A Fine-Grained Access Control and Security Approach for Intelligent Vehicular Transport in 6G Communication System

Zhili Zhou, *Member, IEEE*, Akshat Gaurav, *Graduate Student Member, IEEE*, Brij Bhooshan Gupta, *Senior Member, IEEE*, Miltiadis D. Lytras, *Member, IEEE*, and Imran Razzak, *Senior Member, IEEE*

***Abstract*— The area of intelligent transport systems (ITS) is attracting growing attention because of the integration of the smart IoT with vehicles that improve user safety and overall travel experience. Vehicular ad hoc network (VANET) is the part of ITS; that deals with the routing protocols and security of smart vehicles. However, due to the rapid increase in the number of smart vehicles, the existing network technology's resources unable to handle the traffic load. It expects that the 6G communication system has the ability to fulfill the requirements of VANETs. Only a few studies explore this area, but they also overlooked the security aspect of VANETs in 6G communications networks. In this paper, we present an approach to address authentication and security issues for vehicles in VANET. By authenticating cars in the VANET and identifying various cyber assaults such as DDoS, our method significantly contributes to the intelligent transport communication network. Our approach uses the concepts of identity-based encryption to provide access control to the vehicles and deep learning-based techniques for filtering malicious packets. Our identity-based encryption technique is IND-sID-CCA secure, and a state-of-the-art deep learning algorithm detects malicious packets with an accuracy of 99.72%. These results emphasize the validity of our proposed approach for VANETs in 6G communication systems.**

***Index Terms*— 6G, VANET, IoT, identity-based encryption, deep learning.**

I. Introduction

NUMEROUS individuals have died or been seriously injured in traffic accidents, and patients are frequently unable to reach hospitals on time. Therefore, researchers developed the concept of Vehicular ad hoc network (VANET) in order to increase road safety by establishing standards for vehicle-to-vehicle communication [1]. In VANET, smart vehicles share information that can be used at the time of a pandemic situation to save human lives. The US Federal Communication Commission was the first organization that understood the importance of smart transport systems, and it allocates a 75 MHz bandwidth of 5.9 GHz band to DSRC. In IEEE starts developing WAVE standards for VANET, which are the improvising versions of DSRC standards. VANET consists of moving vehicles equipped with the OBU and stationary RSU's. Initially, in VANET, two types of communication are possible: V2V, in which different smart vehicles communicate with one another, and V2I, in which the smart vehicle shares data with the RSU. However, as technology advances and the number of vehicles increases, numerous new modes of communication are introduced, including V2X (vehicle to everything), V2P (vehicle to pedestrian), and V2N (vehicle to cloud) [2].

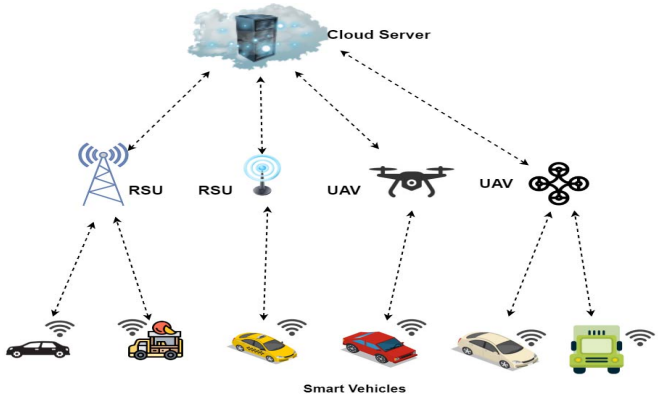

Fig. 1. VANET working in 6G communication system.

Until now, the requirements of the VANET network were fulfilled by the 5G network [3]. However, with the increase in the facilities and number of vehicles, the 5G network is not able to provide ultra-high latency services, security, and high reliability to the VANET devices [4]. Hence, researchers propose that the VANET should be powered by an AI-enabled 6G network [5]–[9]. An ideal 6G enabled VANET network communication is represented in Figure 1. As represented in Figure 1 the smart vehicles can share and access the data

Manuscript received 16 May 2021; revised 7 August 2021; accepted 17 August 2021. Date of publication 2 September 2021; date of current version 8 July 2022. This work was supported in part by the National Natural Science Foundation of China under Grant 61972205, in part by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD) Fund, and in part by the Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET) Fund, China. The Associate Editor for this article was S. Mumtaz. *(Corresponding authors: Brij Bhooshan Gupta and Zhili Zhou.)*

Zhili Zhou is with the Engineering Research Center of Digital Forensics, Ministry of Education, School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China (e-mail: zhou_zhili@163.com).

Akshat Gaurav is with Ronin Institute, Montclair, NJ 07043 USA (e-mail: akshatgaurav470@gmail.com).

Brij Bhooshan Gupta is with the Department of Computer Engineering, National Institute of Technology Kurukshetra, Kurukshetra, Haryana 136119, India, and also with the Department of Computer Science and Information Engineering, Asia University, Wufeng, Taichung 41354, Taiwan (e-mail: gupta.brij@gmail.com).

Miltiadis D. Lytras is with The American College of Greece, King Abdulaziz University, Jeddah 21589, Saudi Arabia (e-mail: mlytras@acg.edu).

Imran Razzak is with Deakin University, Burwood, Vic 3220, Australia (e-mail: imran.razzak@ieee.org).

Digital Object Identifier 10.1109/TITS.2021.3106825

through different sources like UAV, satellites, IoT [10], [11], or fog nodes. 6G enabled VANET has many advantages, as the AI feature of 6G improves the reliability and security of VANET devices, and it is easy to implement machine learning and deep learning techniques in the VANET network. 6G communication network applications are also vulnerable to a number of distinct threats. AI and VLC technology are often used in connected robots and autonomous systems, which may make it difficult to detect fraudulent activity, secure data transfer, and protect against data theft [12]. In this context, this work describes the implementation of a secure data sharing method along with a cyber-attack detection method by using identity-based encryption (IBE) and deep learning techniques. The proposed approach employs the concept of identity-based encryption to manage access control to the VANET's smart vehicles, ensuring that no personal data is leaked. Deep learning technology is used to analyze the anomalies in the traffic and filter out the malicious packets. As the 6G network is IA enabled, it is efficient to implement deep learning and IBE techniques. The smart vehicle in the VANET environment shares a large amount of personal data. But due to limited computation power and limited network compatibility, implementing adequate security measures is challenging. However, this research presents a technique through which smart devices in a VANET environment can achieve privacy and security with their limited resources in a 6G network.

The rest of the paper is organized as follows: section II discusses the previous work in the field of 6G enabled VANET environment. This is followed by section III, which gives the technical knowledge about IBE, which is helpful to understand our proposed approach. section IV and section V cover the system model and the proposed methodology, respectively. The paper will then go on to analyze the implementation results in section VI. Finally, section VII concludes the paper.

II. Related Work

6G is a relatively new topic; the first white paper, related to the 6G communication system, was drafted in 2019 on the first 6G summit in Finland [12]. 6G communication systems have many advantages compared to traditional 5G communication systems. The 6G communication system has better AI compatibility [5], [13] and integration of security tools [14] compared to the 5G communication systems. Due to these advantages of 6G communication systems, many private and government organizations spend money on further research in 6G communication systems [15]. Smart edges, distributed AI, 3D intercoms, and smart radio are the four integral parts of 6G communication systems.

VANET [16] provides a smart transport system, which improves road safety [17], [18]. However, VANET involves smart vehicles that have limited computational power; these vehicles share personal and private information, due to which VANET is targeted by different types of cyberattacks like; data leakage, DoS, DDoS, Blackhole attack, etc. [19]–[22]. Many detection methods were proposed by the researchers for the detection of different types of cyberattacks in the VANET environment [23], [24]. However, most of the cyber attack detection techniques are not able to give an efficient result for the VANET scenario because of the limited resources of the present communication system. However, along with 6G communication systems, it is easy to apply complex detection methods like deep learning techniques for detecting different types of cyberattacks. Deep learning techniques extract the features from raw data automatically that improves the response time of the detection process [25]. In [26] author presents a rigorous technique applicable for the detection of malicious traffic in the VANET environment. The proposed technique uses a convolution neural network (CNN) and Long Short-Term Memory (LSTM). Feature extraction of incoming data traffic is done by CNN, and then LSTM uses those features to analyze the traffic characteristics.

Other than intrusion detection, data leakage is also a critical issue in the VANET environment. The data leaking problem can be resolved by implementing access control methods that enable the data generator to apply rules to the data, ensuring that only authorized users have access to it. Researchers have proposed a variety of access control systems in recent years, including identity-based access control, attribute-based access control, and capability-based access control [27]–[31]. In their carefully designed study, the authors [32] present an IBE scheme that provides a fine-grained access control mechanism for smart devices. The proposed approach uses the unique identity of users to encrypt the data, and the encrypted data is uploaded to the cloud storage. In [33] authors presents a hybrid technique to provide an access control mechanism that uses the concept of blockchain, ABE, and IBE. All previously proposed access control methods are based on bilinear maps; however, the authors in [34] present the access control technique that is based on Lagrange interpolation. The author suggests that, due to the use of the Lagrange interpolation method, the computation cost of the proposed method is reduced. However, the proposed approach ignores the revocation mechanism. In [35] author overcome this limitation by shifting the complex encryption and decryption process to the cloud server that will improve the response time and provide adequate access control.

Although all the access control and attack detection schemes defined above are efficient, they do not consider the advantages of the 6G communication system. The area of the fine-grained access control method in the 6G communication system has not been explored in depth.

III. Preliminaries

Background information needed for the development of identity-based encryption is given in this section. The list of abbreviations used in this section is represented in Table I.

A. Bilinear Map

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of order $m \in \mathbb{Z}_p^*$. Then function $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_2$ fulfills the following properties.

- **Bilinera**: The function $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_2$ is bilinear if

$$\hat{e}(xA, yB) = \hat{e}(A, B)^{xy}; \quad \forall x, y \in \mathbb{Z}; \ \forall A, B \in \mathbb{G}_1$$

TABLE I
LIST OF ABBREVIATIONS

Abbreviation	Meaning
$\mathbb{G}$	Cyclic Group
g	Generator of group $\mathbb{G}$
$\hat{e}$	Bilinear Map
S	Security parameter
M_s	Master Secret
P_{key}	Private Key
P_r	Public parameters
$\mathcal{M}$	Message Space
$\mathcal{C}$	Cipher Space
C_{text}	Cipher Text
M_{text}	Message
ID	Unique identification

- **Non-degenerate**: Pairs of $\mathbb{G}_1 \times \mathbb{G}_{\not\perp}$ not mapped to the identity function of $\mathbb{G}_2$

$$\hat{e}(m, m) \neq 1_{\mathbb{G}_2}$$

- **Efficient**: There exists and efficient algorithm for the calculation of $\hat{e}$(A,B), A,B $\in \mathbb{G}_1$

B. Computational Diffie-Hellman Assumption

Let $\mathbb{G}$ be a cyclic group of order p and generator g. Then for a polynomial-time (q) algorithm $\mathcal{A}$ it is impossible to compute g^{xy} from g, g^x, g^y, where x,y $\in \mathbb{Z}_p^*$

$$Pr\left[\mathcal{A}(q, g, g^x, g^y) = g^{xy}\right] > \frac{1}{n^\beta}$$

where n is large and $\beta > 0$.

C. Decisional Diffie-Hellman Assumption

An algorithm $\mathcal{A}$ for a multiclative cyclic group $\mathbb{G}$ of generator g is called DDH algorithm if it satisfies the following property:

$$\left|Pr\left[\mathcal{A}(q, g, g^x, g^y, g^{xy}) = 1\right] - Pr\left[\mathcal{A}(q, g, g^x, g^y, g^z) = 1\right]\right| > \frac{1}{n}$$

where n is large and x,y,z $\in \mathbb{G}$.

D. Identity-Based Encryption (IBE)

IBE is proposed by Shamir [36] to overcome the limitations of asymmetric key encryption. Unlike asymmetric key encryption, there is no need for certifying authority in the IBE, and the unique identity of the user is used to generate the public key. Therefore, through IBE, many-to-one encryption requires fewer memory requirements. Hence, limited computational power devices in 6G communication systems mostly use the IBE technique for encryption and access control. The example communication between Alice and Bob using IBE is represented in Figure 2. If Alice wants to communicate with Bob, then she encrypts the message using the identity of Bob, and at the receiver end, Bob decrypts the message by his private key that is generated by the private key generator. Following are the four building blocks of the IBE technique.

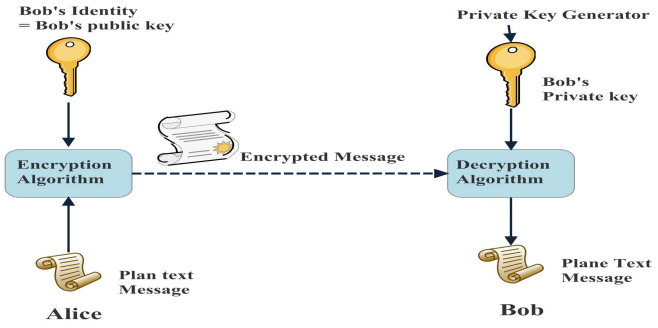

Fig. 2. Identity based encryption.

- **Setup**: The IBE algorithm takes the security parameter S and produces the master key M_s and public parameters P_r.

$$(p_1, p_2, \ldots p_n, M_s) \xleftarrow{\$} \mathcal{G}(1^k)$$

where $\{p_1, p_2, ..p_n\} \in P_r$ and M_s is the master secret.

- **Extraction**: The IBE algorithm takes the unique ID of the user, public parameters, and master key and generates the private key of the user.

$$P_{key} \xleftarrow{\$} \{p \in P_r, ID \leftarrow \{1, 0\}^*, M_s\}$$

- **Encryption**: This set provides access control and by encrypting the data. The user encrypts the data using his unique ID and public parameters.

$$C_{text} \in \mathcal{C} \xleftarrow{\$} \{M_{text} \in \mathcal{M}, p \in P_r, ID \leftarrow \{0, 1\}^*, M_r\}$$

- **Decryption**: This is the reverse process of encryption, in this, the receiver extracts the message using its secret key.

$$M_{text} \in \mathcal{M} \leftarrow \{C_{text} \in \mathcal{C}, p \in P_r, P_{key}\}$$

IV. SYSTEM MODEL

The previous section establishes the technological basis upon which our suggested framework is built. Now, in this section, we'll go further into the details of our proposed framework. Our proposed system makes use of both the IBE concept and deep learning techniques for access control and malicious packet filtering, two critical components of network security. However, before we describe our suggested method, we shall discuss the proposed system model in depth. The system model for the proposed approach is divided into three different layers, each with its own significance. (Figure 3) represents the system model and the importance of each layer is represented as follows:

- **Physical Layer**: It consists of smart vehicles, that are the basic building blocks of the VANET environments. Smart vehicle generates a large amount of data in different forms. This generated data consists of personal and private information about the vehicles. The generated data is forwarded to the stationary RSU or other processing devices through a 6G communication system.

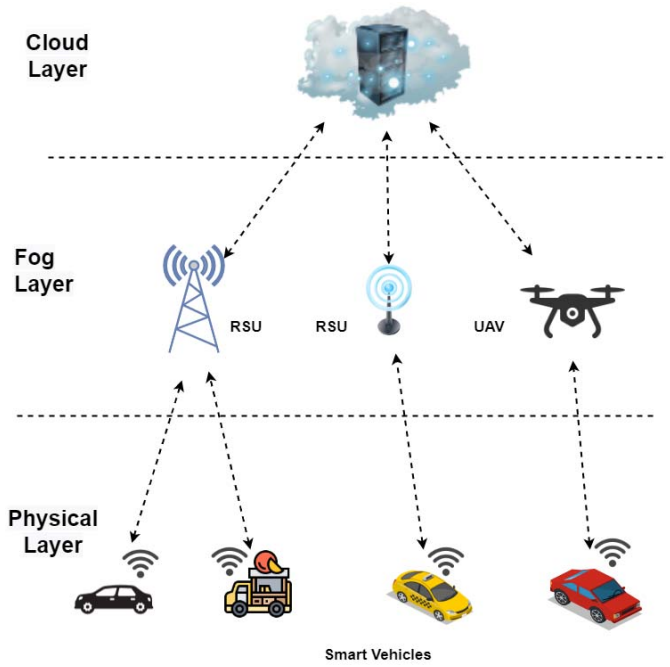

Fig. 3. System model.

- **Fog node layer**: At the start of the VANET technology, the data generated by the smart devices are stored directly at the cloud storage, however, this increases latency and time delay. Therefore, the concept of fog computing is introduced, in which the uploaded data is at first prepossessed at the fog node [37], [38]. In our proposed framework, the stationary RSU or smart device that has high computational power can act as the fog node. Two different fog nodes can communicate and share the data for fast prepossessing.
- **Cloud layer**: It provides the processing and storage services to the VANET network. The data generated by the smart vehicles are stored at the cloud storage for further processing.

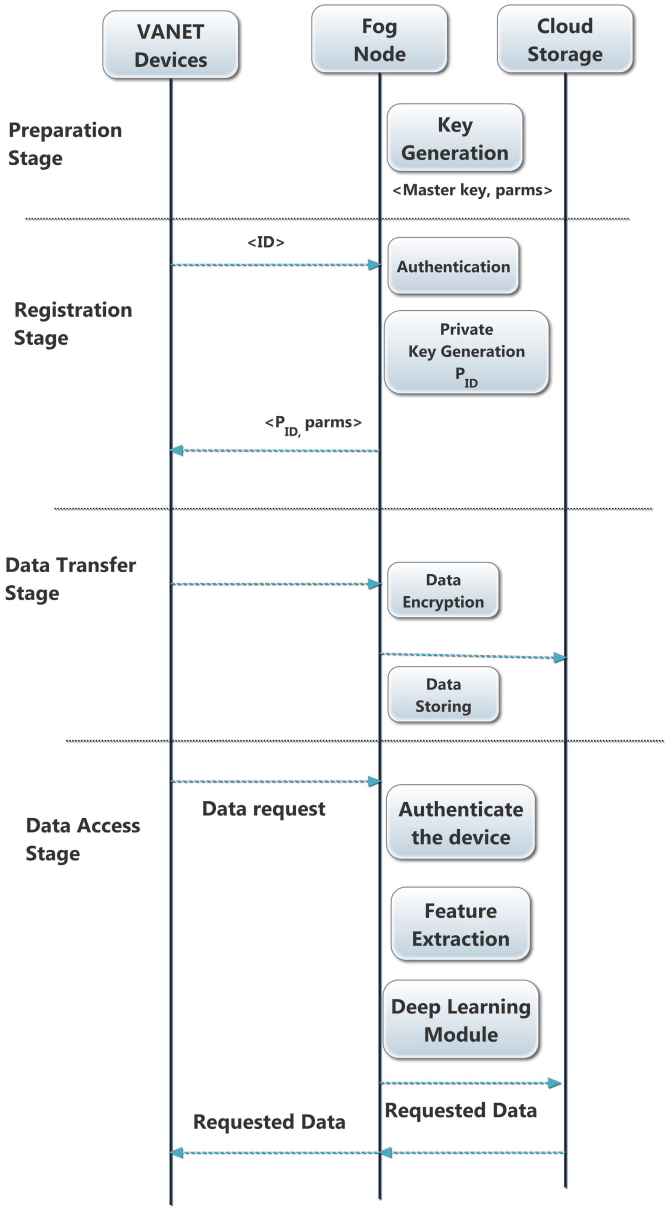

Fig. 4. State diagram of proposed approach.

A. System Interaction

In this section, we will explain the working of our proposed approach. The state diagram of our proposed approach is represented in Figure 4. In our proposed approach, all complex computation related to encryption and key generation is done at the fog node.

- **Preparation Stage**: This is the initial stage of our proposed approach, in this stage, the fog node selects the security (S) parameter and generates the master secret (M_S) and public parameters (P_r).
- **Registration Stage**: This is the second stage of our proposed approach. Whenever a new smart vehicle comes under the range of the fog node, it requests for the secret key and the public parameters, and the fog node generates the secret key according to the unique ID of the smart vehicle.
- **Data Transfer Stage**: In this stage, the smart vehicle starts generating the data, and this data is firstly encrypted by the fog node and then stored at the cloud storage.
- **Data Access Stage**: This is the final stage of the conversation. In this stage, smart vehicles send the access request to the fog node, and the fog node first authenticates the smart vehicle. After authentication, the fog node uses the deep learning model to analyze the packet, and if the packet is legitimate, then only the data request is forwarded to the cloud server.

Assumption 1: The smart device has a unique $ID_i, i \in \mathbb{Z}_p^*$. Where n is the number of smart devices

V. Proposed Methodology

In this section, we give the details of our proposed approach. In the first part of the section, we explain the

identity-based encryption approach. In the later part of the section, the details about the deep learning approach that is used for the detection of malicious packets are explained.

A. Identity-Based Encryption

As explained in the system model, there are 'n' smart vehicles in a region, each has a unique identity (ID). Each smart vehicle collects information from its surroundings and transfers that information to the cloud server through RSU and fog servers.

1) Set-up Phase: As explained in section III, in this phase, the public parameters and the master secret key are generated, and finally, the plain text message is encrypted into the ciphertext. algorithm 1 represents this phase.

Algorithm 1 Set up Phase

Input: Security parameter (S)
Output: Ciphertext (C_{text}) and Index (H)
Begin:
$S \in \mathbb{Z}^*$
$\{params, M_s\} \xleftarrow{\$} \mathcal{G}1^s$
$C_{text1} \xleftarrow{\$} g^{rID}$, where ID $\leftarrow \{0,1\}^*$
$C_{text2} \xleftarrow{\$} Y^r, r \in \mathbb{G}$,
$C_{text3} \xleftarrow{\$} \hat{e}(g,g)^r.M_{text}$,
where $M_{text} \in \mathcal{M}, message\ space$
$C_{text} = (C_{text1}, C_{text2}, C_{text3})$
$C_{text} = (C_{text1}, C_{text2}, C_{text3})$, where $C_{text} \in \mathcal{C}$,
Cipher Space
Hash $\leftarrow H(ID), WhereH : \{0,1\}^* \rightarrow \mathbb{Z}_P^*$
Data store at cloud server: (C_{text}, H(ID))
End

- **Key Generation**: In this stage, the public parameters and master key are generated. In order to keep our approach lightweight, we take fewer public parameters compared to [32].

$$(pram \in P_r, M_s) \xleftarrow{\$} \mathcal{G}(1)^S \tag{1}$$
$$pram = (g, Y) \tag{2}$$
$$M_r = y \tag{3}$$

  where Y = g^y; $y \in \mathbb{Z}_p^*$; g is the generator of the cyclic group $\mathbb{G}$.
- **Encryption**: The plain text ($M \in \mathcal{M}$) is encrypted with the help of the unique ID of the user and *parma*. The final ciphertext ($C_{text} \in \mathcal{C}$) is calculated as follows

$$C_{text1} = g^{rID} \tag{4}$$
$$C_{text2} = Y^r \tag{5}$$
$$C_{text3} = \hat{e}(g,g)^r.M_{text} \tag{6}$$
$$C_{text} = (C_{text1}, C_{text2}, C_{text3}) \tag{7}$$

  where $r \in \mathbb{Z}_p^*$, ID $\leftarrow \{0,1\}^*$

2) Private Key Generation Phase: In this phase, the private key of the user is generated by the private key generator using the master key parameter and the unique ID of the user.

$$P_{key} \leftarrow g^{\frac{1}{TD+yt}} \tag{8}$$

where $t \in \mathbb{Z}_p^*$

3) Encryption Phase: In this phase, the plane text message ($M_{text} \in \mathcal{M}$) is generated from the cipher text ($C_{text} \in \mathcal{C}$). The message is generated by using Equation 9, and this process is represented in algorithm 2.

$$M_{text} \in \mathcal{M} \leftarrow (C_{text1}C_{text2}^t, P_{key}) \tag{9}$$

Algorithm 2 Ecryption Phase

Input: Ciphertext ($C_{text} \in \mathcal{C}$)
Output: Planetext ($M_{text} \in \mathcal{M}$)
Begin:
$t \in \mathbb{Z}_p^*$
$P_{key} \leftarrow (r, ID \leftarrow \{0,1\}^*, P_r)$
$P_{key} = g^{\frac{1}{TD+yt}}$
$C_{temp} \leftarrow C_{text1}C_{text2}^t$
$M'_{text} \leftarrow \frac{C_{text3}}{C_{temp}}$
return: Decrypted Message M'_{text}
End:

Lemma 1: Equation 9 correctly decrypet the cipher text ($C'_{text} \in \mathcal{C}$) and generate the message ($M'_{text} \in \mathcal{M}$)
Proof: Let calculate the three parts of the ciphertext using Equation 4, Equation 5, and Equation 6.

$$C'_{text1} = g^{rID} \tag{10}$$
$$C'_{text2} = Y^r \tag{11}$$
$$C'_{text3} = \hat{e}(g,g)^r.M'_{text} \tag{12}$$

The message is encrypted using Equation 9

$$\hat{e}(C'_{text1}C_{text2}^t, P_{key}) = \hat{e}(g^{rID}Y^t, P_{key}) \tag{13}$$
$$= \hat{e}(g^{rID}g^{ryt}, g^{\frac{1}{TD+yt}}) \tag{14}$$
$$= \hat{e}(g^{(rID+ryt)}, g^{\frac{1}{TD+yt}}) \tag{15}$$
$$= \hat{e}(g^{r(ID+yt)}, g^{\frac{1}{TD+yt}}) \tag{16}$$

As $\hat{j}$ is an admissible bilinear function by using properties of bilinear map, Equation 16 reduce as following:

$$\hat{e}(C'_{text1}C_{text2}^t, P_{text}) = \hat{e}(g,g)^{r.\left(\frac{ID+yt}{TD+yt}\right)} \tag{17}$$
$$= \hat{e}(g,g)^r \tag{18}$$

Substitute the value of $\hat{e}(g,g)^r$ from Equation 18 into Equation 12, we can calculate the value of message(M_{rext}).

$$\frac{C'_{text3}}{\hat{e}(C'_{text1}C_{text2}^t, P_{key})} = M'_{text} \tag{19}$$

Theorem 1: The proposed identity-based approach provides access control, i.e., only the authorized user can decrypt the data.

Proof: Let an adversary $\mathcal{A}$ of unique id (ID_A) wants to access the ciphertext (C_{text}) generated for legitimated user (ID_1). The adversary $\mathcal{A}$ firstly split the ciphertext is using the Equation 4, Equation 5, and Equation 6.

$$C'_{text1} = g^{r'ID_1} \tag{20}$$
$$C'_{text2} = Y^{r't} \tag{21}$$
$$C'_{text3} = e(g,g)^{r}.M'_{text} \tag{22}$$
$$C' = (C'_{text1}, C'_{text2}, C'_{text3}) \tag{23}$$

The adversary first generates its private key and then tries to decrypt this ciphertext using Equation 9.

$$P_{key_A} = g^{\frac{1}{TD_A+yt}} \tag{24}$$
$$\frac{C'_{text3}}{\hat{e}(C'_{text1}C'^{t}_{text2}, P_{key_A})} = \frac{\hat{e}(g,g)^{r}.M_{text}}{\hat{e}(g^{r'ID}Y^{r't}, g^{\frac{1}{TD_A+yt}})} \tag{25}$$
$$= \frac{\hat{e}(g,g)^{r'}.M_{text}}{\hat{e}(g^{r'ID}g^{yr't}, g^{\frac{1}{TD_A+yt}})} \tag{26}$$
$$= \frac{\hat{e}(g,g)^{r'}.M_{text}}{\hat{e}(g^{r'ID+yr's}, g^{\frac{1}{TD_A+y}})} \tag{27}$$
$$= \frac{\hat{e}(g,g)^{r'}.M_{text}}{\hat{e}(g^{r'(ID+yt)}, g^{\frac{1}{TD_A+yt}})} \tag{28}$$
$$= \frac{\hat{t}(g,g)^{r'}.M_{text}}{\hat{e}(g,g)^{\frac{r'(ID+yt)}{(TD_A+yt)}}} \tag{29}$$
$$= \perp (because\ ID \neq ID_A) \tag{30}$$

Algorithm 3 Dataset Prepossessing

Input: Raw dataset
Output: Processed Dataset
Start
while $i_{elements} \neq \emptyset$ **do**
  Column addition to the dataset
  if i^{th} *entry is normal* **then**
    $i_{tag} \leftarrow$normal
  end
  else
    $i_{tag} \leftarrow$malicious
  end
  $i \leftarrow i+1$
end
Normalize the dataset
Split the dataset into training and test
End

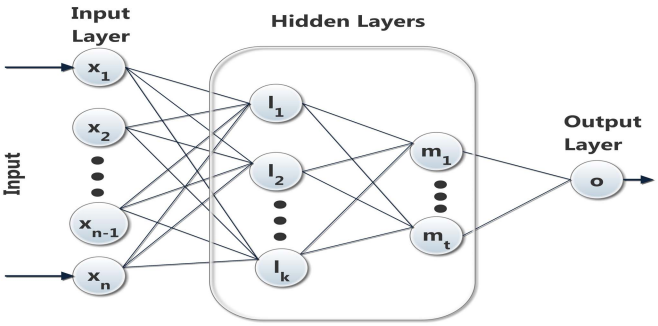

Fig. 5. Deep learning model.

B. Deep Learning-Based Approach

We use the Deep Learning approach for the detection of anomalies in 6G communication systems. There are many deep learning models available for the detection of traffic anomalies, but most of them are not suitable for the limited computational power devices in the VANET network. Only a few researchers have addressed this issue, therefore, we developed our approach that solves this issue. We adopt a lightweight deep learning model that takes only two hidden layers. As the number of hidden layers decreases, the response time of the proposed approach reduces, and the smart vehicle quickly filters out the malicious traffic components.

We use the KDDCUP99 dataset [39] to train our proposed deep learning model. We use the KDDCUP99 data set because it contains different types of cyber attacks, hence, training on the KDDCUP99 data set improves the performance of our deep learning model. However, before training the model, we have to preprocess the dataset and add tags and names to the columns of the data set. algorithm 3 is used to add tags to the dataset, normalized dataset, and splitting the dataset into training and testing datasets.

After prepossessing the dataset, we prepare our deep learning model. Our deep learning model has two hidden layers as represented in Figure 5. The traffic is applied to the input layer, which has 'n' neurons, and each neuron is connected to the next layer through a weight $\mathcal{W}$. This connection of neurons to the next layer through unique weights is kept on repeating until the output layer. At the output layer, the packets in the traffic are tagged as normal or malicious according to their behavior.

We use the following equations to calculate the value of each neuron in the hidden layer.

$$\mathcal{I} = \{j_1, j_2, j_3, \ldots, j_{n-1}, j_n\} \tag{31}$$
$$\mathcal{L}_1 = \sigma(j_1 \times \mathcal{W}_{11} + j_2 \times \mathcal{W}_{21} + \cdots + i_n \times \mathcal{W}_{n1} + \mathcal{B}_1) \tag{32}$$
$$\mathcal{L}_j = \sigma\left(\sum_{i=0}^{i=k} j_i \times \mathcal{W}_{ji}\right) + \mathcal{B}_k \tag{33}$$
$$\mathcal{O} = \sigma(m_1 \times \mathcal{W}_{1o} + m_2 \times \mathcal{W}_{2o} + \cdots + m_t \times \mathcal{W}_{to} + \mathcal{B}_o) \tag{34}$$

where $\mathcal{I}$ represents the input layer, $\mathcal{L}$ represents hidden layers, $\mathcal{W}$ represents the unique weight, σ represents activation function, $\mathcal{O}$ represents the output layer, and $\mathcal{B}$ represents Bias function.

For our proposed approach, we chose the ReLU activation function, whose value changes according to Equation 35.

$$\sigma(i) = \begin{cases} 0 & \text{if } i < 0 \\ i & \text{if } i \geq 0 \end{cases} \tag{35}$$

The working of our deep learning model is represented in algorithm 4, and its details are as following:

Algorithm 4 Deep Learning Module

Input: Incoming Traffic
Output: Identification of Traffic
Begin
$\mathcal{F} \leftarrow \emptyset$
for $\forall \mathcal{P}_i \; in \; \nabla t$ **do**
  $\mathcal{F}_i \leftarrow \mathcal{P}_i^f$
  Apply Deep Learning Model
  $\mathcal{L}_i \leftarrow \mathcal{P}_i^l$
  if $\mathcal{L}_i = Legitimated$ **then**
    Pass the Packet
  end
  else
    Discard the Packet
  end
end
End

- Our deep learning model analysis the incoming traffic for every time window ∇t.
- For each packet ($\mathcal{P}_i$) in the time window ∇t extract the features $\mathcal{F}_i$ of the packet.
- Apply the traffic to the deep learning model and calculate the output label $\mathcal{L}_i$ for the packet.
- IF the $\mathcal{L}_i$ is legitimated then forward the packet.
- If the $\mathcal{L}_i$ is malicious then discard the packet.

VI. Results and Analysis

Our proposed approach provides access control to the smart vehicles in the VANET environment by using an identity-based encryption technique. In addition to access control, our proposed technique utilizes a deep learning model to filter dangerous packets from incoming traffic. In this section, we analyze the implementation results of both models.

We make use of the pairing-based library (PCB), an open-source C library for implementing pairing-based functions. To install the PCB library and simulation IBE method, we utilize an Ubuntu 15.04 computer with 8 GB of RAM.

To analyze the IBE approach, we take ten different test cases. Each test case takes a unique value of the message and user ID and then calculates the ciphertext: C_1, C_2, C_3. The values of C_1, C_2, C_3 are calculated by using Equation 4, Equation 5, and Equation 6. The decryption of ciphertext is done by Equation 9.

The comparison of simulation results for different test cases is represented in Figure 6. The key generation time is calculated by using algorithm 1 and is represented in Figure 6. As Figure 6 shows, the time required to construct the public parameters and the master secret will vary depending on the contents of the message and unique ID values. However, the variation in key generation time is not very large. Message encryption variation can be found in Figure 6. From Figure 6, we can see that the message encryption time slightly varies with the change in message values. Hence, we can interpret that in our proposed approach the data encryption time is nearly constant. If we closely analyze the message

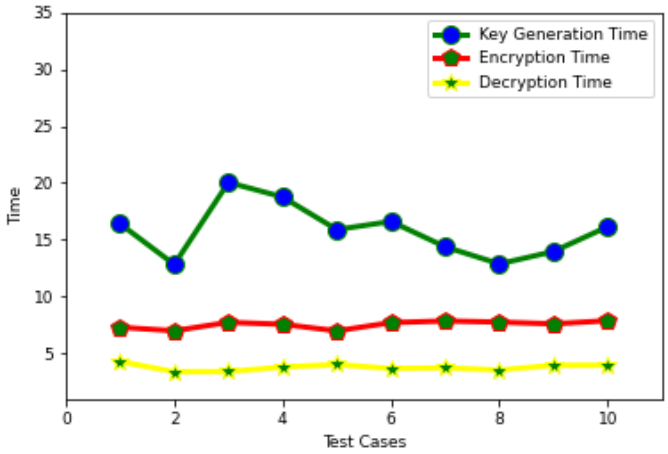

Fig. 6. Identity-based encryption simulation results.

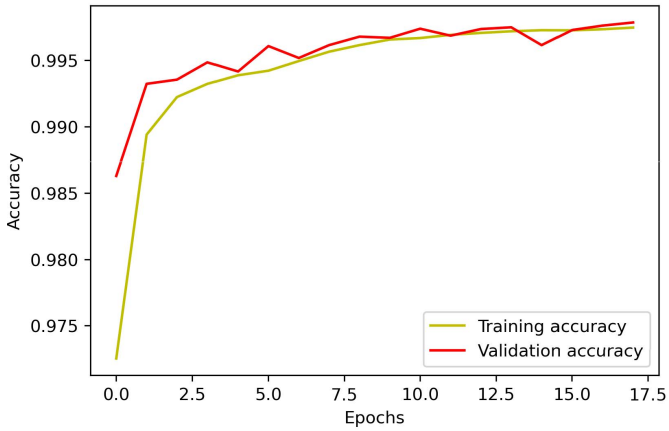

Fig. 7. Variation of accuracy.

decryption time represented in Figure 6, we can see that the data decryption time also slightly varies with the change of message value. Simulation findings show that IBE achieves near-constant encryption and decryption times for varying message complexities.

A. State-of-Art Comparison

In this subsection, we compare our proposed approach with other existing frameworks and techniques. For the state-of-art comparison, we use the following parameters:

- **Precision**: It measures the fraction of legitimated packets from total forwarded packets.

$$P = \frac{TruePositive}{TruePositive + FalsePositive} \tag{36}$$

- **Recall**: It measures the fraction of legitimated packets that are not discarded by the proposed approach.

$$R = \frac{TruePositive}{TruePositive + FalseNegative} \tag{37}$$

- **F1-score**: It measures the success of the proposed approach.

$$F1 - score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{38}$$

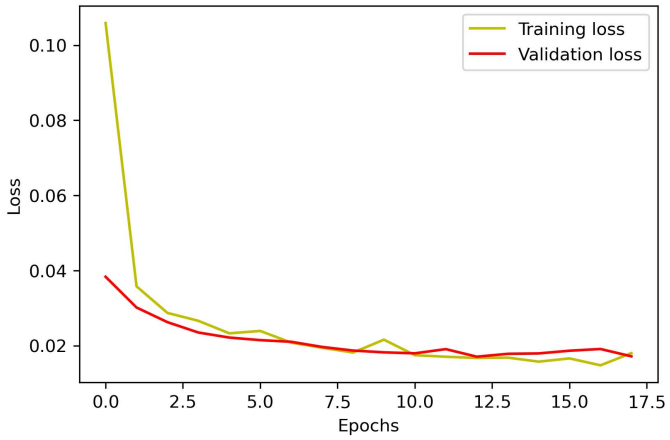

Fig. 8. Variation of loss.

TABLE II
COMPARISON OF OUR PROPOSED APPROACH WITH OTHER EXISTING TECHNIQUES

Model	Accuracy	Precision	Recall	F1-score
MLP	0.8874	0.8857	0.8631	0.8743
Bayes	0.9491	0.9156	0.9185	0.917
Random forest	0.9364	0.8999	0.8968	0.8983
1D-CNN	0.9514	0.9814	0.9017	0.93
LSTM	0.9624	0.9844	0.8989	0.8989
[40]	NA	0.78	0.65	0.69
[41]	NA	0.87	0.86	0.86
[42]	0.9888	0.9827	0.9952	0.9889
[43]	0.9841	0.9834	0.9847	0.9840
[44]	0.9809	NA	0.9593	NA
[45]	NA	NA	0.9474	NA
Our Approach	0.9973	0.96	0.97	0.97

- **Accuracy**: It measures the correctness of our proposed approach.

$$Accuracy = \frac{TruePositive + TrueNegative}{TotalPackets} \quad (39)$$

- **Loss**: It is used to check whether our proposed approach trained properly or not. To calculate the loss curve, we use the 'Categorical cross-entropy formula.

$$L(y, \widehat{y}) = -\sum_{j=0}^{M}\sum_{i=0}^{N}\left(y_{ij} \times \log(\widehat{y_{ij}})\right) \quad (40)$$

where 'y' is the true value and $\widehat{x}$ is the predicted value.

The accuracy and loss curves of our proposed technique are used to compare the performance of the method during training and testing. The accuracy of the measurement is determined by Equation 39, and the loss is calculated using the formula in Equation 40. Figure 7 and Figure 8 depict the variation in accuracy and loss throughout the course of training and testing (validating) time correspondingly. Due to the fact that the accuracy and loss curves change in a comparable manner during the training and validation periods, we may conclude that our proposed model is a good fit.

A comparison of our deep learning with standard machine learning techniques and other traffic filtering techniques is represented in Table II. From the Table II, it is clear that our proposed approach has the highest accuracy, precision, recall, and f1-score values.

VII. CONCLUSION

VANET is an integral part of ITS that focuses on providing safety to vehicle passengers. Early work in this area focused primarily on the development of new techniques and adding new gadgets to the vehicles that can enhance their performance. However, with the increase in the number of vehicles, the limited resources of 5G communication systems are not able to fulfill the requirement of the VANETs. Most studies on the development of VANET technologies have overlooked this issue. Few researchers have addressed this issue and proposed frameworks based on the 6G communication system. 6G Communication Systems provides AI-enabled network services to its users. Therefore, VANET's efficiency will be increased by using 6G communication systems. In this context, we present a framework that will provide access control to devices in the VANET environment and protect it from different cyber attacks. Our proposed framework is based on identity-based encryption (IBE) and deep learning techniques. IBE is used to manage access control, and a deep learning technique detects cyberattacks by analyzing the features of data traffic. We have obtained satisfactory results demonstrating that our proposed framework works properly in the 6G communication system. The strength of our work lies in the development framework that utilizes the resources of the 6G communication system. Our proposed framework represents an important first step toward the development of VANET security techniques for 6G communication systems. Our future studies should concentrate on the improvement of the proposed framework by integrating recent technologies.

REFERENCES

[1] M. Benadda and G. Belalem, "Improving road safety for driver malaise and sleepiness behind the wheel using vehicular cloud computing and body area networks," *Int. J. Softw. Sci. Comput. Intell.*, vol. 12, no. 4, pp. 19–41, 2020.

[2] M. Noor-A-Rahim *et al.*, "6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities," 2020, *arXiv:2012.07753*. [Online]. Available: http://arxiv.org/abs/2012.07753

[3] M. S. Omar *et al.*, "Multiobjective optimization in 5G hybrid networks," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1588–1597, Jun. 2018.

[4] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future intelligent and secure vehicular network toward 6G: Machine-learning approaches," *Proc. IEEE*, vol. 108, no. 2, pp. 292–307, Feb. 2020.

[5] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y.-J.-A. Zhang, "The roadmap to 6G: AI empowered wireless networks," *IEEE Commun. Mag.*, vol. 57, no. 8, pp. 84–90, Aug. 2019.

[6] H. Fatemidokht, M. K. Rafsanjani, B. B. Gupta, and C.-H. Hsu, "Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular ad hoc networks in intelligent transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4757–4769, Jul. 2021.

[7] H. Hiraishi, "Experience-based approach for cognitive vehicle research," *Int. J. Softw. Sci. Comput. Intell.*, vol. 12, no. 4, pp. 60–70, Oct. 2020.

[8] S. Mumtaz, H. Lundqvist, K. M. S. Huq, J. Rodriguez, and A. Radwan, "Smart direct-LTE communication: An energy saving perspective," *Ad Hoc Netw.*, vol. 13, pp. 296–311, Feb. 2014.

[9] K. M. S. Huq, S. Mumtaz, J. Rodriguez, P. Marques, B. Okyere, and V. Frascolla, "Enhanced C-RAN using D2D network," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 100–107, Mar. 2017.

[10] A. Al-Qerem, M. Alauthman, and A. Almomani, "IoT transaction processing through cooperative concurrency control on fog–cloud computing environment," *Soft Comput.*, vol. 24, no. 8, pp. 5695–5711, 2020.

[11] B. B. Gupta and M. Quamara, "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols," *Concurrency Comput. Pract. Exper.*, vol. 32, no. 21, p. e4946, Nov. 2020.

[12] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6G networks: New areas and new challenges," *Digit. Commun. Netw.*, vol. 6, no. 3, pp. 281–291, Aug. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352864820302431

[13] M. Z. Khan, S. Harous, S. U. Hassan, M. U. Ghani Khan, R. Iqbal, and S. Mumtaz, "Deep unified model for face recognition based on convolution neural network and edge computing," *IEEE Access*, vol. 7, pp. 72622–72633, 2019.

[14] T. Zhu, P. Xiong, G. Li, W. Zhou, and P. S. Yu, "Differentially private model publishing in cyber physical systems," *Future Gener. Comput. Syst.*, vol. 108, pp. 1297–1306, Jul. 2020.

[15] P. Yang, Y. Xiao, M. Xiao, and S. Li, "6G Wireless communications: Vision and potential techniques," *IEEE Netw.*, vol. 33, no. 4, pp. 70–75, Jul./Aug. 2019.

[16] J. Shu, L. Zhou, W. Zhang, X. Du, and M. Guizani, "Collaborative intrusion detection for VANETs: A deep learning-based distributed SDN approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4519–4530, Jul. 2020.

[17] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Veh. Commun.*, vol. 9, pp. 19–30, Jul. 2017.

[18] G. Guo and S. Wen, "Communication scheduling and control of a platoon of vehicles in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 6, pp. 1551–1563, Jun. 2016.

[19] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Netw.*, vol. 61, pp. 33–50, Jun. 2017.

[20] L. Xiao, X. Wan, C. Dai, X. Du, X. Chen, and M. Guizani, "Security in mobile edge caching with reinforcement learning," *IEEE Wireless Commun.*, vol. 25, no. 3, pp. 116–122, Jun. 2018.

[21] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2018.

[22] I. Cvitic, D. Perakovic, B. Gupta, and K.-K.-R. Choo, "Boosting-based DDoS detection in Internet of Things systems," *IEEE Internet Things J.*, early access, Jun. 21, 2021, doi: 10.1109/JIOT.2021.3090909.

[23] J. Liang, Q. Lin, J. Chen, and Y. Zhu, "A filter model based on hidden generalized mixture transition distribution model for intrusion detection system in vehicle ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 7, pp. 2707–2722, Jul. 2020.

[24] Y. Zeng, M. Qiu, Z. Ming, and M. Liu, "Senior2Local: A machine learning based intrusion detection method for VANETs," in *Proc. Int. Conf. Smart Comput. Commun.* Springer, 2018, pp. 417–426.

[25] M. Qiu *et al.*, "Data allocation for hybrid memory with genetic algorithm," *IEEE Trans. Emerging Topics Computing*, vol. 3, no. 4, pp. 544–555, Dec. 2015.

[26] Y. Zeng, M. Qiu, D. Zhu, Z. Xue, J. Xiong, and M. Liu, "DeepVCM: A deep learning based intrusion detection method in VANET," in *Proc. IEEE 5th Int. Conf. Big Data Secur. Cloud*, May 2019, pp. 288–293.

[27] Y. Liu *et al.*, "Capability-based IoT access control using blockchain," *Digital Communications and Networks*, vol. 4, Art. no. S2352864820302844, Oct. 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S2352864820302844

[28] X. Yang and W. Ding, "Researches on data encryption scheme based on CP-ASBE of cloud storage," *Int. J. High Perform. Comput. Netw.*, vol. 14, no. 2, pp. 219–228, 2019.

[29] S. Kaushik and C. Gandhi, "Capability based outsourced data access control with assured file deletion and efficient revocation with trust factor in cloud computing," *Int. J. Cloud Appl. Comput.*, vol. 10, no. 1, pp. 64–84, Jan. 2020.

[30] A. Tewari and B. B. Gupta, "Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags," *J. Supercomput.*, vol. 73, no. 3, pp. 1085–1102, Mar. 2017.

[31] F. Mirsadeghi, M. K. Rafsanjani, and B. B. Gupta, "A trust infrastructure based authentication method for clustered vehicular ad hoc networks," *Peer Netw. Appl.*, vol. 4, pp. 1–17, Oct. 2020.

[32] H. Yan, Y. Wang, C. Jia, J. Li, Y. Xiang, and W. Pedrycz, "IoT-FBAC: Function-based access control scheme using identity-based encryption in IoT," *Future Gener. Comput. Syst.*, vol. 95, pp. 344–353, Jun. 2019. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167739X1830997X

[33] S. Sun, R. Du, S. Chen, and W. Li, "Blockchain-based IoT access control system: Towards security, lightweight, and cross-domain," *IEEE Access*, vol. 9, pp. 36868–36878, 2021.

[34] C. Wan and J. Zhang, "Efficient identity-based data transmission for VANET," *J. Ambient Intell. Hum. Comput.*, vol. 9, no. 6, pp. 1861–1871, Nov. 2018.

[35] S.-J. Horng, C.-C. Lu, and W. Zhou, "An identity-based and revocable data-sharing scheme in VANETs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15933–15946, Dec. 2020.

[36] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances Cryptology* (Lecture Notes in Computer Science), vol. 196, G. R. Blakley and D. Chaum, Eds. Berlin, Germany: Springer, 1985, pp. 47–53. [Online]. Available: http://link.springer.com/10.1007/3-540-39568-7_5

[37] M. M. Hussain and M. M. S. Beg, "Using vehicles as fog infrastructures for transportation cyber-physical systems (T-CPS): Fog computing for vehicular networks," *Int. J. Softw. Sci. Comput. Intell.*, vol. 11, no. 1, pp. 47–69, Jan. 2019.

[38] S. P. Ahuja and N. Wheeler, "Architecture of fog-enabled and cloud-enhanced Internet of Things applications," *Int. J. Cloud Appl. Comput.*, vol. 10, no. 1, pp. 1–10, Jan. 2020.

[39] A. Divekar, M. Parekh, V. Savla, R. Mishra, and M. Shirole, "Benchmarking datasets for anomaly-based network intrusion detection: KDD CUP 99 alternatives," in *Proc. IEEE 3rd Int. Conf. Comput., Commun. Secur. (ICCCS)*, Oct. 2018, pp. 1–8.

[40] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2019, pp. 1–8.

[41] F. Hussain, S. Ghazanfar Abbas, M. Husnain, U. Ullah Fayyaz, F. Shahzad, and G. A. Shah, "IoT DoS and DDoS attack detection using ResNet," 2020, *arXiv:2012.01971*. [Online]. Available: http://arxiv.org/abs/2012.01971

[42] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martinez-del-Rincon, and D. Siracusa, "Lucid: A practical, lightweight deep learning solution for DDoS attack detection," *IEEE Trans. Netw. Service Manage.*, vol. 17, no. 2, pp. 876–889, Jun. 2020.

[43] X. Yuan, C. Li, and X. Li, "DeepDefense: Identifying DDoS attack via deep learning," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, May 2017, pp. 1–8.

[44] E. Min, J. Long, Q. Liu, J. Cui, and W. Chen, "TR-IDS: Anomaly-based intrusion detection through text-convolutional neural network and random forest," *Secur. Commun. Netw.*, vol. 2018, pp. 1–9, Jul. 2018.

[45] A. Koay, A. Chen, I. Welch, and W. K. G. Seah, "A new multi classifier system using entropy-based features in DDoS attack detection," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2018, pp. 162–167.

Zhili Zhou (Member, IEEE) received the M.S. and Ph.D. degrees in computer application from the School of Information Science and Engineering, Hunan University, in 2010 and 2014, respectively. He was a Post-Doctoral Fellow with the Department of Electrical and Computer Engineering, University of Windsor, Canada. He is currently a Professor with the School of Computer and Software, Nanjing University of Information Science and Technology, China. His current research interests include multimedia security, information hiding, digital forensics, blockchain, and secret sharing. He is serving as an Associate Editor of *Journal of Real-Time Image Processing* and *Security and Communication Networks*.

Akshat Gaurav (Graduate Student Member, IEEE) received the M.Tech. degree in computer engineering (cyber security) from NIT Kurukshetra, India. His research interests include information security, cyber security, cloud computing, web security, intrusion detection, and computer networks.

Brij Bhooshan Gupta (Senior Member, IEEE) received the Ph.D. degree in information and cyber security from IIT Roorkee, India. In 2009, he was selected for the Canadian Commonwealth Scholarship awarded by the Government of Canada. He is working as the principal investigator of various research and development projects. He has published more than 300 research papers (SCI/SCIE indexed papers: more than 150) in international journals and conferences of high repute, including IEEE, Elsevier, ACM, Springer, Wiley, Taylor & Francis, and Inderscience. His biography was selected and published in the 30th Edition of Marquis Who's Who in the World in 2012. His research interests include information security, cyber security, cloud computing, web security, intrusion detection, and phishing. He received the Young Faculty Research Fellowship Award from the MeitY, Government of India, in 2017, the Outstanding Associate Editor of 2017 for IEEE ACCESS, and the 2020 ICT Express Elsevier Best Reviewer Award. His Google Scholar H-index is 56 with around 10600 citations for his work.

Miltiadis D. Lytras (Member, IEEE) is currently an expert in advanced computer science and management, an editor, a lecturer, and a research consultant, with extensive experience in academia and the business sector in Europe and Asia. He is also a Research Professor with the Deree College—The American College of Greece and a Distinguished Scientist with King Abdulaziz University, Jeddah, Saudi Arabia. He is also a world-class expert in the fields of cognitive computing, information systems, technology-enabled innovation, social networks, computers in human behavior, and knowledge management.

Imran Razzak (Senior Member, IEEE) has been a Senior Lecturer of computer science with the School of Information Technology, Deakin University, since November 2019. He has been actively involved in teaching and research since 2010. Previously, he worked with King Saud bin Abdulaziz University for Health Sciences; the University of Technology, Malaysia; Air University, Islamabad; and the University of Technology, Sydney. He has published more than 130 papers in reputed journals and conferences. He has attracted research grant of 2.4 M AUD and has successfully delivered several research projects. He has received numerous research awards and actively collaborating with several national and international institutes. His area of interest includes machine learning with its application spans a broad range of topics. He has applied machine learning methods with emphasis to natural language processing and image analysis to solve real world problems related to health, finance, and social media.