in [41]. The authors used CNN for feature extraction, proxy re-encryption, and bilinear mapping to carry out encryption and searching of image data in their proposed model. Y. Duan *et al.* put forward a CNN-based retrieval scheme for medical image data [42]. The authors employed Euclidean distance for image features extraction and kNN to evaluate image similarity.

A scheme for partial image encryption for Internet of Things (IoTs) was initially proposed by Jang and Lee [46]. The proposed scheme was based on format-preserving encryption algorithms of FF1 and FF3-1. Hybrid schemes for image encryption are discussed in [47] [48]. A partial image encryption scheme for medical image data was proposed in [49] which incorporates Discrete Cosine Transform (DCT) along with the encryption algorithm. Panduranga and Naveenkumar [50] put forward a selective encryption methodology for securing

satellite and medical images. Partially encrypting RGB image data with pixel position modification based on the region of interest is presented in [51]. It claimed security features of partial encryption and the scheme partially reconstructs the images. The scheme also offers the storage of encrypted data indefinitely using the SMART (Self Monitoring Analysis and Reporting Technology Copyback) method. In [52], the design and implementation of a system that uses a dynamic privacy-preserving partial image sharing technique (PUPPIES) was proposed. The scheme allows data owners to specify specific private regions (e.g. face, SSN number) in an image and to set different privacy policies for each user as a result. A novel scheme for partial image encryption of medical media data was discussed in [53]. A variety of partially encrypted images were obtained by altering the DNA patterns of a chaotic DNA sequence and performing DNA addition. Various partial image encryption techniques are discussed in [54] for smart cameras and in [55] for wireless multimedia sensor networks.

Some of the existing schemes for image-based searching are given in table I. It is evident from the table that while some existing image based schemes [25], [26], [28], [34] and [36] are based on homomorphic cryptosystems, they neither operate on partial images nor do they offer the feature of probabilistic trapdoors. Moreover, the schemes that are dealing with partial image encryption [46], [49], [50], [52]–[55] are based on non-homomorphic schemes without probabilistic trapdoors. To the best of our knowledge, no existing schemes deal with partial image processing, and provides homomorphic searchable encryption with probabilistic trapdoors. This further highlights the claim that the scheme presented in this research is a novel development in the case of partial image encryption technique based on homomorphic encryption and enables searching over the cloud with no threat to data security or privacy.

Algorithms for object detection can be classified on the basis of their approach *i.e.* machine learning and deep learning; as well as their stages *i.e.* single and dual stage detection. Dual stage detection implies object location and classification. Different object detection algorithms are discussed in [56] [57]. The development of YOLO version 4 has reevaluated the performance and accuracy of object detection. It is based on the CSPDarkent53 architecture. Spatial pooling is utilised in the backbone to enhance receptiveness and to locate the necessary characteristics of data images/video frames [58]. It boasts of a lesser requirement of storage and computational time. YOLO v5 was released not long after YOLO v4 with 4 different models having different accuracy levels. However, YOLO v4 is by far considered the fastest real-time model for object detection to date.

III. Preliminaries

A. Paillier Homomorphic Cryptosystem

In 1999, Paillier cryptosystem [59] was proposed by Pascal Paillier with features of asymmetric probabilistic encryption and additive homomorphic property. This partial homomorphic encryption scheme is IND-CPA secure. The basic structure of the Paillier cryptosystem consists of the following three phases: *i.e.* key pair generation, encryption, and decryption.

1) **Key Pair Generation:** It consists of computing n by $n = pq$ and $\lambda = lcm(p-1, q-1)$ where p and q are two independent large prime numbers. A generator g is then selected such that $g \in Z^*_{n^2}$; with order of g being a multiple of n *i.e.* $gcd(n, \lambda) = 1$. The key pair are secret key = (p, q) and public key = (n, g).
2) **Encryption:** A random integer $r \in Z^*_n$ is chosen such that $r < n$ and a message $m \in Z_n$ is encrypted by: $E(m) = g^m.r^n \ mod \ n^2$
3) **Decryption:** A ciphertext c_T is decrypted by taking discrete logarithm of $c^\lambda \in Z_n$ to obtain λ. Since $gcd(n, \lambda) = 1$, thus inverse $\lambda^{-1} \ mod \ n$ is calculated to retrieve message m.

IV. System Model

A. Network Model

The network model comprises of three entities *i.e.* an autonomous vehicle, data owner and a cloud server (CS). The autonomous vehicle, while on road, generates a lot of data through its cameras and sensors; and responds accordingly. The data generated through the mounted camera can be stored locally or transmitted at run time to the owner where it is processed and encrypted before being outsourced to CS. The term 'images/ image data' here refers generally to all footage / video frames / images etc. The network model, however, deals with the secrecy and storage of image data as well as capability of an owner to securely search over encrypted image files. The system flow diagram is shown in figure 2.

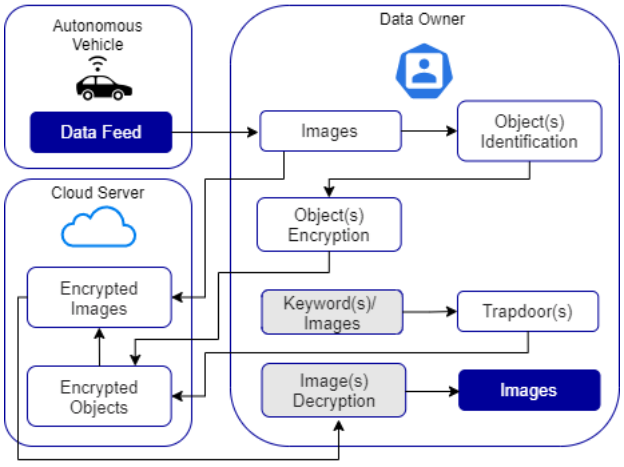

Fig. 2. System Flow Diagram

The owner is the entity that, upon receiving the data, encrypts all images using a standard encryption algorithm such as Advanced Encryption Standard (AES) and stores them on CS. The scheme also processes the images for object identification and classification based on image processing techniques such as YOLO v4 whereas encryption of image objects at the pixel level is carried out by Paillier homomorphic encryption. All those encrypted objects are then outsourced to the CS. Any user can request access to any image through a trapdoor generated by a specific query and can decrypt the

image provided he has the secret key. The user can also be the data owner in the proposed case. A trapdoor is generated by Paillier homomorphic scheme when a user inputs a query image object and requests an image containing that particular object. The CS carries out the search and returns a set of encrypted image(s) containing the encrypted object. The user/data owner can decrypt the encrypted image(s) with the secret key to retrieve the original image. Figure 3 represents different phases of proposed scheme. Figure 3 (a) presents the image encryption phase whereas figure 3 (b) exhibits the image decryption phase. Figure 3 (c) shows the object(s) encryption where the detected objects in an image, are pixelated and pixel values are encrypted by Paillier Homomorphic Encryption after flatting their RGB values. Figure 3 (d) shows the trapdoor generation from an image where the exact same process is carried out as figure 3 (c). However, in the case of trapdoor generation, for the same object, the query yields a different set of encrypted pixel values of trapdoor as the searched object(s).

B. Threat Model

The threat model is established with 2 entities *i.e.* data owner/user and CS, where data is images in the proposed case. An adversary's main aim is to gain unauthorized access to images stored on CS. Since all the communication between the owner and CS is carried out via a public channel, an adversary can easily intercept and launch attack(s) to uncover the underlying data. An adversary in the proposed case could be an outsider or the *honest but curious* CS with the following capabilities/conditions:

- Only passive attacks can be launched by the CS to analyse data or to follow network activity to detect any data or information that might be linked to the encrypted content of images outsourced to the CS.
- Only a polynomially limited number of operations *i.e.* encryption, decryption and / or passive attacks *etc.* may be performed by the attacker. The adversary is not permitted to make a limitless number of attempts or deduce the actual image in an unlimited amount of time.
- The adversary can track the past search queries, search results, and the communication pattern of data owner with CS, and can utilize this information to its advantage.

C. Assumptions

In this research, the following assumptions are made:

- The image feed generated by the autonomous automobile is communicated to the data owner over a secure channel that can not be intercepted by any adversary.
- The owner is presumed to be completely trustworthy and poses no harm to the system's security.

D. Security Goals

Following security goals are established for this research:

- Search pattern hiding, trapdoor unlinkability and mitigating distinguishability attacks: Search pattern refers to the leakage associated with the search queries. It reveals to the adversary if the same object is being searched repeatedly. This requires to have probabilistic / randomized trapdoors to prevent distinguishability attacks.
- Adaptive Security: In the known ciphertext model, the scheme should be proven secure. This means that the CS should not be able to extract anything about the query terms, even if they are aware of the history of previously searched trapdoors in an adaptive adversarial model.
- Secure Trapdoor Generation: Only an authorized person having the correct secret keys should be able to generate a meaningful trapdoor.

V. Security Definitions

In this section, the searchable encryption security definitions are revisited to establish the security of the proposed scheme. These definitions are aligned with the definitions proposed in [60] which are widely accepted and employed in case of probabilistic trapdoor-based searchable encryption schemes.

SD_1: Object - Trapdoor Indistinguishability

Object - Trapdoor Indistinguishability is defined as the process of searching carried out by encrypted trapdoors generated by unencrypted queries. For every query, a trapdoor is generated which is randomized and probabilistic such that the same query being searched twice will yield two trapdoors entirely different from each other and no trapdoor will reveal any information about the underlying query. An adversary $\mathcal{A}$ is unable to distinguish between the trapdoors even if provided with an adaptive history of queries and their associated trapdoors. To forecast contextually relevant query information, the adversary $\mathcal{A}$ must perform a large number of operations in polynomial time and record large amounts of data.

Let $KeyGen, Enc_s, Enc, TrG, SearchOut, Dec$ be a partial image-based homomorphic searchable encryption scheme over a set of images Img_i, image objects I_{obj_i}, query image object Q_{obj_i} security parameter λ and adversary $\mathcal{A}$ over *'N'* number of image objects respectively. A probabilistic experimental function is as follows:

$$
\begin{aligned}
&(k_s, k_p) \leftarrow KeyGen(primebits)\\
&\mathrm{E}_{Img_i} \leftarrow Enc_s(Img_i, k_s)\\
&\mathrm{E}_{obj_i} \leftarrow Enc(k_p, I_{obj_i})\\
&for\ 0 < i < N:\\
&(s_{\mathcal{A}}, Q_{obj_i}) \leftarrow \mathcal{A}(s_{\mathcal{A}}, T_{obj_1}, T_{obj_2}, ...T_{obj_i})\\
&T_{obj_i} \leftarrow TrG(Q_{obj_i}, k_p)\\
&a \leftarrow \{0,1\};\\
&(s_{\mathcal{A}}, Q_{obj_0}, Q_{obj_1} \leftarrow \mathcal{A}(k_s, k_p)\\
&T_{obj_a} \leftarrow TrG(Q_{obj_i}, k_p)\\
&a' \leftarrow \mathcal{A}_{N+1}(s_{\mathcal{A}}, T_{obj_a})\\
&T_{obj'_a} \leftarrow TrG(Q_{obj_j}, k_p); j \in N\\
&if a' = a;\ output\ 1;\\
&otherwise\ output\ 0
\end{aligned}
$$

where $s_{\mathcal{A}}$ shows the adversary $\mathcal{A}$'s state. The scheme is said to be secure with respect to Object-Trapdoor Indistinguishability if the following hold true.

$$Pr[Obj\_Trap_{\mathcal{A}}(\lambda) = 1] \leq \frac{1}{2} + ngl(\lambda)$$

SD_2: Trapdoor-Image Indistinguishability

The complexity of a homomorphic-based searchable encryption protocol is related to trapdoor-image indistinguishability. The queries, trapdoors, and associated object searching should be complicated enough that the trapdoor does not reveal any information about the associated image objects before the search. As a result, even if the history (query, trapdoor, image object) is created adaptively, the trapdoor should be indistinguishable when the same search term appears again. Furthermore, a minute change occurring in the query should significantly alter the trapdoor and thus, the searching over it should yield an altogether different result than before and vice versa. An adversary should not be able to predict the trapdoor leading to the retrieved image from the list of encrypted objects. Thus, query security and user's privacy are ensured throughout in an adaptive adversarial model.

Let $KeyGen, Enc_s, Enc, TrG, SearchOut, Dec$ be a partial image-based homomorphic searchable encryption scheme over a set of images Img_i, image objects I_{obj_i}, security parameter λ and adversary $\mathcal{A}$ over *'M'* number of images respectively. A probabilistic experimental function is as follows:

$(k_s, k_p) \leftarrow KeyGen(primebits)$
$\mathrm{E}_{Img_i} \leftarrow Enc_s(Img_i, k_s)$
$\mathrm{E}_{obj_i} \leftarrow Enc(k_p, I_{obj_i})$
$for\ 0 < i < M:$
$(s_{\mathcal{A}}, T_{obj_i}) \leftarrow \mathcal{A}(s_{\mathcal{A}}, Img_1, Img_2, ...Img_i)$
$Img_i \leftarrow SearchOut(E_{obj_i}, T_{obj_i})$
$a \leftarrow \{0, 1\};$
$(s_{\mathcal{A}}, T_{obj_0}, T_{obj_1} \leftarrow \mathcal{A}(Img_i, k_p)$
$Img_a \leftarrow searchOut(E_{obj_a}, T_{obj_a})$
$a' \leftarrow \mathcal{A}_{N+1}(s_{\mathcal{A}}, Img_a)$
$T_{obj'_a} \leftarrow TrG(Q_{obj_j}, k_p); j \in N$
$if a' = a;\ output\ 1;$
$otherwise\ output\ 0$

where $s_{\mathcal{A}}$ shows the adversary $\mathcal{A}$'s state. The scheme is said to be secure with respect to Trapdoor-Image Indistinguishability if the following hold true.

$$Pr[Trap\_Img_{\mathcal{A}}(\lambda) = 1] \leq \frac{1}{2} + ngl(\lambda)$$

VI. Proposed Methodology

The image searching algorithm is twofold where an object is identified using an image detection algorithm such as YOLO v4. The image is then encrypted with standard encryption such as Advanced Encryption Standard (AES). The proposed scheme uses twofold encryption such that AES is employed in the scheme for image data encryption, to increase the efficiency and performance by reducing the storage and computation overhead. Whereas Paillier homomorphic encryption is carried out over the image object(s) and trapdoors, to introduce highly secure primitives to enable searching over the encrypted data. The object(s) identified are converted to pixels and these pixel values are then encrypted using Paillier homomorphic encryption scheme. The image search is based on those encrypted image objects. The notations and abbreviations used in the definitions and algorithms are mentioned in table II. The proposed scheme consists of the following phases:

TABLE II
Notations and Abbreviations

Ntn. / Abb.	Explanations
CS	Cloud server
Enc(), Dec()	Encryption and decryption function
p, q	Prime numbers
primebits	Number of bits
k_p, k_s	Public Key and Secret (private) Key
GCD()	Greatest common divisor function
LCM()	Least common multiple function
glambda (λ)	λ = LCM(p-1,q-1)
gmu (μ)	Modular Multiplicative Inverse
RN()	Returns a random number
getprime()	Returns the N-bit prime number
S_{ub}	Subtraction function
S_a	Results of the Subtraction function
R_V	Result dictionary containing Obj IDs & S_a
T_{obj_i}	Trapdoor image object
Q_{obj_i}	Query image object
I_{obj_i}	Image object(s)
E_{Img_i}	Encrypted Image(s)
E_{obj_i}	Encrypted Object(s)
E_{F_i}	Encrypted File(s)
D_{Img_i}	Decrypted Image

1) **Key Generation** $(k_s, k_p) \leftarrow KGen(primebits)$**:** It is a probabilistic algorithm that returns a Public Key and Secret (Private) Key based on key pair generation phase of Paillier cryptosystem [59]. The algorithm takes as input a parameter of primebits which determine the number of bits for generating a prime number. The algorithm returns a k_s and k_p. The input parameter "primebits" is used to generate two random prime numbers p & q independent of each other, through which k_s and k_p is generated. The k_s is kept secret and is used for decryption, whereas the k_p can be shared and is used for encryption.

Algorithm 1 Key Generation $(k_s, k_p) \leftarrow KGen(primebits)$

Generate p = getprime (primebits,RN)
Generate q = getprime (primebits,RN)
Let $n = p * q$
while $g = RN();\ GCD(g, n^2) \neq 1$ **do**
  Compute λ = LCM (p-1,q-1)
  Compute Modular Multiplicative Inverse:
  $\mu = (L(g^{\lambda}) mod n^2)^{-1} mod\ n$
  Compute: $l = (pow(g, \lambda, n^2) - 1)/n$
  Calculate: $gmu = libnum.invmod\ (l, n)$
end
return k_s = (λ, μ), k_p = (n, g)

2) **Image Encryption** $E_{Img_i} \leftarrow Enc_s(Img_i, k_s)$**:** The images Img_i are encrypted by AES using secret key k_s and returns encrypted images E_{Img_i}.
3) **Object Encryption** $E_{obj_i} \leftarrow Enc(k_p, I_{obj_i})$**:** This phase, first identifies the objects Obj_i available in images Img_i, and returns the object class name and then encrypts those image objects. The encryption process is based on encryption phase of Paillier cryptosystem

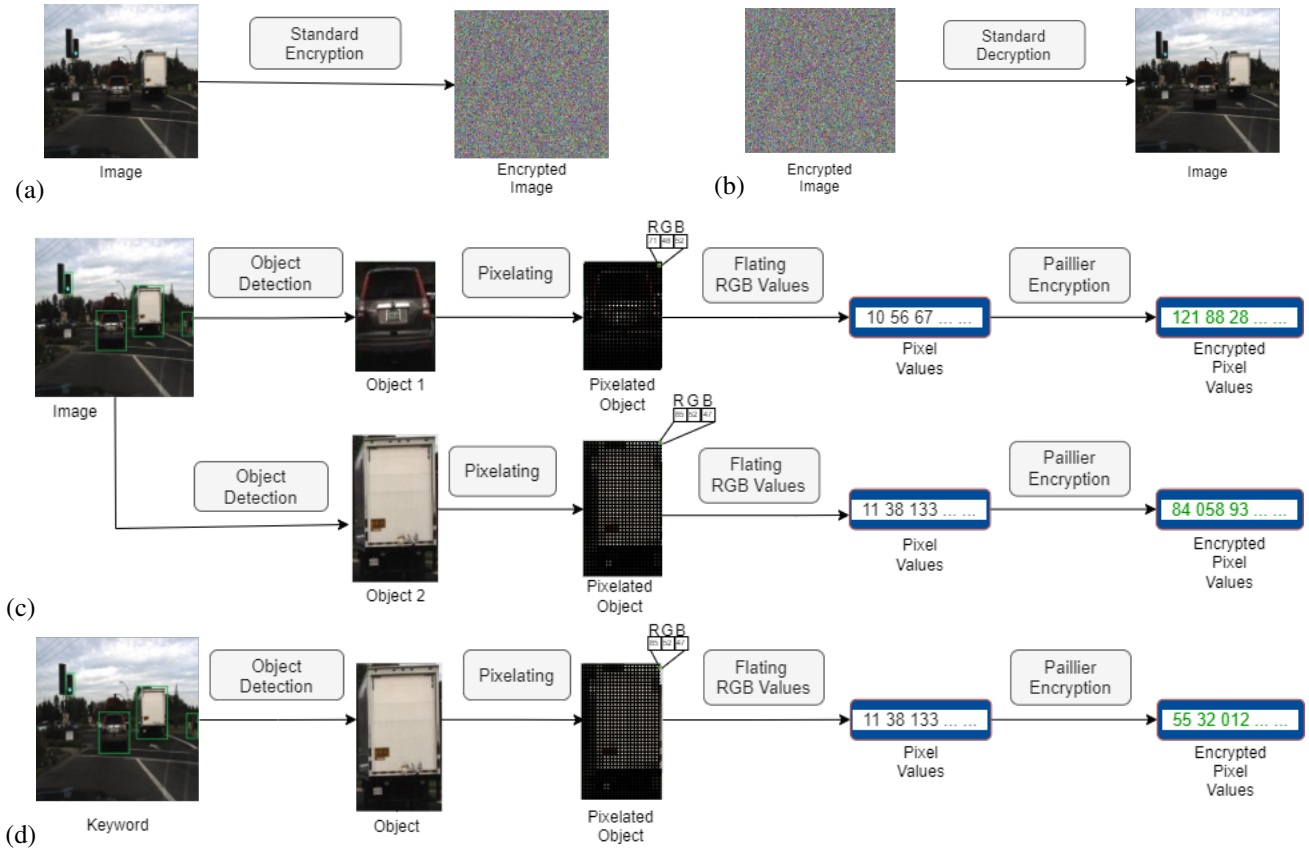

Fig. 3. The Proposed Scheme (a) Image Encryption (b) Image Decryption (c) Object(s) Encryption (d) Trapdoor Generation

Algorithm 2 Image Encryption $E_{Img_i} \leftarrow Enc_s(Img_i, k_s)$

for $i \leftarrow 0$ **to** *M; M are number of images* **do**
  $Enc_s(Img_i, k_s) = E_{Img_i}$
end
return E_{Img_i}

[59] where ciphertexts are generated by an encrypting image objects I_{obj_i} using public key k_p in a *for loop* using *pow() function*. The power function is a simple exponential that will raise the input parameters i.e. g, Obj_i, n^2 to yield the encrypted objects E_{Obj_i}.

Algorithm 3 Object Encryption $E_{obj_i} \leftarrow Enc(k_p, I_{obj_i})$

for $i \leftarrow 0$ **to** *N; N are the number of objects* **do**
  for $i \leftarrow 0$ **to** Obj_i **do**
    Enc $(g^{I_{obj_i}}.r^n)$ % n^2
    E_{Obj_i} = $pow(g, Obj_i, n^2)$
    E_{F_i} = write (E_{Obj_i})
  end
end
return E_{F_i}

4) **Trapdoor Generation** $T_{obj_i} \leftarrow TrG(k_p, Q_{obj_i})$**:** This phase takes a query as input where the query is in the form of an image object. A trapdoor T_{obj_i} is generated by object identification of the query image and encryption of that object Q_{obj_i} using public key k_p in a *for loop* using *pow() function*. The encrypted value of trapdoor will be different for every instance if the same object is encrypted again such that $E_{Obj_i} \neq E'_{Q_{obj_i}}$ if the underlying object is same. The algorithm for generation of trapdoors is based on encryption phase of Paillier cryptosystem [59].

Algorithm 4 Trapdoor Generation $T_{obj_i} \leftarrow TrG(k_p, Q_{obj_i})$

for $i \leftarrow 0$ **to** *K; K are the number of objects pixels* **do**
  Enc $(g^{Q_{obj_i}}.r^n)$ % n^2
  $E'_{Q_{obj_i}}$ = $pow(g, Q_{obj_i}, n^2)$
  T_{obj_i} = write $(E'_{Q_{obj_i}})$
end
return T_{obj_i}

5) **Search Out** $E_{Img_i} \leftarrow SearchOut(E_{obj_i}, T_{obj_i})$**:** The searching algorithm takes a set of encrypted files E_{obj_i} and a trapdoor T_{obj_i} as input. Firstly, the trapdoor T_{obj_i} is subtracted from the E_{obj_i} pixel by pixel through the subtraction function S_{ub}; the values are then accumulated as S_a. A result dictionary R_V containing S_a values and encrypted objects' IDs is sent to the user. The user decrypts the R_V values and occurrence of zero corresponds to a match *i.e.* requested image being stored over cloud. The user then requests explicitly with the image's ID with respect to the object's ID mapping and the corresponding E_{Img_i} is sent over to the user by

CS.

Algorithm 5 Search Out $E_{Img_i} \leftarrow SearchOut(E_{obj_i}, T_{obj_i})$

for $i \leftarrow 0$ **to** E_{F_i} **do**
  $S_a = S_{ub}(T_{I_i}, E_{F_i})$;
  $R\_V = \sum_{a=1}^{i} S_a$
end
return *R_V*
At User's End:
for $y \leftarrow 0$ **to** R_V **do**
  if Dec $(R\_V_y, k_s).get(R\_V_y) == 0$
  $E_{Img_i} = getImage(R\_V_y)$
end
return E_{Img_i}

6) **Image Decryption** $Img_i \leftarrow Dec(E_{Img_i}, k_{aes})$**:** It is the decryption process where user decrypts the encrypted image E_{Img_i} retrieved from CS with private AES key k_{aes} and gets the original image data Img_i.

Algorithm 6 Image Decryption $Img_i \leftarrow Dec(E_{Img_i}, k_{aes})$

for $i \leftarrow 0$ **to** *N; N are number of encrypted images* **do**
  $Dec\ (E_{Img_i},\ k_{aes})$ = D_{Img_i}
end
return Img_i

A. Correctness

The correctness of a scheme specifies that decryption of a homomorphic evaluation on a ciphertext must be identical to evaluation on the underlying plaintext message. Thus, the proposed scheme is deemed correct if the security parameters (g, λ, μ) and key pair k_p, k_s for encrypted image objects E_{Obj_i} by $Enc(k_p, Obj_i)$, the searching by trapdoors T_{I_i} always results in return of corresponding image objects present. The following conditions are met in the proposed scheme with significant probability:

- For $Q_{obj_i} \in I_{Obj_i}$;

$$SearchOut\ (k_p, T_{obj_i}, E_{obj_i}) = I_{Obj_i} \cap Dec(k_s, R\_V) = I_{Obj_i}$$

- For $Q_{obj_i} \notin I_{Obj_i}$;

$$SearchOut\ (k_p, T_{obj_i}, E_{obj_i}) = I_{Obj_i} \cap Dec(k_s, R\_V) = 0$$

B. Soundness

The soundness of a scheme entails that the searching phase of a homomorphic evaluation on an encrypted query must be identical to the evaluation on the underlying keyword and produce sound encrypted results. A scheme is considered sound if the security parameters (g, λ, μ) and key pair k_p, k_s for encrypted image objects E_{Obj_i} by $Enc(k_p, Obj_i)$, the searching by trapdoors T_{I_i} never produce false positives and always produce substantial search outcomes. The following conditions are met in the proposed scheme with significant probability:

- For $Q_{obj_i} \in I_{Obj_i}$;

$$SearchOut\ (k_p, T_{obj_i}, E_{obj_i}) = 1$$

- For $Q_{obj_i} \notin I_{Obj_i}$;

$$SearchOut\ (k_p, T_{obj_i}, E_{obj_i}) = 0$$

VII. Security Analysis

This section presents a game-based approach to verify the security of the scheme.

Game 1: Object-Trapdoor Indistinguishability: Suppose that there are many query objects such that Q_{obj_1}, Q_{obj_2},... Q_{obj_i} in the image data Img_i. The game between an adversary and a challenger constitutes of the following three phases:

- *Query Phase:* The challenger initiates the process by generating multiple encrypted image objects' trapdoors against image data Img_i. The adversary sends a query object Q_{obj_i} and challenger returns the encrypted trapdoor T_{obj_i}. This process continues until the adversary has accumulated polynomial many query object-trapdoor pairs.
- *Challenge Phase:* The adversary chooses two query objects Q_{obj_a} and Q_{obj_b} and sends them over to the challenger. The challenger after tossing a fair coin $a \leftarrow \{0, 1\}$; generates trapdoor T_{obj_a} for Q_{obj_a} and sends it to the adversary.
- *Outcome Phase:* The adversary has to make a correct guess of query object associated to the received trapdoor *a* or *b* with a probability of higher than 1/2 to win the challenge otherwise the scheme is said to be secure with respect to Object-Trapdoor Indistinguishability.

The proposed scheme's phases of key generation, object encryption, and trapdoor generation are based on Paillier cryptosystem's key generation and encryption phases respectively. The proposed scheme yields different encrypted image objects by probabilistic encryption and generates a different trapdoor for the same query on every repetition. The mapping of a trapdoor to an encrypted image object is carried out over a probabilistic searching algorithm leaving the adversary $\mathcal{A}$ with no possible means to correctly guess the underlying image and/or image objects from an encrypted retrieved result. It is also not possible for an adversary $\mathcal{A}$ or CS to guess or predict the search pattern. Thus, due to the probabilistic trapdoors, the proposed scheme fulfills the security definition SD_1.

Game 2: Trapdoor-Image Indistinguishability: Suppose there are many query objects such that T_{obj_1}, T_{obj_2},... T_{obj_i} in the image data Img_i. The game between an adversary and a challenger constitutes of the following three phases:

- *Query Phase:* The challenger initiates the process by generating multiple encrypted image objects against image data Img_i. The adversary sends an encrypted trapdoor T_{obj_i} and challenger returns the corresponding image. This process continues until the adversary has accumulated polynomial many trapdoor-image pairs.

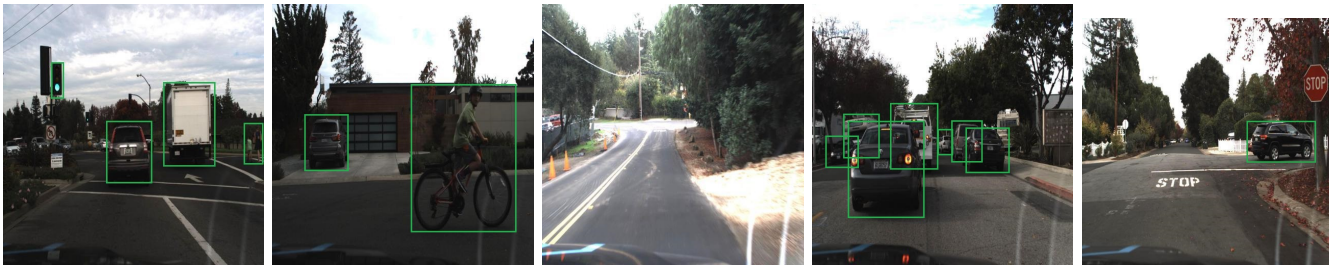

Fig. 4. Multiple Images from Dataset Representing the Presence of Non-uniform Objects

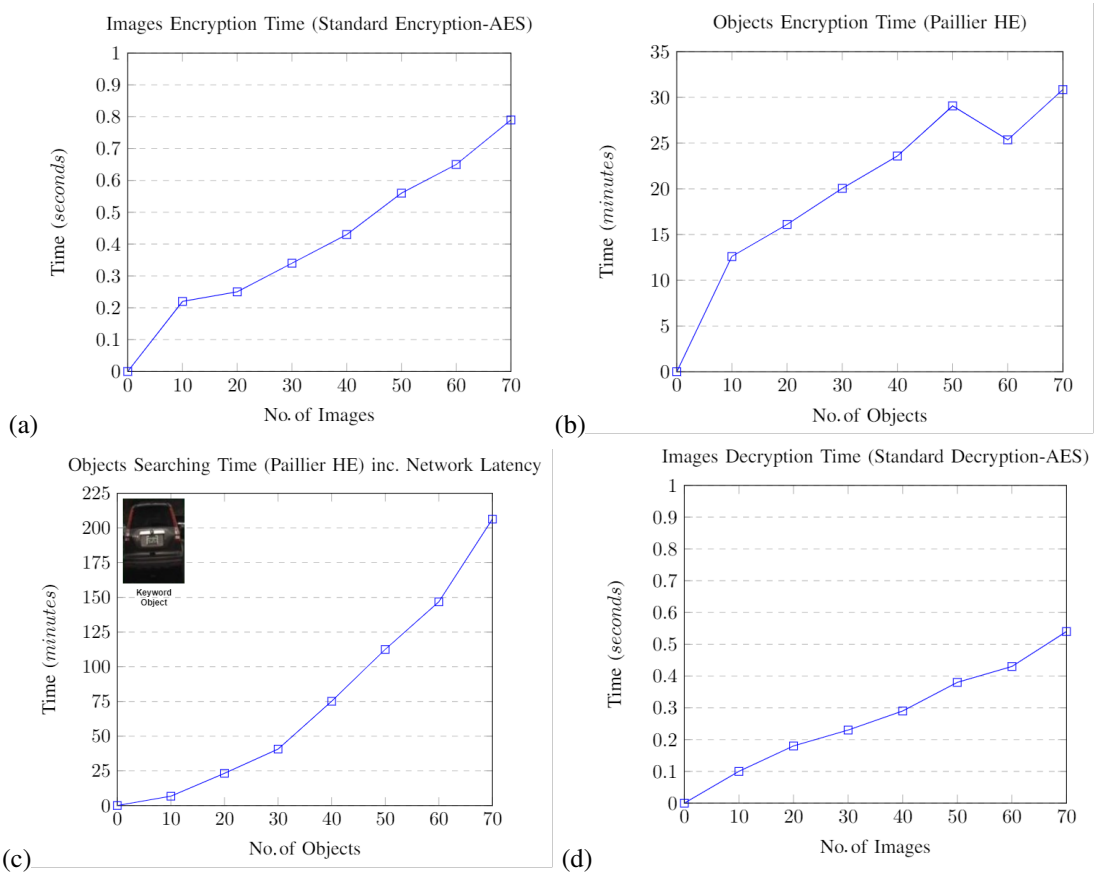

Fig. 5. (a) Image Encryption Time (Standard Encryption-AES) (b) Object Encryption Time (Paillier Homomorphic Encryption) (c) Object Searching Time (Paillier Homomorphic Encryption) including Network Latency (d) Image Decryption Time (Standard Decryption-AES)

- *Challenge Phase:* During the challenge phase, the adversary chooses two new trapdoors T_{obj_a} and T_{obj_b} and sends them over to the challenger. The challenger after tossing a fair coin $a \leftarrow \{0,1\}$; carries out searching among the encrypted image, selects a E_{Obj_a} and sends it to the adversary.
- *Outcome Phase:* The adversary has to make correct guess of image where it was the search result of trapdoor *a* or *b* with a probability of higher than 1/2 to win the challenge otherwise the scheme is said to be secure with respect to Trapdoor-Image Indistinguishability.

Searching in the proposed scheme is carried out at the pixel level of images. This implies that two seemingly identical images with a difference of only one pixel will not be matched and only exact search results will be returned to the user. Prior to the search, it is difficult for an adversary $\mathcal{A}$ to create a link between the query images, trapdoors and search outcomes. This is also true even if the adversary $\mathcal{A}$ keeps a track of the search history and its results. Therefore, the chance of predicting the right outcome of an adversary $\mathcal{A}$ is less than 1/2 since the object queries to trapdoors are produced using probabilistic encryption and each encrypted trapdoor is unique. Hence, the proposed scheme fulfils security definition SD_2.

In a typical model, it is assumed that the attack is initiated by adversary $\mathcal{A}$, thus the adversary is not restricted by substituting any weak structure for the proposed method. The information that is exposed within polynomial time is the focus of the leakages described below:

- Leakage L_1: It is associated with data stored on CS. *i.e.* number of encrypted images and number of encrypted

image objects. All image data outsourced on CS is stored after encryption so the CS can have no information about the underlying plaintexts but only about the number of files being stored on it.

$$L_1 = \begin{Bmatrix} E_{Img_i}, E_{obj_i}, (number\ of\ E_{Img_i}), \\ (number\ of\ E_{Obj_i}) \end{Bmatrix}$$

- Leakage L_2: It is associated with the generation of trapdoors from queries. The trapdoor is probabilistically generated by Paillier encryption and reveals no information about the underlying query image object.

$$L_2 = \left\{((g^{Q_{obj_i}}) * (r^n))(mod n^2)\right\}$$

- Leakage L_3: It is associated with the proposed scheme's search outcome. The searching is carried out at CS and its results are accessible to all entities including CS, data owner as well as adversary $\mathcal{A}$. The search outcomes are encrypted results of a subtraction operation and can only be decrypted by the data owner (in possession of the secret key) and reveal no information about the underlying search queries or image objects.

$$L_3 = \left\{S_{ub}(T_{obj_i}, E_{obj_i}), (R\_V)\right\}$$

The assumptions and leakages described above are interconnected and interdependent. As a result, to achieve the highest level of security, it is required that all security assumptions are scrupulously observed. Furthermore, none of the leakages are giving away the plaintext or any information about the characteristics of plaintext; therefore the proposed scheme strengths and align with the security definitions. Also, such a scheme can be called as a privacy-preserving searchable encryption scheme as per the Corollary 1 presented in [60].

VIII. Performance Analysis

The simulations were carried out in a client-cloud scenario where the standard encryption/ decryption (AES in this case) of images, Paillier homomorphic encryption for image objects is carried out at client's end and Paillier homomorphic encryption searching is done over at CS.

A. System Specification

- **Client Side:** OS Ubuntu 18.04.5 LTS (64 bits) with 16 GB RAM, Intel Core i7-7700 CPU @ 3.6 GHz x 8 and 1 TB SSD storage.
- **Server Side:** Contabo Cloud Platform running an operating system Ubuntu 20.04 with CPU having 10 vCPU Cores, 60 GB RAM, 1.6 TB SSD storage, 1 Gbit/s port and data transfer rate of 32 TB traffic (100 Mbps).

B. Dataset Description

The images were taken from dataset [61]. The dataset, shared by Roboflow in April 2020, has been generated by a webcam mounted on a car with video frames from its feed treated as images. The data set contains more than 15000 images and labels of objects include car, truck, pedestrian, traffic lights etc. Object detection was carried by YOLO v4 on Google Colab. The images are diverse and non-uniform as evident from figure 4, with some having multiple detectable objects, some having objects far away from the detection range, some objects out of the car's driveway and some having no detectable object.

C. Performance Metrics

To measure the performance of the proposed scheme, tests were conducted over a total of 70 images. Figure 5 (a) represents the graphical representation of the results of standard encryption that was AES encryption of image data in proposed scheme. The encryption was performed by the client in iterations of 10 images to plot results easily in graphical representation. The graph is plotted with iteration of 10 images on x-axis against time in seconds on y-axis. The image encryption takes a linear time with the increase in the number of images and takes 0.8 seconds to encrypt 70 images.

Figure 5 (b) shows the image objects encryption time using Paillier homomorphic encryption performed on the client side. The image objects encryption was also carried out at client's end. A graph is plotted with iteration of 10 objects on x-axis against time in minutes on y-axis. A slight non-uniformity is observed due to the non-uniformity of the number of objects within the dataset. This has already been highlighted in the dataset description. The dip in the graph is due to the non uniform presence of objects in the images as shown in figure 4. For a total of 70 objects, the proposed scheme takes a total of 30 minutes. A trapdoor was generated by a query image of 85 Kbs in 21.23 seconds. The trapdoor was generated for the object "car" that has been shown within the 5 (c).

The object searching time is carried out on the Cloud Server. Since this is a true deployment, it also includes the network latency. As shown in 5 (c), a graph is plotted with the number of images over which the search is being conducted plotted on x-axis, and the time in minutes is plotted on the y-axis. The searching is the most resource intensive task that requires some alternative resources such as the cloud. This is in line with the proposed assumption of importance of connecting autonomous vehicles to the cloud and to further emphasize this, the cloud was configured to provide us with the minimum resources. It is observed that to search against the previously generated trapdoor, the time required is 205 minutes. It is acknowledged that the searching is consuming too much time which is by virtue of not incorporating any mechanisms to enhance the performance such as multi-core processing and parallel threading (that will be done in the future). Figure 5 (d) shows the results of AES decryption of image data with the number of images on x-axis and time in seconds on the y-axis. The slope of which is linear, i.e. for 70 images the decryption time is approximately 0.55 seconds.

D. Performance Complexity

The computational overhead is discussed with regard to different phases (i.e. Key Generation, Image Data Encryption, Trapdoor Generation, Searching, and Decryption Phase) of the proposed scheme. For each algorithm, the asymptotic notations are represented where the analysis is based on an upper bound

TABLE III
COMPLEXITY COMPARISON

Phases	Proposed Scheme	[37]	[41]	[42]
Key Generation	$\mathcal{O}(2^{\lambda})$	$\mathcal{O}(2^{\lambda+1})$	$(2^{\lambda+1})$	$\mathcal{O}(2^{\lambda})$
Image Encryption	$\mathcal{O}(M)$	$\mathcal{O}(2M+1)$	$\mathcal{O}(M^2)$	$\mathcal{O}(M^2+1)$
Object Encryption	$\mathcal{O}(N.K)$	-	-	-
Index Generation	-	-	$\mathcal{O}(8M.S^2)$	$\mathcal{O}(4M.S^2)$
Trapdoor Generation	$\mathcal{O}(K+1)$	$\mathcal{O}(D.F+1)$	$\mathcal{O}(8S^2)$	$\mathcal{O}(4S^2)$
Searching	$\mathcal{O}(M.N.K)$	$\mathcal{O}(M(M-1))$	$\mathcal{O}(4.M.S)$	$\mathcal{O}(4.C.S^2+2.C.S)$
Image Decryption	$\mathcal{O}(M)$	$\mathcal{O}(2M+1)$	$\mathcal{O}(M^2)$	$\mathcal{O}(M^2+1)$

M = total number of images, N = total number of objects, K = image pixels,
S = number of images in each class, C = CNN input matrix of order c x c

analysis of the set of images and image objects. The complexity for the Key Generation phase is $\mathcal{O}(2^{\lambda})$ for the proposed scheme. Complexity for Image encryption and decryption is same for proposed scheme i.e. $\mathcal{O}(M)$. The scheme proposed in this research follows object encryption having complexity $\mathcal{O}(N.K)$. Complexity of Trapdoor generation algorithm and searching in proposed scheme is $\mathcal{O}(K+1)$ and $\mathcal{O}(M.N.K)$ respectively. A comparison of computational complexity is presented in table III.

E. Performance Enhancements

The simulations were carried out on the proposed scheme with comparison against generic Paillier-based homomorphic searchable encryption scheme [59] for 1 image containing 1 object as been shown within the 5 (c). The proposed scheme consists of image encryption and decryption by AES, object encryption and searching by Paillier homomorphic encryption and decryption of images is by carried out via AES. The AES encryption and decryption time for 1 image was carried out in 0.025 and 0.021 seconds respectively. The 2.55 MB sized image was compressed to 770 Kbs after AES encryption and format was changed from 'jpeg' to 'png' to retain its original features. The size of object detected from the image was 146 Kbs and was increased to 1.79 MB after Paillier encryption. Object encryption and searching by Paillier encryption was carried out in 21.68 and 21.04 seconds respectively. The overall storage overhead of the proposed scheme comes out to be 2.54 MB and takes up a total of 42.766 seconds.

The encryption, searching and decryption of same image of 2.55 MB by Paillier based homomorphic searchable encryption scheme, took 633.03, 263.31 and 507.11 seconds respectively. The storage overhead in this case came out to be 49.496 MB. The total time for the execution of this scheme was calculated to be 1403.45 seconds. By this comparison, the proposed scheme reduces storage overhead by approximately 20 times and is nearly 33 times more efficient as compared to generic Paillier Homomorphic Encryption based searching scheme.

Another important requirement of the cloud is the change in the size of image object data before and after Paillier Homomorphic Encryption is performed. It can be seen in table IV that for 70 images, the unencrypted image data size is 8.1 MB which increases to 4.3 GB after encryption. The data size generated after encryption, and its local management and storage, can be a challenge. It is therefore necessary to make use of an externally hosted cloud system. In the future, we will also work on the compression of these encrypted images.

TABLE IV
SIZE COMPARISON OF IMAGE OBJECTS BEFORE AND AFTER ENCRYPTION WITH PAILLIER HOMOMORPHIC ENCRYPTION

No. of Objects	Unencrypted Image Objects Size	Encrypted Image Objects Size
10	2.8MB	261MB
20	4.8MB	808MB
30	5.4MB	1.3GB
40	6.3MB	2.1GB
50	7.3MB	2.7GB
60	7.0MB	3.6GB
70	8.1MB	4.3GB

IX. CONCLUSIONS AND FUTURE WORK

A novel partial image-based homomorphic scheme is proposed for preserving the privacy of data captured from autonomous vehicles. The proposed scheme allows search at the pixel level and uses Paillier homomorphic encryption. The generated search query/ trapdoor is also probabilistic, leading to maintaining indistinguishability. The proposed approach is therefore referred to as a privacy-preserving searchable encryption scheme. The implementation is deployed on a cloud environment "Contabo" and tested over a real-world data set. The proposed scheme reduces storage overhead by approximately 20 times and is nearly 33 times more efficient in performance compared to the generic Paillier homomorphic encryption-based searching scheme. The results also demonstrate the correctness of the scheme and highlight the requirement of connecting autonomous vehicles to a cloud environment, to achieve elevated levels of security and privacy. The efficiency of the scheme can be achieved by introducing parallel processing along with proposing mechanisms for compressing images to reduce the required storage. The proposed scheme involves human intervention for the encryption, searching, and decryption of the images. Although this research is pioneering, human involvement may be termed a dependency. In the future, we plan to shift towards edge/fog computing to increase the performance and enhance efficiency by making the vehicle an edge device so that the entity of the data owner is removed from the network model.

ACKNOWLEDGEMENT

This work was carried out by the "Information Security and Privacy Lab.", NUST, Islamabad, Pakistan supported by the National Centre for Cyber Security, Pakistan, under the project titled "Privacy Preserving Search over Sensitive Data Stored in the Cloud". This work was also supported in part by the UK

EPSRC “Sustainable urban power supply through intelligent control and enhanced restoration of AC/DC networks”, under Grant EP/T021985/1.

REFERENCES

[1] S. Cepni, M. E. Atik, and Z. Duran, “Vehicle detection using different deep learning algorithms from image sequence,” *Baltic Journal of Modern Computing*, vol. 8, no. 2, pp. 347–358, 2020.

[2] A. M. Khan, “Vehicle and pedestrian detection using yolov3 and yolov4 for self-driving cars,” Ph.D. dissertation, CALIFORNIA STATE UNIVERSITY SAN MARCOS, 1921.

[3] P. Silva, E. Monteiro, and P. Simoes, “Privacy in the cloud: A survey of existing solutions and research challenges,” *IEEE Access*, vol. 9, pp. 10 473–10 497, 2021.

[4]

[5] Y. Shen and S. Pearson, “Privacy enhancing technologies: A review,” *Hewlet Packard Development Company. Disponible en https://bit. ly/3cfpAKz*, 2011.

[6] M. Tebaa, S. El Hajji, and A. El Ghazi, “Homomorphic encryption applied to the cloud computing security,” in *Proceedings of the World Congress on Engineering*, vol. 1, no. 2012, 2012, pp. 4–6.

[7] T. Burghardt, E. Buchmann, and K. Böhm, “Why do privacy-enhancement mechanisms fail, after all? a survey of both, the user and the provider perspective,” in *Workshop W2Trust, in conjunction with IFIPTM*, vol. 8, 2008.

[8] F. Stalder, “The failure of privacy enhancing technologies (pets) and the voiding of privacy,” *Sociological Research Online*, vol. 7, no. 2, pp. 25–39, 2002.

[9] X. Yi, R. Paulet, and E. Bertino, “Homomorphic encryption,” in *Homomorphic Encryption and Applications*. Springer, 2014, pp. 27–46.

[10] Y. Iqbal, S. Tahir, H. Tahir, F. Khan, S. Saeed, A. M. Almuhaideb, and A. M. Syed, “A novel homomorphic approach for preserving privacy of patient data in telemedicine,” *Sensors*, vol. 22, no. 12, p. 4432, 2022.

[11] J. Liu, X. Li, Q. Jiang, M. S. Obaidat, and P. Vijayakumar, “Bua: A blockchain-based unlinkable authentication in vanets,” in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE, 2020, pp. 1–6.

[12] X. Li, J. Liu, M. S. Obaidat, P. Vijayakumar, Q. Jiang, and R. Amin, “An unlinkable authenticated key agreement with collusion resistant for vanets,” *IEEE Transactions on Vehicular Technology*, vol. 70, no. 8, pp. 7992–8006, 2021.

[13] F. Wei, S. Zeadally, P. Vijayakumar, N. Kumar, and D. He, “An intelligent terminal based privacy-preserving multi-modal implicit authentication protocol for internet of connected vehicles,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 3939–3951, 2020.

[14] O. Kocabas and T. Soyata, “Towards privacy-preserving medical cloud computing using homomorphic encryption,” in *Virtual and Mobile Healthcare: Breakthroughs in Research and Practice*. IGI Global, 2020, pp. 93–125.

[15] M. Tebaa, K. Zkik, and S. El Hajji, “Hybrid homomorphic encryption method for protecting the privacy of banking data in the cloud,” *International Journal of Security and Its Applications*, vol. 9, no. 6, pp. 61–70, 2015.

[16] S. Obla, X. Gong, A. Aloufi, P. Hu, and D. Takabi, “Effective activation functions for homomorphic evaluation of deep neural networks,” *IEEE Access*, vol. 8, pp. 153 098–153 112, 2020.

[17] S. Yaji, K. Bangera, and B. Neelima, “Privacy preserving in blockchain based on partial homomorphic encryption system for ai applications,” in *2018 IEEE 25th International Conference on High Performance Computing Workshops (HiPCW)*. IEEE, 2018, pp. 81–85.

[18] M. Azees, P. Vijayakumar, and L. J. Deboarh, “Eaap: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467–2476, 2017.

[19] P. Vijayakumar, M. Azees, A. Kannan, and L. J. Deborah, “Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015–1028, 2015.

[20] P. Vijayakumar, M. Azees, S. A. Kozlov, and J. J. Rodrigues, “An anonymous batch authentication and key exchange protocols for 6g enabled vanets,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 2, pp. 1630–1638, 2021.

[21] K. Chamili, M. J. Nordin, W. Ismail, and A. Radman, “Searchable encryption: A review,” *International Journal of Security and Its Applications*, vol. 11, pp. 79–88, 2017.

[22] Y. Wang, J. Wang, and X. Chen, “Secure searchable encryption: a survey,” *Journal of communications and information networks*, vol. 1, no. 4, pp. 52–65, 2016.

[23] C. Bösch, P. Hartel, W. Jonker, and A. Peter, “A survey of provably secure searchable encryption,” *ACM Computing Surveys (CSUR)*, vol. 47, no. 2, pp. 1–51, 2014.

[24] C.-Y. Hsu, C.-S. Lu, and S.-C. Pei, “Homomorphic encryption-based secure sift for privacy-preserving feature extraction,” in *Media Watermarking, Security, and Forensics III*, vol. 7880. International Society for Optics and Photonics, 2011, p. 788005.

[25] C. Y. Hsu, C. S. Lu, and S. C. Pei, “Image feature extraction in encrypted domain with privacy-preserving sift,” *IEEE Transactions on Image Processing*, vol. 21, no. 11, pp. 4593–4607, 2012.

[26] S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren, “Securing sift: Privacy-preserving outsourcing computation of feature extractions over encrypted image data,” *IEEE Transactions on Image Processing*, vol. 25, no. 7, pp. 3411–3425, 2016.

[27] Z. Qin, J. Weng, Y. Cui, and K. Ren, “Privacy-preserving image processing in the cloud,” *IEEE cloud computing*, vol. 5, no. 2, pp. 48–57, 2018.

[28] T. Yang, J. Ma, Q. Wang, Y. Miao, X. Wang, and Q. Meng, “Image feature extraction in encrypted domain with privacy-preserving hahn moments,” *IEEE Access*, vol. 6, pp. 47 521–47 534, 2018.

[29] Y. Zhu, X. Sun, Z. Xia, and N. Xiong, “Secure similarity search over encrypted cloud images,” *International Journal of Security and Its Applications*, vol. 9, no. 8, pp. 1–14, 2015.

[30] S. F. Sultana and D. Shubhangi, “Privacy preserving lbp based feature extraction on encrypted images,” in *2017 International Conference on Computer Communication and Informatics (ICCCI)*. IEEE, 2017, pp. 1–4.

[31] Z. Xia, N. N. Xiong, A. V. Vasilakos, and X. Sun, “Epcbir: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing,” *Information Sciences*, vol. 387, pp. 195–204, 2017.

[32] Y. Wang, M. Miao, J. Shen, and J. Wang, “Towards efficient privacy-preserving encrypted image search in cloud computing,” *Soft Computing*, vol. 23, no. 6, pp. 2101–2112, 2019.

[33] Z. Xia, L. Lu, T. Qin, H. Shim, X. Chen, and B. Jeon, “A privacy-preserving image retrieval based on ac-coefficients and color histograms in cloud environment,” *CMC-COMPUTERS MATERIALS & CONTINUA*, vol. 58, no. 1, pp. 27–43, 2019.

[34] L. Zhang, T. Jung, K. Liu, X.-Y. Li, X. Ding, J. Gu, and Y. Liu, “Pic: Enable large-scale privacy preserving content-based image search on cloud,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 28, no. 11, pp. 3258–3271, 2017.

[35] Q. Zou, J. Wang, J. Ye, J. Shen, and X. Chen, “Efficient and secure encrypted image search in mobile cloud computing,” *Soft Computing*, vol. 21, no. 11, pp. 2959–2969, 2017.

[36] C. Guo, J. Jia, K.-K. R. Choo, and Y. Jie, “Privacy-preserving image search (ppis): Secure classification and searching using convolutional neural network over large-scale encrypted medical images,” *Computers & Security*, vol. 99, p. 102021, 2020.

[37] A. I. Abdulsada and N. A. Taha, “Towards efficient privacy-preserving image similarity detection,” in *AIP Conference Proceedings*, vol. 2144, no. 1. AIP Publishing LLC, 2019, p. 050005.

[38] R. Punithavathi, A. Ramalingam, C. Kurangi, A. Reddy, and J. Uthayakumar, “Secure content based image retrieval system using deep learning with multi share creation scheme in cloud environment,” *Multimedia Tools and Applications*, vol. 80, no. 17, pp. 26 889–26 910, 2021.

[39] A. Du, L. Wang, S. Cheng, and N. Ao, “A privacy-protected image retrieval scheme for fast and secure image search,” *Symmetry*, vol. 12, no. 2, p. 282, 2020.

[40] Y. Duan, Y. Li, L. Lu, and Y. Ding, “A faster outsourced medical image retrieval scheme with privacy preservation,” *Journal of Systems Architecture*, vol. 122, p. 102356, 2022.

[41] Y. Li, J. Ma, Y. Miao, Y. Wang, T. Yang, X. Liu, and K.-K. R. Choo, “Traceable and controllable encrypted cloud image search in multi-user settings,” *IEEE Transactions on Cloud Computing*, 2020.

[42] Y. Duan, Y. Li, L. Lu, and Y. Ding, “A faster outsourced medical image retrieval scheme with privacy preservation,” *Journal of Systems Architecture*, vol. 122, p. 102356, 2022.

[43] C. Zhang, L. Zhu, S. Zhang, and W. Yu, “Tdhppir: an efficient deep hashing based privacy-preserving image retrieval method,” *Neurocomputing*, vol. 406, pp. 386–398, 2020.

[44] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, “A privacy-preserving and copy-deterrence content-based image retrieval scheme

in cloud computing," *IEEE transactions on information forensics and security*, vol. 11, no. 11, pp. 2594–2608, 2016.
[45] J. Yuan, S. Yu, and L. Guo, "Seisa: Secure and efficient encrypted image search with access control," in *2015 IEEE conference on computer communications (INFOCOM)*. IEEE, 2015, pp. 2083–2091.
[46] W. Jang and S.-Y. Lee, "Partial image encryption using format-preserving encryption in image processing systems for internet of things environment," *International Journal of Distributed Sensor Networks*, vol. 16, no. 3, p. 1550147720914779, 2020.
[47] M. Steinebach, H. Liu, R. Stein, and F. Mayer, "Hybrid image encryption," *Electronic Imaging*, vol. 2018, no. 7, pp. 371–1, 2018.
[48] J. C. Dagadu, J.-P. Li, and E. O. Aboagye, "Medical image encryption based on hybrid chaotic dna diffusion," *Wireless Personal Communications*, vol. 108, no. 1, pp. 591–612, 2019.
[49] M. K. Abdmouleh, A. Khalfallah, and M. S. Bouhlel, "A novel selective encryption scheme for medical images transmission based-on jpeg compression algorithm," *Procedia computer science*, vol. 112, pp. 369–376, 2017.
[50] H. Panduranga and S. Naveenkumar, "Selective image encryption for medical and satellite images," *International Journal of Engineering and Technology (IJET)*, vol. 5, no. 1, pp. 115–121, 2013.
[51] B. Parameshachari, R. Karappa, K. S. Soyjaudah, and S. K. Devi, "Partial image encryption algorithm using pixel position manipulation technique: the smart copyback system," in *2014 4th international conference on artificial intelligence with applications in engineering and technology*. IEEE, 2014, pp. 177–181.
[52] 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 *2016 46th annual IEEE/IFIP international conference on dependable systems and networks (DSN)*. IEEE, 2016, pp. 359–370.
[53] B. Parameshachari, H. Panduranga, S. Naveenkumar *et al.*, "Partial encryption of medical images by dual dna addition using dna encoding," in *2017 international conference on recent innovations in signal processing and embedded systems (RISE)*. IEEE, 2017, pp. 310–314.
[54] S. Naveenkumar, H. Panduranga *et al.*, "Partial image encryption for smart camera," in *2013 International Conference on Recent Trends in Information Technology (ICRTIT)*. IEEE, 2013, pp. 126–132.
[55] M. A. Khan, J. Ahmad, Q. Javaid, and N. A. Saqib, "An efficient and secure partial image encryption for wireless multimedia sensor networks using discrete wavelet transform, chaotic maps and substitution box," *Journal of Modern Optics*, vol. 64, no. 5, pp. 531–540, 2017.
[56] J. Li and Z. Wu, "The application of yolov4 and a new pedestrian clustering algorithm to implement social distance monitoring during the covid-19 pandemic," in *Journal of Physics: Conference Series*, vol. 1865, no. 4. IOP Publishing, 2021, p. 042019.
[57] A. M. Khan, "Vehicle and pedestrian detection using yolov3 and yolov4 for self-driving cars," Ph.D. dissertation, CALIFORNIA STATE UNIVERSITY SAN MARCOS, 1921.
[58] A. Bochkovskiy, C.-Y. Wang, and H.-Y. M. Liao, "Yolov4: Optimal speed and accuracy of object detection," *arXiv preprint arXiv:2004.10934*, 2020.
[59] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International conference on the theory and applications of cryptographic techniques*. Springer, 1999, pp. 223–238.
[60] S. Tahir, S. Ruj, Y. Rahulamathavan, M. Rajarajan, and C. Glackin, "A new secure and lightweight searchable encryption scheme over encrypted cloud data," *IEEE Transactions on Emerging Topics in Computing*, vol. 7, no. 4, pp. 530–544, 2017.
[61] Udacity, "Self-driving-car/annotations at master · udacity/self-driving-car." [Online]. Available: https://github.com/udacity/self-driving-car/tree/master/annotations

Aiman Sultan received her BE degree in Electrical (Telecomm) Engineering and MS degree in Information Security from NUST, Islamabad, Pakistan in 2014 and 2021 respectively. She is currently pursuing her PhD studies in Information Security from NUST, Islamabad, Pakistan and working as research assistant at Information Security and Privacy Lab established at NUST. Her research interests include Network Security, Cryptographic Protocols Design and Cloud Security.

Shahzaib Tahir received his PhD in Information Engineering from City, University of London, UK. He received his MS degree in Information Security from NUST, Pakistan. He served as Research Fellow at the City, University of London, UK. He is an Assistant Professor in the Department of Information Security, NUST and also the founder and the CTO of CityDefend Limited, UK. His research interest include applied cryptography and cloud security. Dr Shahzaib is a Senior Member of IEEE and also an alumni of InnovateUK CyberASAP.

Hasan Tahir is an Associate Professor and Head of Department Information Security at School of Electrical Engineering and Computer Science (SEECS), NUST. He holds a PhD in Information Security from the University of Essex UK. He holds an MS in Software Engineering from NUST. He specializes in Computer Security, IoT and PUFs. He is a Senior Member of IEEE and an AFHEA.

Tayyaba Anwer received her BS degree in computer science from university of Bradford in 2019. She is currently pursuing her MS in Information Security from NUST, Islamabad, Pakistan and working as Software Developer at Information Security and Privacy Lab established at NUST. Her research interests include Network Security and Cloud Security.

Fawad Khan received his Ph.D. degree from the School of Cyber Engineering, Xidian University in 2018 and works at the National University of Science and Technology, Pakistan. His research interests include access control, blockchain, and privacy preserving techniques. His professional services include Technical Program Committee Member and reviewer for several international journals and conferences.

Muttukrishnan Rajarajan is Professor of Security Engineering at the City, University of London, UK. He obtained his Ph.D. from City University London in 2001. His areas of interest include mobile security, intrusion detection and privacy techniques. He is also a visiting fellow at the BT, UK and is currently actively engaged in the UK Governments Identity Assurance programme (Verify UK). He is a Senior Member of IEEE, Member of ACM and Advisory board member of the IISP UK.

Omer Rana is the Dean of International for the Physical Sciences and Engineering College, Cardiff, UK. He obtained his BE in Engineering and MSc from Imperial College of Science, Technology Medicine (London University) and University of Southampton in 1989 and 1994 respectively. He gained his PhD from Imperial College of Science, Technology Medicine (London University) in 1998. He is a senior member of IEEE, senior member of ACM and an FHEA UK.