Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.032826
Article

A Privacy-Preserving System Design for Digital Presence Protection

Eric Yocam[1], Ahmad Alomari[2], Amjad Gawanmeh[3,*] and Wathiq Mansoor[3]

[1]Department of Computer and Cyber Sciences, The Beacom College, Dakota State University, South Dakota, USA
[2]Department of Software Engineering and Information Technology, Ecole de Technologie Superieure (ETS), Montreal, Canada
[3]College of Engineering and IT, University of Dubai, Dubai, United Arab Emirates
*Corresponding Author: Amjad Gawanmeh. Email: amjad.gawanmeh@ieee.org
Received: 30 May 2022; Accepted: 21 December 2022

Abstract: A person's privacy has become a growing concern, given the nature of an expansive reliance on real-time video activities with video capture, stream, and storage. This paper presents an innovative system design based on a privacy-preserving model. The proposed system design is implemented by employing an enhanced capability that overcomes today's single parameter-based access control protection mechanism for digital privacy preservation. The enhanced capability combines multiple access control parameters: facial expression, resource, environment, location, and time. The proposed system design demonstrated that a person's facial expressions combined with a set of access control rules can achieve a person's privacy-preserving preferences. The findings resulted in different facial expressions successfully triggering a person's face to be blurred and a person's privacy when using a real-time video conferencing service captured from a webcam or virtual webcam. A comparison analysis of capabilities between existing designs and the proposed system design shows enhancement of the capabilities of the proposed system. A series of experiments exercising the enhanced, real-time multi-parameter-based system was shown as a viable path forward for preserving a person's privacy while using a webcam or virtual webcam to capture, stream, and store videos.

Keywords: Attribute-based access control; authentication; authorization; biometrics; facial recognition; identity; privacy; machine learning; deep learning

1 Introduction

The capability to capture individuals on video has recently increased substantially as technology continues to evolve at a record pace [1]. The ubiquitous nature of video capture directly challenges existing protections for a person's privacy [2]. A person's privacy is jeopardized when a person has not consented to video capture either individually (video conference call) or among a group of people (e.g., conference room, classroom setting). Likewise, a person's behavior is not only facial expressions

but also making hand gestures (e.g., pointing, finger counting) and performing an activity (e.g., sit, stand, walk) that can be captured with video [3,4]. The collection and use of a person's data (e.g., video capture) raises concern about the consequences of tracking and monitoring a person's behavior and context [5]. Preserving a person's privacy can be achieved using a policy maintained within an authorization process to either allow viewing or block viewing of a person's face when captured on a video device. An emerging threat to preserving a person's privacy is using face swapping artificial intelligence (AI) based algorithms (e.g., deepfake) within a video, which can be difficult to detect [6].

Another privacy concern is when a person is remotely video captured, where respiratory rate or heart rate monitoring can be detected. This physiological information (not to mention cognitive or emotional state information) can be used to determine whether a person is physically healthy or at a high risk of contracting a disease [7]. The unauthorized use of a person's physiological information by an insurance provider, captured in this manner, may put a person's insurance coverage. Furthermore, privacy risk exists for processing operations classifying individuals based on soft traits like facial expressions may also impact personal freedoms and human rights [8]. A system can be designed to protect a person's digital presence by preserving the person's privacy. In addition, there is much recent interest in applying AI methods in privacy preservation [9–12]. However, there are many challenges in preserving a person's privacy against potential unauthorized access, abusive use, and a lack of privacy consent protections in live streaming and live events.

This paper proposes and implements a novel framework for protecting a person's digital presence. The novelty represents an enhanced capability that enables fine-tuning access control that combines parameters. The parameters include facial expression, resource, environment, location, and time. This enhanced capability overcomes today's single parameter or binary (e.g., blur or not blur) access control capability when protecting a person's privacy. The system design is based on an implementation of a privacy preserving model. The model consists of both identity authentication and attribute-based authorization. The model capabilities support the following: 1) using artificial intelligence-based video processing techniques (e.g., facial identity and facial expression recognition), 2) transformation of privacy parameters from privacy consent preferences into access control policies, 3) enabling fine-grained access control policies, and 4) limiting unrestricted access of specific video contents (e.g., a person's face) during video capture, stream, and storage [13]. The person's facial expressions (e.g., happy, sad, neutral, angry, disgusted, and surprised) are biometric markers that can be used as part of an access control mechanism such as attribute-based access control (ABAC). ABAC policy parameters configured from a person's privacy consent preferences result in a person's face being blurred or not blurred. For example, a person's face can be blurred during a real-time videoconferencing session using video captured from a webcam or virtual webcam. Likewise, other ABAC policy parameters can be based on environmental bounding (e.g., classroom setting), location bounding (e.g., Washington state), and temporal bounding (e.g., between 8 am to 5 pm). Any one or all the policy parameters can be configured to provide a person with privacy-preserving protection.

The rest of this paper is organized as follows: Section 2 presents related work on the subject. Section 3 defines the privacy-preserving model. Section 4 presents an implementation of the framework. Section 5 discusses results, experimentation, limitations, and open issues. Finally, Section 6 concludes the paper.

2 Related Work

A review of related work addresses two aspects of this study. First, a review of comparable related work identifies initial system designs and models with missing capabilities that this study

has addressed. Second, a review of relevant related work identifies specific components necessary for constructing the proposed privacy-preserving model as part of the system design.

The contribution of this paper addresses the missing capabilities of initial system designs and models with a new system design and model that adds a capability that overcomes today's single parameter-based access control protection mechanism for digital privacy preservation. The enhanced capability combines multiple access control parameters, including facial expression, resource, environment, location, and time. A review of comparable related work identifies initial system designs and models with missing capabilities. It demonstrates the completeness of the proposed privacy-preserving model as part of the system design (see Table 1). The related works are relevant and comparable to this study. A not applicable (N/A) within a comparable related work represents a missing capability and highlights the need for this study.

A review of related work supports the proposed privacy-preserving model as part of the system design. A particular related work supports a component of the privacy-preserving model. The related work includes digital privacy rights, privacy consent, digital presence, biometric markers, facial recognition, and attribute-based access control. In addition, greater detail for each of the related works is presented within each of the subsections.

Table 1: Comparable related work

Reference	Privacy attribute	Access control mechanism	Machine learning/deep learning with performance metrics	Model type	System design/proposed solution
[14]	Stored data privacy protection	Attribute-based access control (ABAC)	Not applicable (N/A)	Privacy-preserving	Revocable ciphertext policy attribute-based encryption scheme
[15]	User privacy protection	ABAC	N/A	Privacy-preserving	Access control, encryption and digital signatures.
[16]	Automatic personal privacy filtering during unconstrained streaming activities, facial recognition	N/A	Convolutional neural network (CNN) (accuracy 89%)	Privacy-preserving	Fast and accurate pixelation of irrelevant people's faces
[17]	Digital presence, digital authentication, facial recognition	N/A	K-nearest neighbor (KNN) (accuracy: 96%)	Authentication of a person's identity	Efficient mechanism to carry out the recognition of facial features to satisfy the authentication of a system

(Continued)

Table 1: Continued

Reference	Privacy attribute	Access control mechanism	Machine learning/deep learning with performance metrics	Model type	System design/proposed solution
This study	Digital privacy rights, privacy consent, digital presence, biometric markers, and facial recognition	ABAC	KNN (accuracy: 89%) & CNN (accuracy: 63%)	Privacy-preserving	Enhanced access control capability with multiple parameters facial expression, resource, environment, location, and time

2.1 Digital Privacy Rights

A relationship exists between confidentiality and privacy. Confidentiality protects against a third party's unauthorized use of a person's information. In contrast, privacy protects a person's right to control his or her information collected, maintained, and shared with others by a third-party [18]. A digital privacy right represents the level of privacy protection a person exercises while connected to the Internet. A person's digital privacy right may be exercised when the person is unwilling for a third party to collect, maintain and share a person's information. For example, a third party may tend to abuse a person's right by sharing a person's current location and other related identification and tracking information considered confidential and private to a person.

2.2 Privacy Consent

Privacy becomes relevant when a person does not want his or her data shared with others. Similarly, data privacy defines who has access to a person's data. Data protection consists of a collection of tools and policies to limit access to a person's data [19]. Privacy consent represents an agreement to limit access to a person's data. The agreement can be represented by attributes (or privacy preferences) established to protect a person's privacy associated with his or her identity. The person's privacy consent translates into a set of privacy preferences and protected data.

2.3 Digital Presence

A digital presence refers to a person's digital footprint representing a trail that a person leaves behind when accessing and using the Internet. Much of the Internet traffic is now video and along with growing online video demand. The difficulty in verifying video data capture, stream, and storage protections highlight the emerging privacy concern with protecting a person's right to privacy associated with his or her digital presence [20].

2.4 Biometric Markers

A biometric marker identifies a particular person's feature (or attribute) that is unique to that person, such as a fingerprint, iris scan, deoxyribonucleic Acid (DNA), facial characteristic, or voice. A person's face can be recognized among many other faces and used to identify a specific person [21]. A facial expression can be considered a facial characteristic and considered a biometric marker. Once

a person's identity has been established, a set of access controls can be used to trigger actions based on a person's facial expression. For example, recorded video data maintained and stored by video conference service providers (or a third party) may not be adequately secured and get tampered with by malicious people (e.g., deepfakes). A person's privacy right can be abused when a third party gets access to a recorded video of the person that otherwise was not supposed to have access [22].

2.5 Facial Recognition

A person's face represents a biometric marker that can establish a person's identity. For example, a United States driver's license and a United States passport both have an image of the person's face embedded in the documents. Specifically, the association of a person's image (or likeness), person's name, and other specific information establish the person's identity. Facial recognition can be used for a person's identity [23]. Therefore, the person's digital presence may increase the likelihood of becoming susceptible to identity fraud and theft. For example, deepfakes are frequently in the headline news, given the rapid technological evolution used to develop realistic deepfakes. A deepfake allows a malicious person to manipulate another person's facial expressions (e.g., happy, sad, angry, fearful, neutral, disgusted, and surprised) when captured on video and replay the deepfake video to commit identity fraud and theft [24]. Other works discussed relational extractions combined with facial recognition [25,26]. Other real time face recognition systems [27] and other types of objects [28,29].

2.6 Attribute Based Access Control

The three common types of access control include access control lists (ACL), role-based access control (RBAC), and ABAC. The advantage of using ABAC over other access controls approaches is flexibility and fine-grained control and is best represented in a comparable study that aligns with this study's use of an attribute-based access control model for privacy preservation. The National Institute of Standards and Technology (NIST) provides a guide (e.g., SP 800-162) that outlines a framework for an ABAC. An ABAC is typically chosen since the attributes found within the ABAC provide flexibility beyond other access control schemes by providing granular control of access parameters. For example, various attributes can be defined within the ABAC, where the granular control of access parameters includes facial expression, resource, environment, location, and time.

3 Privacy Preservation Model

The novel privacy-preserving model is divided into two primary model components—identity authentication and attribute-based authorization. The identity authentication model consists of three parts: authenticator, identity proving and face database. The attribute-based authorization consists of four parts, including policy enforcement point (PEP), policy decision point (PDP), policy administration point (PAP), and policy information point (PIP). The related work (found in the previous section) represents the privacy attribute and relates to identity authentication, attribute-based authorization, or both model components (see Table 2).

The identity proofing is an identity authentication component that establishes a person's identity and relates to the digital presence where the person's identity must be protected when accessing and using the Internet. The parameter settings are associated with capturing 30 facial grayscale images of a person used for training a face recognizer. The face database is an identity authentication component containing a set of face images used to establish the person's identity and relates to biometric markers representing features (or attributes) that are unique to a person found within the set of face images

to establish a person's identity. The parameter settings are associated with labelling and storing each image within a directory for training a face recognizer.

Table 2: Privacy-preserving model components

Privacy attribute	Model component	
	Identity authentication	Attribute-based authorization
Digital privacy rights	Not applicable (N/A)	Policy information point
Privacy consent	N/A	Policy information point
Digital presence	Identity proofing	Policy administration point
Biometric markers	Face database	Policy decision point
Facial recognition	Authenticator	Policy decision point
Attribute-based access control	N/A	Policy enforcement point

The authenticator is an identity authentication component that authenticates a person's identity and relates to facial recognition when matching a person's face to an established identity. The parameter settings are associated with recognizing a person using a prediction algorithm based on a trained set of facial images. The PIP is an attribute-based authorization component serving the PDP by retrieving digital privacy attributes and relates to both digital privacy rights protecting a person's right to control aspects of privacy and privacy consent establishing a set of privacy preferences and protections. The parameter settings are associated with a consent agreement with privacy preferences established for a person.

The PAP is an attribute-based authorization component that enables managing privacy preferences and relates to the digital presence where a person's privacy preferences and protections can be managed when accessing and using the Internet. The parameter settings are associated with managing consent agreements with configured privacy preferences for a person. The PDP is an attribute-based authorization component that transforms privacy preferences and protections into attribute-based access authorization responses and relates to both biometric markers representing features (or attributes) that are unique to a person captured on video, stream or storage and facial recognition when matching a person's face to determine an attribute-based authorization. The parameter settings are associated with translating the consent agreement configured privacy preferences for a person into a set of attributed-based access control settings. When a person's face has been recognized, a person's privacy protection ensues depending on the combination of the attributed-based access control settings invoked (e.g., facial expression, resource, environment, location, and time).

The PEP is an attribute-based authorization component that enforces the person's privacy preferences and protections and relates to the enforcement of one or more parameters within the attribute-based access control mechanism. The parameter settings are associated with the enforcement of a person's privacy protection.

3.1 Model Components

The privacy-preserving model has been implemented as a system that protects a person's privacy. The model combines identity authentication and attribute-based authorization using facial recognition algorithms for identity and detection of facial biometric markers and attribute-based access control for access management as illustrated in Fig. 1.

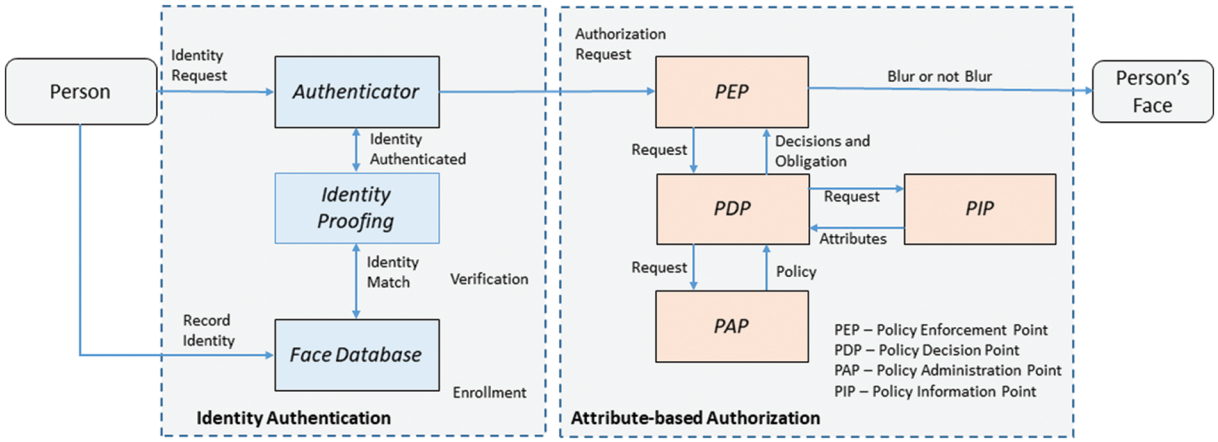

Figure 1: Privacy-preserving model

3.2 Identity Authentication

The identity authentication refers to the process of recognizing a person's identity and consists of two parts, including verification and enrollment, as shown in Fig. 2. The authenticator and identity proofing are part of the verification that consists of the authenticator, identity proofing and face database. The authentication provides the enforcement of correctly identifying a person.

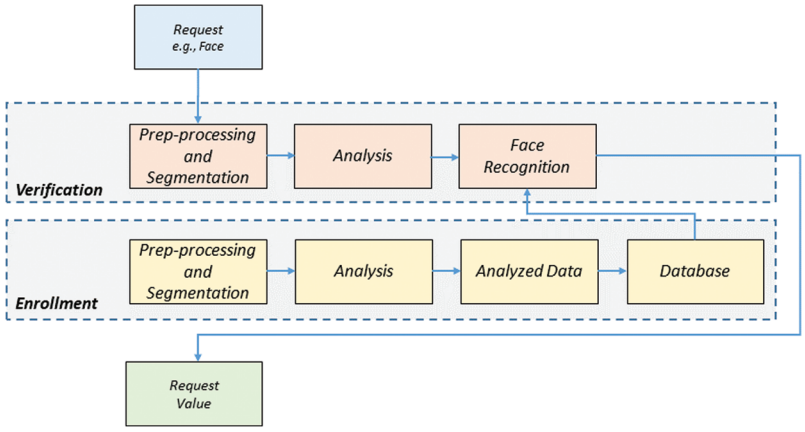

Figure 2: Structure of an authentication request

The identity proofing provides matching the identity based on facial recognition of the person's face that is found within the face database. The face database is part of enrollment. The face database is a set of facial images collect during enrollment of the person's face. The enrollment takes place before verification to establish the person's identity.

3.3 Attribute-Based Authentication

The ABAC refers to the process of giving a person the ability to access a resource. The attribute-based authentication consists of four parts, including PEP, PDP, PAP, and PIP. The PEP enforces the access decision based on a collection of attributes required for making the decision. The PDP

computes the access decision. The PAP stores the policies in a repository. The PIP retrieves the attributes necessary for policy evaluation.

The ABAC extends the access control model beyond the traditional models (e.g., ACL, RBAC) using lists or roles but with access rights based on user, environment, and resources [30,31]. The access control is determined to allow a person's face to be viewable or not. A request is sent to the ABAC once the identity authentication has been completed, as shown in Fig. 3. The review of the policy determines an outcome and generates a response. Facial recognition is based on feature extraction using the Convolution Neural Network (CNN) algorithm [32].

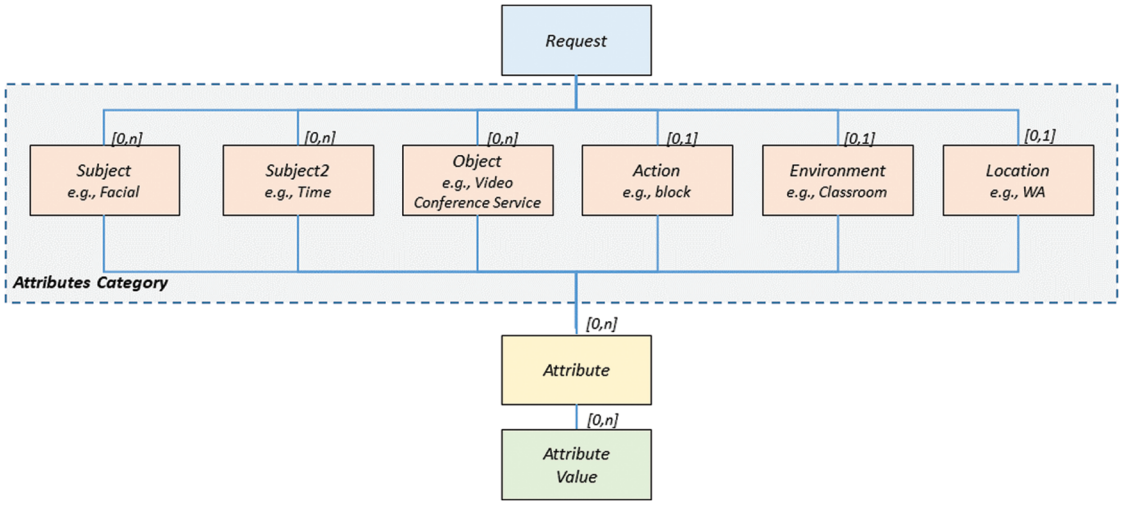

Figure 3: Structure of an authorization request

The ABAC policy configuration maintains the privacy preferences established by the person's consent settings. The informed consent settings establish the facial expression that permits viewing person's face. Once successfully authorized, a person's face is either viewable or not viewable within the real time video stream or saved video capture.

4 System Implementation

The implementation of the protecting privacy-preserving model consists of three parts including development environment, dataset selection, system design, and system results.

4.1 Development Environment

The development environment includes Python 3, Open-source computer vision library (OpenCV), Keras, TensorFlow 2.0., Casbin, and Open Broadcaster Software (OMS), as shown in Fig. 4. OpenCV is a library that provides a combination of computer vision and machine learning functions. Keras is built in Python and provides a neural network library. TensorFlow 2.0 is a library that provides scalable machine learning and deep learning functions. The facial identity and recognition are performed in real-time with the OpenCV library: TensorFlow and Keras [33,34]. Casbin is a library that provides open-source access control functions for ABAC. OMS is open-source video recording and live streaming software. The OMS provides a virtual webcam that permits the privacy-preserving model within the system to be connected between webcam and video teleconferencing service (e.g., Zoom, Microsoft Teams, Google Meet).

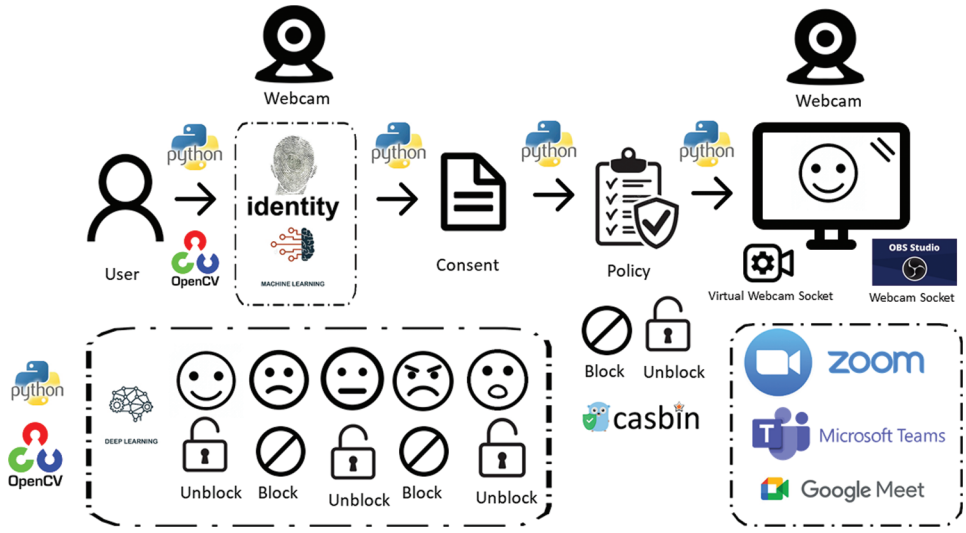

Figure 4: Contextual overview of system and development environment

4.2 Dataset Selection

Two datasets were used within the system. A relatively small dataset was generated for the system within the authentication process, and a significantly larger dataset within the authorization process. The K-Nearest Neighbor (k-NN) model generates a database of captured images that form the dataset. The CNN model uses the facial emotion recognition 2013 (FER-2013) dataset published at the International Conference on Machine Learning and consists of over 35,000 grayscales, 48 × 48-sized face images with seven facial expressions, including angry, disgusted, fearful, happy, neutral, sad, and surprised.

4.3 System Design

Facial identity is maintained using a face recognition process that starts with building a library of face images acquired from still images and videos. In order to process an image for recognition, several parameters are collected from that image's features and compared with the existing library. A similarity value is obtained based on the proposed model, which is then used to identify the identity based on the calculated value for the face [35]. Fig. 5 shows a demonstration of the image library capturing process.

Facial identity recognition uses a k-NN classification algorithm. The k-NN algorithm is used for classification [36]. To avoid any biasing, each class is represented by an equal number of instances, and a 10-fold cross validation tactic is employed to avoid the limitation of the dataset size [37]. The additional algorithm used besides the k-NN algorithm is the Haar Cascade algorithm [38]. The Haar Cascade classifier functions as a detection algorithm to identify faces, based on edge or line detection features, from a source image in a video. Therefore, minimizing the error rate is critical when selecting the feature for classification (e.g., Haar Cascade classifier). A histogram captures a range of confidence between 87 and 89 percent when detecting the identity, as shown in Fig. 6.

Figure 5: Facial image library captured for identity authentication

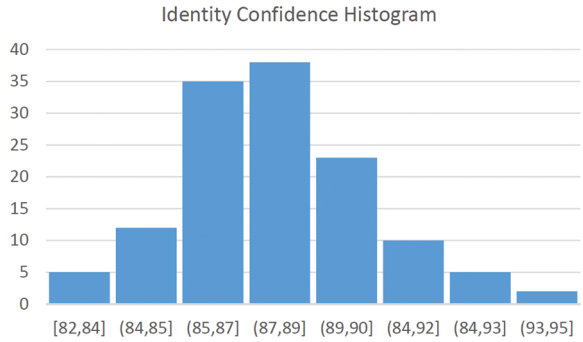

Figure 6: Confidence levels when detecting a person's identity

The facial expression recognition used a 4-layer Convolutional Neural Network (CNN) model to perform image classification [39]. Epochs play a vital role in deciding the accuracy of the models used in the system. The procedure starts with using the Haar cascade method to extract the face in each frame obtained from the live stream. Next, the extracted image is resized into a fixed width square of 48 pixels. This image is used as input to the CNN model, producing a list of SoftMax scores for all the classes of facial expression. Finally, the facial expression with the maximum score is displayed on the screen. The facial expression recognition uses a simple four-layers CNN with a test accuracy of approximately 63% in 50 epochs. When constructing the H5 model, the CNN model accuracy vs. epochs and loss vs. epoch plots can be generated by OpenCV for facial expression recognition. The selection of epochs number selected was 50. The training to a testing ratio of the CNN model was

80/20. When a person's face has been recognized, a person's privacy protection ensues depending on the combination of the attributed-based access control settings invoked (e.g., facial expression, resource, environment, location, and time). The portion of attribute-based access control pertains to facial expression and the 4-layer CNN model used for facial expression recognition with a set of parameter settings (see Table 3).

Table 3: Convolutional neural network parameters

No.	Parameter	Value
1	Number of persons	35,887
2	Training dataset size	28,709
3	Testing dataset size	7178
4	Number of facial expressions	7
5	Number of layers	4
6	Batch size	64
7	Epochs	50
8	Learning rate	0.0001
9	Decay rate	1e–6
10	Momentum	0.9
11	Frame rate	25 frames/sec
12	Frame size	48×48

A model-optimization technique that contributes to the model performance and accuracy is using a 4-layer CNN optimization method. The model accuracy determines the level of facial expression detection, as shown in Fig. 7. In this case, the training accuracy depicts an overfit model where training accuracy increases, and validation accuracy slightly increases and then levels off. The overfit of the accuracy model is acceptable, given the amount of data collected. However, the accuracy can be improved by increasing regularization, increasing the number of parameters, or collecting more data. *Accuracy* is a metric applied to classification tasks. Accuracy describes what percentage of the test data have been correctly classified. The performance of the method is obtained through the correct predictions from the total number of cases in the training set, which can be inversely correlated with the loss.

The model loss determines the amount of loss with the detection, as shown in Fig. 7. In this case, the training loss depicts an overfit model where training loss decreases and validation loss increases. The overfit of the loss model is acceptable since the model is trained to fit the train data as well as possible. The loss depends on how the model predicts classes for the classification. The optimization process tries to minimize loss with the training data (e.g., Adam optimizer). The lower the loss, the better the loss value over the training data after each epoch.

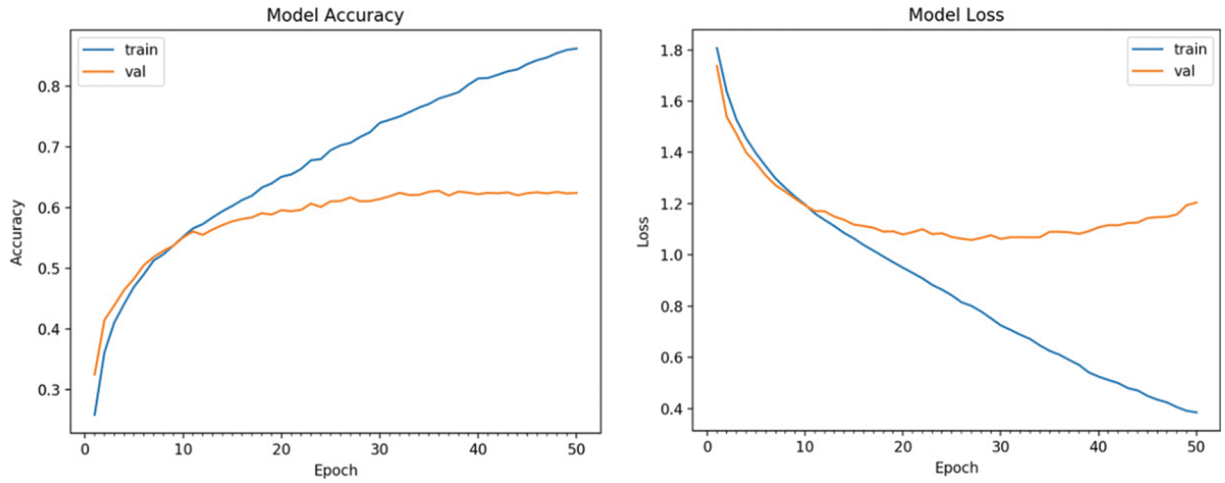

Figure 7: Convolution neural network model accuracy for facial expression recognition and recognition

NIST provides a framework for establishing an ABAC system [40], as shown in Fig. 8. ABAC will decide the access level through a predefined policy that matches the calculated value of the attributes and the environmental conditions with the rules defined in the access control rules. Attributes include characteristics of the subject, object, and environmental conditions. A simplified equation for ABAC can be expressed as:

```
Access Control Policy = Subject Attributes + Object Attributes +
Environment Attributes
Access Control Policy = {Action (Block, No Block)}
        Example: Action is "Block", resulting in blur face or
Action is "No Block" resulting in not blur face
Subject Attributes:
Subject = {Subject, Subject Rule1 (Facial Expression)}
        Example: Subject is "Happy"
Subject Rule1 is "Facial"
Subject2 = {Subject2, Subject Rule2 (Time)}
        Example: Subject2 is "Time"
Subject Rule is "Between 8:00 AM and 5:00 PM"
Object Attributes:
Object = {Object}
        Example: Object is "Zoom"
Environment Attributes:
Environment = {Environment} + {Location}
    Example: Environment is "Classroom" and Location is "WA"
```

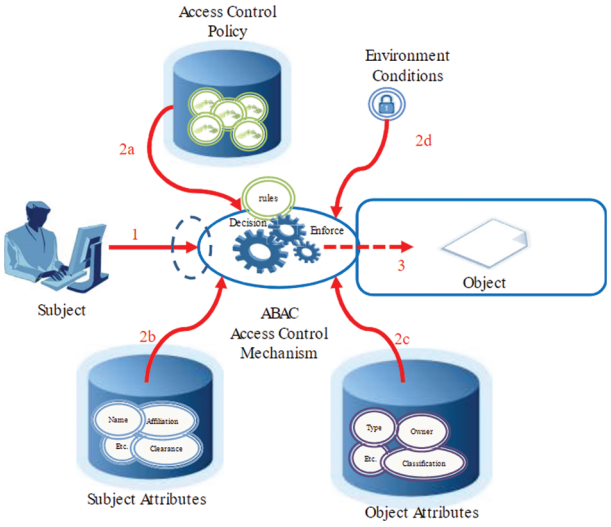

Figure 8: Attribute-based access control representation [40]

The system design for the ABAC is based on the NIST framework. The simplified aspects of the NIST defined version of ABAC include model, policy, requests, and enforcement [41]. The ABAC model, policy, requests, and enforcement are based on an authorization library that supports access control models from Casbin. In addition, the ABAC model includes request definition, policy definition, policy effect and matches (see Table 4).

Table 4: Attribute-based access control model notation

[request_definition]	r = sub, sub2, obj, act, env, loc
[policy_definition]	p = sub_rule, sub_rule2, obj, act, env, loc
[policy_effect]	e = some (where (p.eft == allow))
[matchers]	m = eval(p.sub_rule) && eval(p.sub_rule2) && r.obj == p.obj && r.act == p.act && r.env == p.env && r.loc == p.loc

The ABAC policy comprises a configuration file for facial attribute rules with parameters including subject rule, subject, object, action, environment, and location (see Table 5). The p.sub_rule is a user-defined type consisting of necessary attributes found in the policy. For example, a block blurs the recognized face with a Gaussian blur and OpenCV.

The ABAC policy consists of a configuration file for time-bounded attribute rules with parameters including subject rule, subject, object, action, environment, and location (see Table 6). The ABAC request format for the facial attribute rules passing parameters includes subject, object, action, environment, and location. The ABAC provides fine-grained access control by passing parameters ensuring data confidentiality of a person's face and addressing the privacy challenges related to data privacy and access control. The ABAC facial request is evaluated based on the facial policy rule configuration and model with an enforcement response of either true or false. A response of true results in a facial policy rule match. A response of false results in an unmatched facial policy rule within the policy configuration file.

Table 5: Attribute-based access control policy notation

p.sub_rule	p.sub	r.obj	p.act	p.env	p.loc
p, r.sub.facial	"happy"	zoom	no_block	class_room	WA
p, r.sub.facial	"angry"	zoom	block	class_room	WA
p, r.sub.facial	"sad"	zoom	block	class_room	WA
p, r.sub.facial	"neutral"	zoom	no_block	class_room	WA

Table 6: Attribute-based access control time bounded policy notation

ABAC notation	sub_rule	sub	obj	act	env	loc
Time boundary policy	p, r.sub2.tim > "0800" && r.sub2.tim < "1700"	8:00 am to 5:00 pm	zoom	no_block	class_room	WA
Facial request	'facial': 'happy'	'facial': 'happy'	zoom	no_block	class_room	WA
Time bound request	'tim': '1200'	'tim': '1200'	zoom	no_block	class_room	WA

Likewise, a policy parameter can consist of a time-bounded attribute within the ABAC system [42]. The ABAC request format for the time-bounded attribute rules passing parameters includes subject, object, action, environment, and location. The ABAC time-bounded request is evaluated based on the time-bounded policy rule configuration and model with an enforcement response of either true or false. A response of true results in a time-bounded policy rule match. The response of false results in a time-bounded policy rule unmatched within the policy configuration file. The ABAC enforcement of the policy rules is performed by evaluating the request. The overhead to execute an enforcement command is 0.007510 milliseconds and represents a time complexity of O(1). The following query represents the enforcement:

e.enforce (sub, sub2, obj, act, env, loc).

Likewise, the ABAC evaluation parameters of the policy rules are represented by

sub = 'facial': 'happy', sub2 = 'tim': '1200', obj = "zoom", act = "no_block", env = "class_room", and loc = "WA"

5 Results, Experimentation, Limitations, and Future Work

A person's privacy is jeopardized when a person has not consented to be captured on video either individually (e.g., video conference call) or among a group of people (e.g., video surveillance). The results produced by implementing the model into a working system demonstrate that a person's face may be blurred to remain anonymous depending on the person's choice to preserve privacy. The resultant solution represents a privacy preservation model as part of an enhanced, real-time multi-parameter-based system. As previously discussed, this enhanced capability is necessary to overcome

today's single parameter-based access control protection mechanism for digital privacy preservation where the multi-parameters include facial expression, resource, environment, location, and time (see Table 7).

Table 7: Privacy-preserving method comparison

Reference	Privacy attribute	Access control mechanism	Method used
[42]	Stored data privacy protection	Encryption algorithm, watermarking, Blockchain for fine-grain access control	Single parameter-based access control protection mechanism
[43]	User privacy protection	Clark-wilson (CW) security model	Single parameter-based access control protection mechanism
[44]	Automatic personal privacy Filtering, unconstrained streaming, facial recognition	Discretionary access to data based on needs and approvals	Single parameter-based access control protection mechanism
[45]	Digital presence, digital authentication, facial recognition	Face liveness detection with behavior challenge-response	Single parameter-based access control protection mechanism
This study	Digital privacy rights, privacy consent, digital presence, biometric markers, and facial recognition	ABAC	Enhanced capability with multi-parameters includes facial expression, resource, environment, location, and time

The resultant solution can be divided into distinct phases during operation: 1) identify a person. 2) capture a person's facial expressions. 3) enforce a set of privacy-preserving preferences. Finally, perform attribute-based access control that will either blur or not blur a person's face when captured in real-time from a webcam, as shown in Fig. 9. The experimentation demonstrates a combination of exercised access control parameters, including facial expression, resource, environment, location, and time. The attempts made, successes and failures were collected (see Table 8). The attempts made resulted in a range between 101 and 112 attempts. A successful outcome resulted in a range between 94% and 97%. An unsuccessful outcome resulted in a range between 3% and 6%.

The proposed model is efficient and can work in real time to provide the required privacy preservation while doing live conferencing or live streaming. In addition, privacy preservation can be set or customized by the user depending on the scenario, i.e., it can be more restricted or more relaxed based on the situation. The limitations of the approach include interoperability, testing with several faces, and testing in different weather and lighting conditions. In future work, we intend to provide a complete application programming interface (API) based implementation that can be integrated with other social media platforms or mobile apps. In addition, we intend to test under several lightning scenarios and various faces.

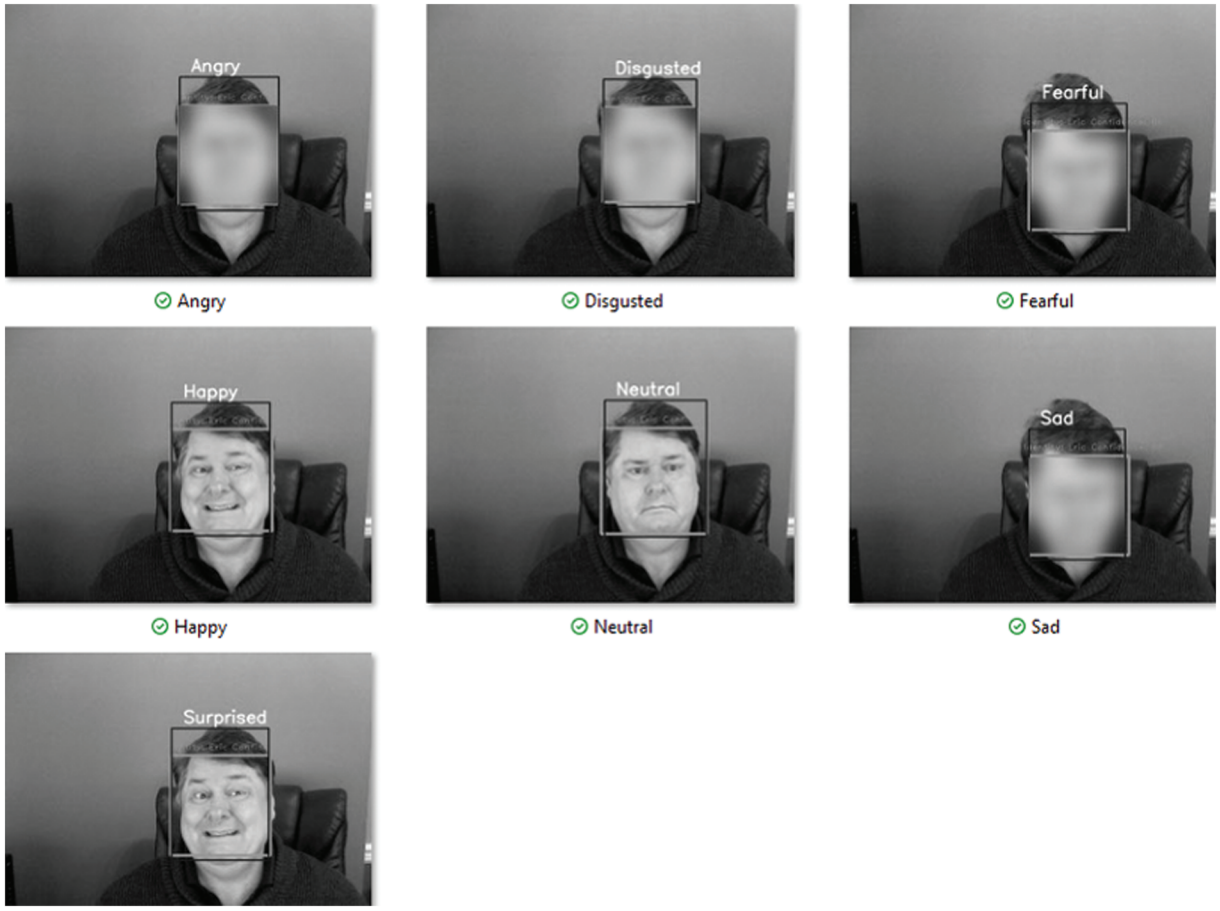

Figure 9: Privacy-preserving preferences in action

Table 8: Experimentation

Facial expression	Resource (e.g., video conferencing service)	Environment	Location (e.g., within Washington state)	Time boundary	Privacy protection attempts made (identified)	Privacy protection success (blurred)	Privacy protection unsuccessful (unblurred)
Multiple expressions	Zoom	Home	Sammamish	9:00 AM–9:30 AM	115	95%	5%
Multiple expressions	Microsoft teams	Office	Bellevue	10:00 AM–10:30 AM	101	97%	3%
Multiple expressions	GoToMeeting	Mobile	Redmond	1:00 PM–1:30 PM	103	96%	4%
Multiple expressions	Skype	Mobile	Issaquah	2:00 PM–2:30 PM	112	94%	6%

6 Conclusions

This paper described an innovative system design with the implementation of a novel privacy-preserving model. The system combines facial identity recognition, facial expression recognition, and attribute-based access control. The facial identity is based on a Haar-cascade classifier based on the K-Nearest Neighbor matching algorithm. Facial recognition is based on feature extraction using the Convolution Neural Network algorithm. Both facial recognition for facial identity recognition and facial expression recognition is performed in real-time. Attribute-based access provides granular control of access parameters, including facial expression, resource, environment, location, and time.

The results from the system design demonstrated that a person's facial expressions combined with a set of access control rules could achieve a person's privacy-preserving preferences. The facial expression triggered a person's face to be blurred to remain anonymous when using a real-time video conferencing service captured from a webcam or virtual webcam. Any future work might include a further investigation into extending the biometric markers within the privacy-preserving model implementation. Some additional biometric markers to consider are the following: recognizing a person's gesture, person's bodily movement, and person's age. Gesture recognition of a person's hand may be used with access control to blur inappropriate gestures. Detecting a person's bodily movement may provide additional insights, especially when combined with facial expressions and gestures. The ability to detect a person's age may be used to protect the identity of children.

Funding Statement: No research fund was used to conduct this research. APC charge will be provided by University of Dubai.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Fitwi and Y. Chen, "Privacy-preserving selective video surveillance," in *29th Int. Conf. on Computer Communications and Networks (ICCCN), 2020*, Honolulu, Hawaii, USA, pp. 1–10, 2020. https://doi.org/10.1109/ICCCN49398.2020.9209688

[2] F. Tariq, N. Kanwal, M. S. Ansari, A. Afzaal, M. N. Asghar *et al.,* "Towards a privacy preserving surveillance approach for smart cities," in *Proc. of 3rd Smart Cities Symp. (SCS 2020)*, Online, pp. 450–455, 2020. https://doi.org/10.1049/icp.2021.0966

[3] H. Badave and M. Kuber, "Face recognition based activity detection for security application," in *Proc. of Int. Conf. on Artificial Intelligence and Smart Systems (ICAIS)*, Coimbatore, India, pp. 487–491, 2021. https://doi.org/10.1109/ICAIS50930.2021.9395829

[4] B. Feng, Y. Lin, T. Xu and J. Duan, "A survey on privacy preservation in video big data," in *2021 Int. Conf. on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, Mauritius, Mauritius, pp. 1–6, 2021. https://doi.org/10.1109/ICECCME52200.2021.9591105

[5] M. Akil, L. Islami, S. Fischer-Hübner, L. A. Martucci and A. Zuccato, "Privacy-preserving identifiers for IoT: A systematic literature review," *IEEE Access*, vol. 8, pp. 168470–168485, 2020. https://doi.org/10.1109/ACCESS.2020.3023659

[6] A. A. Maksutov, V. O. Morozov, A. A. Lavrenov and A. S. Smirnov, "Methods of deepfake detection based on machine learning," in *Proc. of Institute of Electrical and Electronics Engineers Conf. of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, St. Petersburg and Moscow, Russia, pp. 408–411, 2020. https://doi.org/10.1109/EIConRus49466.2020.9039057

[7] M. Chen, Q. Zhu, H. Zhang, M. Wu and Q. Wang, "Respiratory rate estimation from face videos," in *2019 IEEE EMBS Int. Conf. on Biomedical & Health Informatics (BHI)*, Chicago, IL, USA, pp. 1–4, 2019. https://doi.org/10.1109/BHI.2019.8834499

[8] T. Bisztray, N. Gruschka, T. Bourlai and L. Fritsch, "Emerging biometric modalities and their use: Loopholes in the terminology of the GDPR and resulting privacy risks," in *Proc. of Int. Conf. of the Biometrics Special Interest Group (BIOSIG)*, Darmstadt, Germany, pp. 1–5, 2021. https://doi.org/10.1109/BIOSIG52210.2021.9548298

[9] M. Hamdi, H. Bouhamed, A. AlGarni, H. Elmannai and S. Meshoul, "Deep learning and uniform lbp histograms for position recognition of elderly people with privacy preservation," *International Journal of Computers, Communications and Control*, vol. 16, pp. 1–15, Agora University, Oradea, Romania, 2021. https://doi.org/10.15837/ijccc.2021.5.4256

[10] A. Agarwal, P. Chattopadhyay and L. Wang, "Privacy preservation through facial de-identification with simultaneous emotion preservation," *Signal Image and Video Processing*, vol. 15, no. 5, pp. 951–958, 2021.

[11] H. Xu, Z. Cai, D. Takabi and W. Li, "Audio-visual autoencoding for privacy-preserving video streaming," *Institute of Electrical and Electronics Engineers Internet of Things Journal*, vol. 9, no. 3, pp. 1749–1761, 2021.

[12] J. Liu, K. Fan, H. Li and Y. Yang, "A blockchain-based privacy preservation scheme in multimedia network," *Multimedia Tools and Applications*, vol. 80, no. 20, pp. 30691–30705, 2021.

[13] H. Kim, Y. Cha, T. Kim and P. Kim, "A study on the security threats and privacy policy of intelligent video surveillance system considering 5 G network architecture," in *Proc. of Int. Conf. on Electronics, Information, and Communication (ICEIC)*, Barcelona, Spain, pp. 1–4, 2020. https://doi.org/10.1109/ICEIC49074.2020.9051302

[14] C. Lachner, T. Rausch and S. Dustdar, "A privacy preserving system for AI-assisted video analytics," in *2021 IEEE 5th Int. Conf. on Fog and Edge Computing (ICFEC)*, Melbourne, Australia, pp. 74–78, 2021. https://doi.org/10.1109/ICFEC51620.2021.00018

[15] C. Pathmabandu, J. Grundy, M. B. Chhetri and Z. Baig, "An informed consent model for managing the privacy paradox in smart buildings," in *2020 35th IEEE/ACM Int. Conf. on Automated Software Engineering Workshops*, Melbourne, Australia, pp. 19–26, 2020. https://doi.org/10.1145/3417113.3422180

[16] A. J. Perez, S. Zeadally, S. Griffith, L. Y. M. Garcia and J. A. Mouloud, "A user study of a wearable system to enhance bystanders' facial privacy," *Internet of Things (IoT)*, vol. 1, no. 2, pp. 198–217, 2020. https://doi.org/10.3390/iot1020013

[17] J. Li, Z. Li, G. Tyson and G. Xie, "Your privilege gives your privacy away: An analysis of a home security camera service," in *Proc. of INFOCOM, 2020–IEEE Conf. on Computer Communications*, Toronto, ON, Canada, pp. 387–396, 2020. https://doi.org/10.1109/INFOCOM41043.2020.9155516

[18] G. Liashenko and A. Astrakhantsev, "Implementation biometric data security in remote authentication systems via network steganography," in *2019 Conf. on Mathematical Control Theory, Advances in Information and Communication Technology and Systems, Lecture Notes in Networks and Systems (LNNS) Kyiv, Ukraine*, Cham, Springer, Vol. 152, pp. 257–273, 2019. https://doi.org/10.1007/978-3-030-58359-0_14

[19] K. Rabieh, S. Mercan, K. Akkaya, V. Baboolal and R. S. Aygun, "Privacy-preserving and efficient sharing of drone videos in public safety scenarios using proxy re-encryption," in *2020 IEEE 21st Int. Conf. on Information Reuse and Integration for Data Science (IRI)*, Las Vegas, NV, USA, pp. 45–52, 2020. https://doi.org/10.1109/IRI49571.2020.00015

[20] L. Zahara, P. Musa, E. Prasetyo Wibowo, I. Karim and S. Bahri Musa, "The facial emotion recognition (FER-2013) dataset for prediction system of micro-expressions face using the convolutional neural network (CNN) algorithm-based Raspberry Pi," in *2020 Fifth Int. Conf. on Informatics and Computing (ICIC)*, Gorontalo, Indonesia, pp. 1–9, 2020. https://doi.org/10.1109/ICIC50835.2020.9288560

[21] L. Verdoliva, "Media forensics and deepfakes: An overview," *Institute of Electrical and Electronics Engineers Journal of Selected Topics in Signal Processing*, vol. 14, no. 5, pp. 910–932, 2020. https://doi.org/10.1109/JSTSP.2020.3002101

[22] K. Seol, Y. -G. Kim, E. Lee, Y. -D. Seo and D. -K. Baik, "Privacy-preserving attribute-based access control model for XML-based electronic health record system," *Institute of Electrical and Electronics Engineers Access*, vol. 6, pp. 9114–9128, 2018. https://doi.org/10.1109/ACCESS.2018.2800288

[23] S. T. Kim and Y. M. Ro, "Attended relation feature representation of facial dynamics for facial authentication," *Institute of Electrical and Electronics Engineers Transactions on Information Forensics and Security*, vol. 14, no. 7, pp. 1768–1778, 2019. https://doi.org/10.1109/TIFS.2018.2885276

[24] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su *et al.,* "A survey on access control in the age of internet of things," *Institute of Electrical and Electronics Engineers Internet of Things Journal*, vol. 7, no. 6, pp. 4682–4696, 2020. https://doi.org/10.1109/JIOT.2020.2969326

[25] V. R. P. Rao, C. A. H. Puwakpitiyage, D. A. Shafiq, F. Islam, D. O. D. Handayani *et al.,* "Design and development of facial recognition based library management system (FRLMS)," in *2018 Int. Conf. on Computing, Engineering, and Design (ICCED)*, Bangkok, Thailand, pp. 119–124, 2018. https://doi.org/10.1109/ICCED.2018.00032

[26] Y. Cheng, H. Meng, Y. Lei and X. Tan, "Research on privacy protection technology in face identity authentication system based on edge computing," in *2021 Institute of Electrical and Electronics Engineers Int. Conf. on Artificial Intelligence and Industrial Design (AIID)*, Guangzhou, China, pp. 438–449, 2021. https://doi.org/10.1109/AIID51893.2021.9456477

[27] L. Yadav, R. K. Yadav and V. Kumar, "An efficient approach towards face recognition using deep reinforcement learning, Viola Jones and K-nearest neighbor," in *2021 2nd Int. Conf. on Advances in Computing, Communication, Embedded and Secure Systems (ACCESS)*, Ernakulam, India, pp. 112–117, 2021. https://doi.org/10.1109/ACCESS51619.2021.9563326

[28] S. M. Qaisar, M. Krichen and A. Mihoub, "Hand gesture recognition based on shape context analysis," in *2021 1st Int. Conf. on Artificial Intelligence and Data Analytics (CAIDA)*, Riyadh, Saudi Arabia, pp. 127–131, 2021. https://doi.org/10.1109/CAIDA51941.2021.9425200

[29] S. Suryakala, K. Muthumeenakshi and S. J. Gladwin, "Vision based vehicle/pedestrian detection in traffic surveillance system," in *2019 Int. Conf. on Communication and Signal Processing (ICCSP)*, Chennai, India, pp. 0506–0510, 2019. https://doi.org/10.1109/ICCSP.2019.8697954

[30] E. Pranav, S. Kamal, C. Satheesh Chandran and M. H. Supriya, "Facial emotion recognition using deep convolutional neural network," in *2020 Int. Conf. on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India, pp. 317–320, 2020. https://doi.org/10.1109/ICACCS48705.2020.9074302

[31] V. C. Hu, D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang *et al.,* "Guide to attribute-based access control (ABAC) definition and considerations (draft)," *NIST special publication*, vol. 800, no. 162, pp. 1–54, 2013.

[32] R. Poojary and A. Pai, "Comparative study of model optimization techniques in fine-tuned CNN models," in *2019 Int. Conf. on Electrical and Computing Technologies and Applications (ICECTA)*, Ras Al Khaimah, United Arab Emirates, pp. 1–4, 2019. https://doi.org/10.1109/ICECTA48151.2019.8959681

[33] K. Krishnaveni and G. R. Priyadharsini, "Evaluating the performance of facial expression recognition model via various classifiers," in *2021 Third Int. Conf. on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, Tirunelveli, India, pp. 925–929, 2021. https://doi.org/10.1109/ICICV50876.2021.9388472

[34] Z. Xin, L. Liu and G. Hancke, "AACS: Attribute-based access control mechanism for smart locks," *Symmetry*, vol. 12, no. 6, pp. –1050, 2020. https://doi.org/10.3390/sym12061050

[35] A. Liu, X. Du and N. Wang, "Unstructured text resource access control attribute mining technology based on convolutional neural network," *Institute of Electrical and Electronics Engineers Access*, vol. 7, pp. 43031–43041, 2019. https://doi.org/10.1109/ACCESS.2019.2907815

[36] R. Xu, J. Joshi and P. Krishnamurthy, "An integrated privacy preserving attribute-based access control framework supporting secure deduplication," *Institute of Electrical and Electronics Engineers Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 706–721, 2021. https://doi.org/10.1109/TDSC.2019.2946073

[37] X. Qin, Y. Huang, Z. Yang and X. Li, "An access control scheme with fine-grained time constrained attributes based on smart contract and trapdoor," in *2016 26th Int. Conf. on Telecommunications (ICT)*, Hanoi, Vietnam, pp. 249–253, 2019. https://doi.org/10.1109/ICT.2019.8798859
[38] F. C. Chollet, Keras, 2015. [Online]. Available: https://github.com/fchollet/keras
[39] J. Zhou and C. -M. Pun, "Personal privacy protection via irrelevant faces tracking and pixelation in video live streaming," *Institute of Electrical and Electronics Engineers Transactions on Information Forensics and Security*, vol. 16, pp. 1088–1103, 2021. https://doi.org/10.1109/TIFS.2020.3029913
[40] M. Abadi, A. Agarwal, P. Barham, E. Brevdo, Z. Chen *et al.,* "TensorFlow: Large-scale machine learning on heterogeneous distributed systems," arXiv preprint arXiv: 1603.04467, 2016.
[41] P. Tam, S. Math, C. Nam and S. Kim, "Adaptive resource optimized edge federated learning in real-time image sensing classifications," *Institute of Electrical and Electronics Engineers Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 14, pp. 10929–10940, 2021. https://doi.org/10.1109/JSTARS.2021.3120724
[42] Y. Yang, F. Duan, M. Zhang, J. Liu, J. Li *et al.,* "Privacy protection management model for internet of things data," in *Proc. of 7th Institute of Electrical and Electronics Engineers Int. Conf. on Data Science in Cyberspace (DSC)*, Guilin, China, pp. 219–226, 2022. https://doi.org/10.1109/DSC55868.2022.00036
[43] F. Avorgbedor and J. Liu, "Enhancing user privacy protection by enforcing Clark-Wilson security model on facebook," in *2020 Institute of Electrical and Electronics Engineers International Conference on Electro Information Technology (EIT)*, pp. 155–161, 2020. https://doi.org/10.1109/EIT48999.2020.9208279
[44] F. Rastoceanu, D. Hritcu, C. Grozea and M. Lazar, "Securing personal data in a video identification system," in *2022 14th Int. Conf. on Communications (ICC)*, Bucharest, Romania, pp. 1–6, 2022. https://doi.org/10.1109/COMM54429.2022.9817196
[45] J. Dave, A. Khan, B. Gupta, A. Gangwar and S. Suman, "Human-computer interaction methodology to attain face liveness detection," in *2021 2nd Int. Conf. for Emerging Technology (INCET)*, Belgaum, India, pp. 1–4, 2021.