An Intelligent Security Framework Based on Collaborative Mutual Authentication Model for Smart City Networks

ALAA O. KHADIDOS, S. SHITHARTH, HARIPRASATH MANOHARAN, AYMAN YAFOZ, ADIL O. KHADIDOS, AND KHALED H. ALYOUBI

ABSTRACT

With the advent of smart city networks and increased utilization of vehicles, the Internet of Vehicles (IoV) has attracted more attention from researchers. But, providing security to this type of network is one of the challenging and demanding tasks in the present day. For this purpose, the conventional works developed many networking frameworks and methodologies to enhance the privacy and security of smart city systems. Still, it has the significant limitations of high complexity in algorithm design, requires more time consumption for processing, reduced maintenance, and does not require proper authentication verification. Therefore, the primary purpose of this work is to develop a new security model for smart city networks using a combination of methodologies. Here, the Collaborative Mutual Authentication (CMA) mechanism is used to validate the identity of users based on the private key, public key, session key, and generated hash function. In addition, the Meta-heuristic Genetic Algorithm – Random Forest (MGA-RF) technique is deployed to detect the attacks in the network, ensuring the security of the smart city. During an evaluation, the proposed authentication-based security mechanism’s performance is validated using various parameters, and the results are compared with the recent state-of-the-art models.

INDEX TERMS
Collaborative mutual authentication (CMA), Internet of Vehicles (IoV), meta-heuristic genetic algorithm – random forest (MGA-RF), security, session key generation, artificial intelligence (AI), smart city.

I. INTRODUCTION

In recent decades, the smart city technologies [1], [2] has received significant attention due to its competence in improving the quality of life expectancy and safety of urban citizens. In smart city systems, different communication technologies are used to manage both the network and data, including big data, cloud computing, and networking systems [3], [4], [5], [6]. The general smart city applications are depicted in Fig 1, which comprises smart street lighting, smart grid, traffic management, and health systems. Here, the criticality level of each system is assessed based on its working operations and functionalities. Nevertheless, the most challenging issues in the smart city systems [7], [8], [9] are data transmission/delivery to many sensors and actuators deployed in the network, such as vehicles, infrastructures, and buildings. To solve this problem, the Internet of Vehicles (IoV) [10], [11] is integrated with an Internet of Things (IoT) [12] to improve the communication strategies in smart city networks. Because it provides the most suitable features [13], [14] of reduced cost consumption, congestion elimination, and safety assurance. The IoV is a
A. O. Khadidos et al.: Intelligent Security Framework Based on CMA Model for Smart City Networks

FIGURE 1. Illustration of smart city applications.

communication model that establishes reliable and safe communication between vehicles and infrastructures.

Moreover, the different types of security requirements [15], [16], [17], [18] must be satisfied to ensure the secured communication in smart city architecture, which includes the followings:

- **Integrity** – This property can be satisfied by detecting the manipulations done on the message.
- **Confidentiality** – Data confidentiality can be guaranteed only if the authorised vehicles receive the message.
- **Mutual Authentication** – The receiver vehicle should be definite that the message is transferred only by the authorized source.
- **Secrecy** – The forward secrecy can be maintained based on the key exchange between the sender and receiver sides with a specific time limit.

A. CONTRIBUTIONS

The significant contributions behind this work are as follows:

A. Mutual authentication and critical agreement processes ensure increased security and privacy of an open network.

B. Data transmission confidentiality and integrity are guaranteed using the session key generation and agreement controlling policies.

C. A meta-heuristic-based machine learning classifier is utilized to spot the other attacking users in the network.

D. Reliable and secured data communication is established between the V2V and V2I entities with proper registration, authentication, and key agreement phases.

B. OBJECTIVES

An intelligent security framework establishes reliable and secured communications between the vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) entities in smart city networks. Also, a Collaborative Mutual Authentication (CMA) model is deployed for properly authenticating the login requested vehicle users or infrastructure entities. In addition, the smart city network is protected against outside attackers by using the hybrid Meta-heuristic Genetic Algorithm – Random Forest (MGA-RF) based machine learning classification algorithm. The MGA optimization technique selects the optimal features based on the best solution. Then, the RF classifier predicts the attack in the network by using the selected features. Here, an integrated CMA-MGA-RF mechanism is deployed to ensure security and reliable data transmission between the entities of smart city systems. Moreover, the proposed security framework’s performance and effectiveness are validated and compared using various evaluation measures.

C. ORGANISATION

The remaining portions of this paper are structuralised as follows: Section II reviews some of the existing security architectures used in smart city applications with their advantages and disadvantages. Then, Section III presents a clear description of the proposed security framework for smart city development with its algorithmic steps and flow illustration. Section IV has validated the experimental and comparative analysis of existing and proposed security architectures. Finally, the overall paper is summarized with its obtainments and future scope in Section V.

II. RELATED WORKS

This section investigates the working modules and functionalities of different approaches to improve smart city systems’ security. Also, it discusses the advantages and disadvantages of each technique based on its functionalities and performance outcomes.

[19] designed a deep learning model-based IoT framework for increasing the security of smart cities with increased scalability, reduced latency and cost consumption. The main intention of this work was to establish a secured communication infrastructure in smart cities based on the factors of anonymity, privacy, confidentiality, authentication, repudiation and sensitivity. Also, this architecture comprises three different layers connection, conversion and application, where the blockchain was utilized to ensure security and privacy. The key benefits of this work were reduced storage problems, computational cost, and high quality of service. Still, it lacks the issues of high design complexity and reduced performance efficiency. However, it has the significant limitations of reduced trustworthiness and lack of social control. Reference [20] developed a hybridized network architecture to ensure both the privacy and security of the smart city environment. Here, the emerging Software Defined Networking (SDN) architecture was integrated with the blockchain technologies to obtain the benefits of both distributed and centralised systems. Moreover, this work
investigates the major challenging tasks in the smart city systems, which include the followings:

- Reduced latency
- High mobility
- Bandwidth limitations
- Fault tolerance
- Stability maintenance

Also, the Proof of Work (PoW) scheme was deployed, enhancing the security of distributed smart city network architecture. One of the blockchain methodologies helps find the most suitable solution based on the hash function. Still, this work is limited by central issues of high complexity in architecture designing and reduced performance efficiency. Reference [21] investigated the problems such as increased network latency, traffic, and sand security breaches related to the smart city application systems. Also, some of the essential requirements used for improving the architecture of the smart city systems [22] have been discussed in this work, which was network route updation, communication delay, fast data processing, security against attacks, ensuring both user and data privacy requirements, and time-sensitive applications. Reference [23] conducted a detailed review of the recent technologies to design an efficient smart city architecture with security enhancement and crime reduction factors. This work studied the key elements used for improving the communication capability and security of smart city networking architecture.

Reference [24] intended to ensure the trustworthiness of the smart city networking architecture by analyzing the impacts of malicious users and anchors in a crowdsensing system. The main intention of this work was to develop a vote-based crowdsensing system for improving the framework of smart city applications with the help of public sensor data, vote required for communication establishment, built-in sensors and readings. Reference [25] conducted a comprehensive review of the functionalities of SDN for establishing secure data communication at varying scales. The different types of smart city energy, health, and transportation applications have been categorized here. In addition, the critical components of smart city systems were explored in this paper, including smart education, the Internet of Things (IoT), agriculture, mobility, health, etc. Reference [26] developed a new traffic classification model based on an IoT architecture to improve smart city application QoS. The main intention of this work was to incorporate the functionalities of feature extraction, optimization, and classification models for traffic analysis in smart cities. The major stages involved in this network design were capsule network formation with a dynamic routing mechanism and traffic classification based on Convolutional Neural Network (CNN) model. Here, the dynamic routing algorithm was deployed to establish the data transformation in the capsule network by estimating the coupling coefficients and weight matrix. Then, the CNN model was utilized to categorize the traffic as benign or malware. The significant advantages of this work were high classification accuracy and better performance outcomes. However, it has the limitations of reduced security and privacy measures, which degrades the effectiveness of the overall network communication system.

Reference [6] intended to increase the security of smart city networks using the Multi-Access Mobile Edge Computing (MA-MEC) model. This paper aimed to incorporate the functionalities of a heterogeneous IoT framework for constructing a smart city. The types of attacks concentrated in this work were replay attacks, spoofing attacks, eavesdropping, node capturing, and side-channel attacks. This work has performed wiretap coding, resource allocation, key generation, and authentication to detect these attacks. The key benefits of this paper were reduced complexity, minimized resource consumption, ensured secrecy, and improved adaptation capability. Yet, it has the significant drawbacks of key generation overhead, high redundancy and network overhead. Reference [5] deployed a Reconfigurable Intelligent Surfaces (RIS) assisted networking architecture in increasing intelligent city communications' flexibility. The symbiotic relationship was estimated between the communication architecture and smart cities to establish RIS-supported communication. Also, it intended to obtain the parameters of improved QoS, security, and resource exploitation in the smart city network. The disadvantages behind this system were high sensitivity, more energy consumption, and reduced performance outcomes.

Reference [27] implemented an enhanced traffic classification model for identifying the DDoS attacks in the SDN-enabled smart city network. Also, it intends to minimize the load and increase the flexibility of SDN architecture against harmful DDoS attacks. For this purpose, a Random Forest (RF) classification model was incorporated with the backtracking methodology for accurately identifying the attacks by computing the conditional entropy. Reference [28] employed an Elliptic Curve Cryptography (ECC) technique to increase smart city networks’ security by ensuring secure message communication. Here, an Automated Validation of Internet Security Protocols and Applications (AVISPA) tool was utilized to perform an authentication-based security verification against attacks like replay, man-in-middle, and brute force [29].

Moreover, the session key generation and validation were performed to maintain the message secrecy. However, the critical limitations behind this paper were increased computational complexity, cost and time consumption measures. Reference [30] investigated various issues and challenges related to deploying security in smart city architecture. Here, the importance of using blockchain methodology was discussed to guarantee the properties of transparency, democracy, security, automation, and trust in smart city networks. Based on this scrutiny, it was studied that the blockchain methodology could be more helpful in improving smart city applications due to its significant properties of energy efficiency, cost-effectiveness, security, data storage and regulation.

Reference [31] developed a policy-based security mechanism to detect the malicious and untrustworthy nodes in the
smart city networking architecture. To improve the security of the smart system, the IoT framework was incorporated into this design, which helps to perform policy management based on contextual information. The major stages involved in this structure were data collection, policy management, malicious identification, data fusion, and trust management. The main advantage of this work was increased attack detection rate, reduced false positives, and time consumption. Yet, the effectiveness of this security architecture needs to be improved by analyzing the attacking patterns accurately. Reference [32] recommended a deep learning model for increasing the security of smart city networking systems. The main intention of this paper was to detect replay attacks with improved accuracy using the deep convolution neural network model. For this purpose, this work utilised a real-time benchmark smart city dataset, which helps evaluate the suggested model’s performance.

This review studies ensuring privacy and security measures in innovative city applications. Also, the different types of architectures deployed in the conventional works to enhance the effectiveness of smart city systems are analyzed, which can be more helpful for designing the proposed system architecture. Though the significant drawbacks that exist in the existing methodologies are as follows:

- Minimized fault tolerance capability
- Inefficient network controlling and management
- High-cost consumption for maintenance
- Reduced scalability and vulnerability
- Incompetent security on user data access control

The proposed work aims to develop an intelligent security framework for smart city networks to solve these problems.

Blockchain model is used to efficiently manage and understand the network by resolving the security risks. The purpose of the proposed work is to develop a lightweight distributed ledger blockchain based machine learning protocol for strengthening the security of smart city networks. The algorithms used in this framework are Collaborative Mutual Authentication (CMA) based blockchain model, and Meta-Heuristic Genetic Algorithm – Random Forest (MGA-RF) machine learning approach, which are implemented by using the Network Simulator tool. In this framework, the smart city network is constructed with the set of wireless nodes, where the nodes are treated as the vehicles. Once the network is created, each and every node participated in this architecture are need to be properly registered and authenticated for enabling the data communication or transmission, which is performed with the help of blockchain methodology. Also, the malicious/attacking vehicle nodes are identified and detected from the network by using the MGA-RF machine learning model. This framework is highly secured with the modules of network initialization, registration, login, mutual authentication, topology management, and attack analysis.

### III. RESEARCH METHODOLOGY

This section presents a detailed description of the proposed Collaborative Mutual Authentication (CMA) with Meta-Heuristic Genetic Algorithm – Random Forest (MGA-RF) based security framework for smart city networks. This work’s main intention is to ensure the privacy and security measures of smart city systems by establishing a secured communication between vehicle to vehicle (V2V) and vehicle to infrastructure (V2I). The overall architecture of the proposed smart city environment model is depicted in Fig 3 (a), and its corresponding working flow representation is illustrated in Fig 2. In this framework, the Internet of Vehicles (IoV) model is utilized to establish the communication between V2V and V2I. Implementing an IoV architecture model benefits secured data sharing, control, interaction, and maintenance in a smart city environment. Here, the vehicles can gather the traffic information related to the location and speed and transmits those data to other vehicles or infrastructures.

Similarly, the infrastructure can provide vehicle drivers and travellers with beneficial services and traffic information. The layered architecture model of the proposed smart city

![FIGURE 2. The flow of the proposed system.](image-url)
The significant problems of the smart city framework are collecting and transmitting the information to the different actuators and sensors integrated with smart objects like vehicles, infrastructure, buildings, etc. To solve this problem, the Internet of Vehicle (IoV) incorporated with VANET and IoT systems is utilized in this work, which helps avoid congestion operating costs and ensures safety measures. In an IoV environment, the vehicle and other entities’ communication is established using a vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications. Here, the vehicles can collect traffic information like speed and location and transmit it to the other vehicles or infrastructure units. The infrastructure provides the required services and traffic information to the drivers or passengers of the vehicles. Despite the advantages, the IoV has some serious issues due to the insecure data transmission between the entities. Because the malicious users intend to access the authenticated users’ private information, which leads to vehicular accidents due to the wrong traffic status updation, it is essential to develop an intelligent and advanced security model to ensure smart city networks’ security.

Thus, the proposed work proposes implementing a novel Collaborative Mutual Authentication (CMA) scheme incorporated with the Meta-heuristic Genetic Algorithm – Random Forest (MGA-RF) technique to ensure security and reliable data transmission between the entities of smart city systems. Data communication and transmission are established between the V2V and V2I components in the proposed framework, where the vehicles are considered vehicle users. During the initialization setup, the cyclic additive group-based bilinear mapping is performed for generating the master private and public key pair.

Here, the Smart city Vehicle Information System (SVIS) server selects the parameters for generating the keys, including the chosen randomly sizeable prime number, cyclic additive group member functions, bilinear mapping function, generator of cyclic group, and hash function. Based on these, the keys are generated, and the set of values is considered the system parameters, which can be used for further communications. After setting the network topology, all users and infrastructures must register with the Road Side Unit (RSU) server, and only the authenticated vehicle users and infrastructures are allowed for communication. In the registration phase, the remote user, user identity, unique password, and user biometric information are considered for registering vehicle users and infrastructure entities. In this environment, fingerprint-based biometric information is gathered from the vehicle users for registration. Then, the collected information is stored in the cloud system, and the centralized server provides access to the data. Here, the blockchain security model is used to secure the private credentials of the users. The constant values are generated according to the specifications of requested vehicle users or infrastructure entities. The corresponding user shares their generated information with the SVIS server unit.
Consequently, the server checks the identity of the requested user by matching it with the database system; if it is a new user, the server device can store the new user’s information in the 0th array; otherwise, it can append the information in the existing collection. After this process, the server can generate the corresponding user’s verification ID and weight value using the hash function set, user identity, master public key, and constant value. Based on these values, the smart card can be generated for the registration requested user, and consequently, other entities are registered with the server unit. The smart card is a kind of electronic authorization card used to check the validity and authenticity of the vehicle users. So, all vehicles participating in the smart city environment should register with the centralized server to obtain the smart card. Also, the vehicle user or infrastructure with this smart card is considered the authenticated participants, and the registered participants are allowed further data transmission and communications. Here, the blockchain data storage system is used to securely store the information of vehicle users. Typically, the blockchain is defined as a kind of digital ledger technology used primarily to store transactional information. The data are stored as signed blocks linked with each other. For instance, the sample blocks of information are shown below:

| Block A | Block B |
|---------|---------|
| {       | {       |
| Metadata: { }, | Metadata: { }, |
| Transactions: [ ], | Transactions: [ ], |
| None: 289, | None: 5685, |
| Hash: 00002d096d256 } | PreHash: 00002d096d256, Hash: 0001c6a12158 } |

| Block C |
|---------|
| {       |
| Metadata: { }, |
| Transactions: [ ], |
| None: 85 |
| PreHash: 0001c6a12158 |
| Hash: 00003d08745b } |

Moreover, the blockchain is immutable, so there is no possibility of changing the information in the data blocks. The primary advantage of using blockchain databases is that they provide an efficient way to store the data securely. After successful registration, the vehicle users or infrastructure must log in to participate in the communication. The authenticated entities needed to provide their smart card, unique identity, password, and biometric information during this process. After that, these parameters were validated based on the hash value. If the generated hash value of the smart card is invalid, the session can be automatically aborted; otherwise, the pseudo-random number and timestamp values are generated for the requested smart card vehicle user/infrastructure entity. Then, the login parameters are transmitted to the server unit for proper authentication and validation. Here, the Collaborative Mutual Authentication (CMA) mechanism is implemented for validating the authenticity of the login requested vehicle user/infrastructure. During this process, the server validates the session of the login requested entity; if the condition is valid, the blockchain integrated bilinear mapping model generates the session key based on the public key’s parameters, identity, password, and biometric information.

Finally, the server can transmit the authenticated message to the requested user/infrastructure entity. The key agreement policy has been utilized to verify the time stamp validity on the user side. The authenticated users can only extract the session key for further data transmission with other entities. In addition, the security analysis is performed to detect other attacking activities in the smart city networks, which is accomplished by using the hybrid Meta-heuristic Genetic Algorithm integrated with Random Forest (MGA-RF) technique. This framework’s novel contribution ensures the security of data transmission and communication between the entities at each system module like registration, login, proper authentication, session key generation, and key agreement controlling policy validation.

Moreover, other attacking activities are also detected and classified using the optimization-based machine learning classification mechanism. Hence, this framework guarantees reliable and secured communication between the V2V and V2I entities in the smart city networks. It filters the malicious users and outside attackers based on proper authentication and key agreement functions. The key advantages of this work are high security, robustness, reliability, reduced cost consumption, minimized time consumption, and increased efficiency. Table 1 shows the list of symbols used in the proposed methodology with its descriptions.

### B. INITIALIZATION

In this phase, the Smart city Vehicle Information System (SVIS) server defines the set of parameters at first, which includes the large prime number $p$, cyclic additive group $G$, bilinear map $b$, hash function $hash_{fun}$, and updated hash function $H_{fun}$. Then, the master private key $Master_{PK}$ and public keys $Master_{BK}$ are generated and integrated with the predefined parameters, which helps to secure the server database. The algorithmic steps involved in the initialization process are illustrated Algorithm 1.

### C. REGISTRATION

After initialization, the registration process can be mainly performed to allow the vehicles for accessing and exchanging traffic information from/to the other objects in an IoV architecture. During this process, the remote user $R_u$, user identity, password, and biometric information $BM_U$ are taken as the inputs for registration. Then, the constant value $C_U$ is gen-
generating for both infrastructure and vehicle with the password parameters and hash function $H_{\text{fun}}$ of biometric information.

### Algorithm 1: Initialization

**Step 1:** Smart city Vehicle Information System (SVIS) server $H_S$ sets up its parameters.

**Step 2:** $H_S$ selects the public parameters \{ $q_p, M_1, M_2, b_m, P, \text{hash}_{\text{fun}}, H_{\text{fun}}$ \} $q_p$ – large prime number, $M_1 \& M_2$ are the cyclic additive group which is generated by $P$, and $b_m$ is the bilinear map. $P$ is the generator of $M_1 \& M_2$, $\text{hash}_{\text{fun}}$ – hash function which is computed from $Z_q$, and $H_{\text{fun}}$ – computed hash function.

**Step 3:** Generate the master private key as follows,

$$\text{Master}_{PK} = s_m \epsilon Z_q$$

where, $s_m$ indicates the master private key.

**Step 4:** Generate the master public key as follows,

$$\text{Master}_{BK} = s_m P$$

**Step 5:** Announces their generated information as system parameters,

$$\text{param} = \{ q_p, M_1, M_2, b_m, P, \text{hash}_{\text{fun}}, H_{\text{fun}}, \text{Master}_{BK} \}$$

Consequently, the user can transmit generated message to the server, which validates the identity of the infrastructure/vehicle based on the database entries. If the entry is new to the server $H_S$, it can automatically store the record at the initial array; otherwise, it adds the record in the existing array.

**D. LOGIN PHASE**

After registration, the user can enter their details to log in into the system with the smart card information $SC_U$, password $PW_U$ and biometric information $BM_U$. Then, the defined parameters have been validated with the stored record $V_U$ based on the hash function $\text{hash}_{\text{fun}}$. If the generated hash value for the given information of $ID_U, PW_U$ and $BM_U$ are not valid, the session gets automatically terminated. Otherwise, the pseudo-random number has been generated for $SC_U$ with the initialization of time stamp of $T_U$. Consequently, the login request can be formed and transferred to the remote server based on this information.

**E. COLLABORATIVE MUTUAL AUTHENTICATION**

Here, the collaborative mutual authentication mechanism is implemented in this system to validate the users’ identity to ensure security. After getting the login request, the RSU server $H_S$ can validate the session time for the request received from the user. If the condition is satisfied, the blockchain-based bilinear mapping model is utilized for computing the parameters of $s_m$ and $R_U P$. Consequently, the
Algorithm 2 Registration Phase

Input: Remote User $R_U$, User Identity $ID_U$, password $PW_U$, User Biometric information $BM_U$;

Step 1: Generate constant value for the user (i.e. vehicle/infrastructure),
$$C_U = PW_U \oplus H_{\text{fun}}(BM_U)$$
Step 2: User sends this generated message to RSU server $H_S$.
Step 3: Server $H_S$ checks the identity $ID_U$ in its database.
Step 4: If (the identity is new)
    - The server can store the record at $0^{th}$ array;
Step 5: Else
    - The record can be appended in the existing array;
Step 6: Then, the server $H_S$ computes and stores the verification ID $V_U$ and weight for the user $Wt_U$ as shown below,
    $$V_U = H_{\text{fun}}(ID_U | C_U)$$
    $$Wt_U = C_U \oplus H_{\text{fun}}(ID_U | s_m)$$
Step 7: Finally, the server $H_S$ adapts smart card and forwards to the remote user.
$$SC_U = \{V_U, Wt_U, Master_{BK}, hash_{fun}, H_{fun}\}$$

Algorithm 3 Login Phase

Step 1: User can use their smart card $SC_U$ with card reader for inserting their Identity $ID_U$, password $PW_U$, Biometric information $BM_U$
Step 2: Then, the following parameters have been validated for $SC_U$ as shown below:
$$hash_{fun}(ID_U | PW_U \oplus H_{\text{fun}}(BM_U))$$
Check its value with the stored $V_U$.
Step 3: If the computed hash value of $SC_U$ is invalid, Session got aborted;
Step 4: Then, the pseudo random number $rp_U \in Z_q$ is generated for $SC_U$ and time stamp $T_U$ is initiated.
Step 5: After that, the following log in parameters are computed,
$$N_U = H_{\text{fun}}(ID_U)$$
$$N_{s_m} = H_{\text{fun}}(ID_S)$$
$$R_U = rp_U N_U$$
$$K_U = b_{m}(Master_{BK}, rp_U N_{H_s})$$
$$Auth_U = E_{sk}(ID_U | T_U | rp_U) \parallel E_{sk}$$. encrypted symmetric key
Step 6: Finally, the generated information is organized as follows:
$$LoginRequ = R_U, T_U, Auth_U$$ to server $H_S$
This login request can be transmitted to the server.

| Registration | RSIV RSU server $H_S$ |
|--------------|-----------------------|
| Remote User $R_U$ | $SC_U = \{V_U, Wt_U, Master_{BK}, hash_{fun}, H_{fun}\}$ |
| **Compute** | $C_U = PW_U \oplus H_{\text{fun}}(BM_U)$ |
| **Sends** | $(C_U, ID_U)$ to RSU server $H_S$ |

RSU Server $H_S$ checks its identity $ID_U$ in its database.
If it is new, store the records at $0^{th}$ array; Otherwise, append the records into existing array.
Then, $H_S$ adapts smart card $SC_U = \{V_U, Wt_U, Master_{BK}, hash_{fun}, H_{fun}\}$
Send smart card to $R_U$ securely.

$Auth_U$ is decrypted for getting the encrypted information of $ID_U$, $T_U$, and $rp_U$. Then, the hash function is computed for $ID_U$ that helps to validate the remote vehicle user as whether authorized or unauthorised. If the session time mismatches for the requested user, the RSU server $H_S$ can generate the random number for the particular request. At that time, it computes the login parameters of the user for obtaining the authenticated smart card $Auth_{s_m}$. Based on the parameters of $T_U, R_U, R_{s_m}, T_{s_m}$ and $Login_{s_m}$, the session key is generated by computing the hash function of these measures. Finally, the authenticated message is transferred to the remote vehicle user with $R_{s_m}, T_{s_m}$, and $Auth_{s_m}$.

| Login | RSIV RSU server $H_S$ |
|-------|-----------------------|
| Remote Vehicle $R_U$ | $LoginRequ = R_U, T_U, Auth_U$ to server $H_S$ |

User inserts $SC_U$ into card reader with $ID_U$, $PW_U$, and $BM_U$. Then, $SC_U$ estimates
$$hash_{\text{fun}}(ID_U | PW_U \oplus H_{\text{fun}}(BM_U))$$
If $hash(SC_U)$ is invalid, Session aborted; Otherwise, $SC_U$ generates the number $rp_U \in Z_q$ and initiates the time stamp $T_U$.
Compute the values of $N_U$, $N_{s_m}, R_U, K_U$ and $Auth_U$. Then, the transfer the login request $LoginRequ$.
Based on the receiving $LoginRequ$ from remote vehicle user $R_U$, the authentication can be performed.

Once the authentication is accomplished at the server side, the key agreement process can be performed at the remote vehicle user side. During this phase, the user can validate the time stamp value, if it is match with the login parameters, the authenticated message is verified based on the hash value of $T_U, R_U, T_{s_m}, R_{s_m}, Login_{s_m}$, and $K_U$. Consequently, the session key verification is also performed at the user side by the updated hash value.
Algorithm 4 Collaborative Mutual Authentication

Step 1: RSU server $H_S$ verifies the session time validity once it received the login request for requested user.

$$\Delta T \leq T_{sm} - T_U$$

Step 2: If the above condition is valid,

a. Then, the following parameters are estimated by using the block chain based bilinear map model;

$$K_{sm} = b_m (s_m, R_UP)$$

b. Decrypt $Auth_{sm}$ and obtain the encrypted information $ID_U || T_U || RP_U$;

c. Compute $N_U = H_{fun}(ID_U)$ and Verify $R_U = RP_U N_U$

Step 3: Else

The RSU server $H_S$ generates a random number $r_{psm} \in Z_q$.

Step 4: Compute the following parameters:

$$\begin{align*}
N_{sm} &= H_{fun}(ID_S), \\
R_{sm} &= r_{psm} N_{sm}, \\
login_{sm} &= r_{psm} R_{sm}, \\
Auth_{sm} &= hash_{fun}(T_U || R_U || T_{sm} || R_{sm} || login_{sm} || K_{sm})
\end{align*}$$

Step 5: Then, the session key is generated as follows;

$$\begin{align*}
sess_{sm}^{key} &= hash_{fun}(T_U || R_U || T_{sm} || R_{sm} || login_{sm})
\end{align*}$$

Step 6: At last, transfer the authentication message to user $R_U \quad MA = (R_{sm}, T_{sm}, Auth_{sm})$

F. TOPOLOGY MANAGEMENT

As mentioned in the layered architecture Fig 3 (b), the topology management is performed in this environment to maintain the network connectivity. Also, it helps to reduce the network overhead with increased operating efficiency. Here, the cluster optimization problem is considered as the Governing Set (GS), which comprises the subset of nodes. The processes involved in the network topology management process is illustrated as follows, and its variable descriptions are listed in Table 1.

Input: Neighbor information of node $D$

$$\begin{align*}
InitCH_{set} &= N_{CH_d}^D, \\
G_d &= (V_d, E_d)
\end{align*}$$

//Where,

$$\begin{align*}
V_d &= U_{CH \in N_d^{CH}} \psi_{CH} UD, \\
U_d, V_d \in E_d & \text{ if } U_d \in N_d^{v}, \\
[CH_{set}, ClMemSet] &= FormationCluster_GS(G_d, D, [InitCH_{set}]), \\
if [CH_{set}] < [InitCH_{set}] & \text{ then } reconClusters(ClMemSet)
\end{align*}$$

$$\begin{align*}
end
\end{align*}$$

function $[CH_{set}, ClMemSet]$

$$\begin{align*}
= FormationCluster_GS(G_d, D[InitCH_{set}]), \\
t' &= \arg \max \{|N_{ID}^d (t') \cap V_d \cap ID| \}
\end{align*}$$

$$S = V_d / N_{ID}^d (t') \cap ID$$

while $S \neq 0$ and $|CH_{set}| \leq CH_{max}$ do

$$\begin{align*}
\text{foreach } n_j \in S & \text{ do } \\
Nighl' &= \max \{|N_{ID}^d (t) \cap S| \}, \\
t_j &= \arg \max \{|N_{ID}^d (t) \cap S| \}
\end{align*}$$

end for

$$j = \arg \max Nighl'$$

$CH_{set} \leftarrow n_j$

$ClMemSet \leftarrow \{CH : n_j\}$

Primary Channel $t_j$, Members: $N_{ID}^d (t_j) \cap S \cup n_j$

$S = SN_{ID}^d (t_j) \cap S \cup n_j$

end while

return

Algorithm 5 Key Agreement

Step 1: User $R_U$ verifies its time stamp validity,

$$\Delta T \leq T_{sm} - T_U$$

Step 2: If valid user estimates, $login_U = r_{psm} R_{sm}$

Step 3: Verifies the following equation,

$$Auth_{sm} = hash_{fun}(T_U || R_U || T_{sm} || R_{sm} || login_{sm} || K_U)$$

Step 4: If equation holds computes the common session key as,

$$sess_{sm}^{key} = hash_{fun}(T_U || R_U || T_{sm} || R_{sm} || login_{sm})$$

Authentication & Key Agreement

Remote Vehicle User $R_U$ SVIS RSU server $H_S$

Verifies the session time validity $\Delta T \leq T_{sm} - T_U$;

If (Valid)

$$K_{sm} = b_m (s_m, R_UP),$$

$ID_U || T_U || RP_U$

$N_{sm} = H_{fun}(ID_U)$

$R_U = r_{psm} N_{sm}$

Else

$R_U = r_{psm} N_{sm}$

Compute $N_{sm}$, $R_{sm}$, $login_{sm}$, and $Auth_{sm}$;

Generate $sess_{sm}^{key}$ and send message to $R_U$. 

User $R_U$ verifies the time stamp validity, $\Delta T \leq T_{sm} - T_U$;

If (the user is valid)$login_U = r_{psm} R_{sm}$;

$$Auth_{sm} = hash_{fun}(T_U || R_U || T_{sm} || R_{sm} || login_{sm} || K_U)$$

Estimate the common session key $sess_{sm}^{key} = hash_{fun}(T_U || R_U || T_{sm} || R_{sm} || login_{sm})$
G. ATTACK ANALYSIS

In addition, the proposed work implements the machine learning classification model for identifying the attacks in the smart city systems, which is considered a supplementary security module used for guaranteeing reliable network communication. In this work, a separate database has been maintained for storing the previous history of data communications, which comprises the information related to the vehicles and infrastructures that participated in the touch. Then, the characteristics of these entities are stored in the form of features to avoid malicious attacks in future data communications. Based on the learning of these features, the attacks are identified and classified using the Meta-Heuristic Genetic Algorithm – Random Forest (MGA-RF) technique is implemented in this phase, which is used to increase the overall security of networking systems. The main intention of using this approach is to minimize the complexity of the training model with improved attack detection accuracy. In this mechanism, the MGA is utilized to select the best optimal solution for improving the recognition accuracy of the attack detection system. For this purpose, the crossover, mutation and selection functions are computed, which are used to construct the classification model. The RF is a bootstrap resampling model mainly used to extract more samples from the given dataset. The technique’s significant benefits are increased computational efficiency, reduced designing complexity, improved accuracy, and a high recognition rate. The number of classes cap U sub cap C in the labelled data is computed in this phase, which is used to increase the overall security of networking systems.

Algorithm 6 Meta-Heuristic Genetic Algorithm – Random Forest (MGA-RF)

Step 1: To compute the number of classes in the labelled data
\[ U_C = \text{unique}(L_N) \]
// \( U_C \) – number of classes in labeled data
\[ L_N = \text{Number of labels} \]

Step 2: Create root node \( N_{rt} \) containing training data \( D_{tr} \) about the presented users.

Step 3: Consider the training data \( D_{tr} \) as chromosomes.

Step 4: Perform a selection of chromosomes based on the root node \( N_{rt} \).

Step 5: Compute objective function to construct a tree with respect to \( N_{rt} \).

Step 6: Randomly select \( y\% \) of possible splitting features in \( N_L \) by \( N_L \) is the number of samples presented in each class.
\[ \text{if } \text{Fit}_{chr} < \text{Fit}_{pre} \]
\[ \text{split}_{prob} = N_L(U_C) * y\% \]
\[ \text{end if} \]
//Where, \( \text{Fit}_{chr} \) – fitness value for chromosome and \( \text{Fit}_{pre} \) - fitness value for previous chromosome.

Step 7: The crossover and mutation probability is computed with respect to crossover rate and mutation rate.

Step 8: Create child node \( N_{ch} \) with highest information gain to split on possible values.

Step 9: Predict corresponding class for test data \( D_{te} \) by matching all instances.
\[ \text{pred}_{cls} = N_L(N_{ch}) \]

Consequently, the chromosome selection is performed based on the root node, and the objective function is estimated for constructing the tree with the root node. Then, the possible splitting features are randomly selected concerning the fitness values of chromosomes. After that, the crossover and mutation functions are estimated and based on this value, the child node is created with the highest possible gain value. Finally, all instances are matched with the test data to accurately predict the corresponding label class. The algorithmic steps involved in this technique are illustrated in Algorithm 6.

Fig 4 (a) shows the network deployment framework, where the set of nodes are positioned in different locations with the RSU, and Fig 4 (b) depicts the detection of malicious users on the network region. Consequently, Fig 4(c) shows the number of requested users in the network, and the overall requested, authenticated, and malicious users are depicted in Fig 4(d).

As shown in Fig 4 (a), the smart city network is constructed by using the simulation, and the network comprises the group of vehicle nodes and RSUs. When the vehicle crosses the RSU, it can update the details to RSU. In the deployed network, there may be a possibility for the malicious users highlighted in black, as shown in Fig 4 (b). Here, the machine learning technique named, MGA-RF is used to detect malicious users by analyzing the features, which are the information of vehicle users. In this framework, the security is strengthened in two phases, which include the proper vehicle registration & authentication, and attack analysis using MGA-RF. Then, the vehicle users can request the RSU to enable the data transmission/communication with the neighborhood vehicle users. As shown in Fig 4 (c), the requested vehicle users are highlighted in red color, where the RSU can authenticate the requested vehicle users for communication. After that, the data transmission/communication is established between the authenticated vehicles in a certain range, as shown in Fig 4 (d).

H. SECURITY ANALYSIS

Table 2 depicts the proposed CMA-MGA-RF model-based smart city networking architecture’s security and privacy analysis. Here, the different types of security features and their related issues are evaluated for the proposed system. The proposed model’s security analysis is assessed concerning varying security issues and their corresponding features. The properties that must be satisfied are resiliency, digital ledger, efficiency, anonymity, smart contract, persistency, and decentralization to ensure better performance and increased security of the system. These properties are assessed under security problems like third-party accessibility, eavesdropping, controlling access, frequent availability, data honesty,
FIGURE 4. Network deployment with (a) Set of vehicle users and RSU (b) Detection of malicious users (c) Requested nodes (d) Requested, authenticated and malicious nodes.

single-point failure, trustfulness, invariability, and data privacy. According to this analysis, it is identified that the proposed framework could efficiently satisfy all these properties with guaranteed network security. Due to incorporating the MGA-RF with the security framework, the reliable data transmission and communication of smart city networks are highly improved. The proposed framework satisfies the properties of resiliency, digital ledger, efficiency, anonymity, smart contract, persistency, and decentralization.

IV. RESULTS AND DISCUSSION

This section validates the performance analysis of existing and proposed techniques using various evaluation indicators. Some conventional security architectures have been compared with the proposed framework based on latency, computational time, True Positive Rate (TPR), and False Positive Rate (FPR). Typically, the overall effectiveness of the networking framework is determined by increased scalability and reduced latency measures. Figures 5 and 6 show the total latency of both existing and proposed approaches concerning the industrial data source and the number of sources. The results show that the total latency of the proposed CMA-MGA-RF model is efficiently reduced compared to the conventional approaches for both numbers services and industrial sources.

Table 3 presents the comparative analysis of both existing [10] and proposed techniques based on the computational time of Desktop Computer (DC) (ms). Here, the computational time is measured by the time required for designing the security architecture with minimized complexity. Moreover, computational cost and time are the most extensively used performance indicators for validating the overall effectiveness of the networking systems. The analysis proves that the proposed CMA-MGA-RF model requires reduced computational time for processing the security functions and detecting the attacking events on the smart city networks. Compared
to conventional techniques, the proposed model provides less computational time for both DC and RP in milliseconds.

Consequently, Table 4 and Table 5 compares the communication cost and storage overhead of conventional and proposed security schemes based on the communications of V2V and V2I respectively. Here, the $T_{AE}$ represents the asymmetric encryption, $T_{AD}$ indicates the asymmetric decryption, $T_S$ is the signing operation, $T_{SE}$ denotes the symmetric encryption, $T_{SD}$ symmetric decryption, and $T_h$ indicates the hash function. The obtained results depict that the proposed security model requires reduced communication cost and storage overhead, when compared to the other techniques.

Fig 7 illustrates the TPR and FPR analysis of both existing [27] and proposed classification systems, which includes the models of center line, RL-RF, SVM, RF, and Bayes Net. Typically, the TPR and FPR measures are used to validate that how effectively the classifier predicts the attacking labels as normal or attack, which are
computed as follows:

\[
TPR = \frac{TP}{TP + FN} \tag{1}
\]

\[
FPR = \frac{FP}{FP + TN} \tag{2}
\]

where, TP indicates the True Positives, TN indicates the True Negatives, FP is the False Positives, and FN is the False Negatives (FN). Based on this evaluation, it is analyzed that the proposed CMA-MGA-RF model provides an increased TPR by accurately classifying the attacking labels compared to the other approaches. The accuracy is one of the essential measures used for validating the performance of overall security systems, which is calculated as follows:

\[
Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{3}
\]

Also, the attack detection mechanism’s effectiveness depends on the measure of accuracy. It is calculated based on the percentage of accurately detected flows concerning the total number of predictions. Table 6 and Fig 8 show the accuracy analysis of existing and proposed security mechanisms, including RL-RF, BayesNet, RF, SVM, and proposed CMA-MGA-RF mechanisms. From the results, it is evident that the proposed technique outperforms the other methods with increased accuracy. Precision, recall, and TPR are the performance measures mainly used to determine that how the classification technique could actually predict the exact values at the time of attack detection. Also, the relevancy level of both actual and predicted class labels are estimated with respect to the classified outcomes, which ensures an improved performance of the proposed technique with reduced training level.

\[
Precision = \frac{TP}{TP + FP} \tag{4}
\]

\[
Recall = \frac{TP}{TP + FN} \tag{5}
\]

Table 7 compares the existing and proposed security mechanisms based on accuracy, precision, recall, and TPR measures. The techniques considered for this analysis are Bayes Net, C4.5, Naïve Bayes (NB), Random Forest (RF), Random Tree (RT), and proposed CMA-MGA-RF. Then, its corresponding graphical representations are presented in Fig 9 and
Table 7. Overall performance analysis of existing and proposed techniques.

| Algorithms        | Accuracy | Precision | Recall | TPR |
|-------------------|----------|-----------|--------|-----|
| BayesNet          | 99.77    | 1.00      | 0.99   | 0.99|
| C4.5              | 99.99    | 1.00      | 1.00   | 1.00|
| Naive Bayes       | 99.79    | 0.99      | 0.98   | 0.99|
| Random Forest     | 99.99    | 1.00      | 1.00   | 1.00|
| Random Tree       | 99.99    | 1.00      | 1.00   | 1.00|
| CMA-MGA-RF        | 99.99    | 1.00      | 1.00   | 1.00|

Fig. 10. Based on this comparative analysis, it is stated that the proposed CMA-MGA-RF technique provides improved results compared to the other techniques. Because it ensures the security of smart city networks by the key generation, authentication, and key agreement processes, these modules help to ensure the authorized access on the network with increased privacy and security measures. Also, it detects the attacking activities by accurately predicting the classified labels based on the optimal fitness computation of MGA. Table 8 presents the Time Taken to Build Model (TTBM) analysis of existing and proposed mechanisms. These results also indicate that the proposed technique consumes less time for constructing the security framework. Compared to the other models, the TTBM of the proposed CMA-MGA-RF model takes less time to design the networking system.

V. CONCLUSION

This paper proposed intelligent network architecture to ensure the privacy and security of smart city networks. The key focus of this work is to establish secure and valid network communication by applying the proper authentication mechanism. The major stages involved in this system design are the registration phase, login phase, authentication phase, key agreement phase, and attack analysis. At first, the smart card generation is carried out during the registration process based on the hash function value. Then, the user can log in to the system with their smart card, authentication key, identity, and passwords. Once the remote server receives a request from the appropriate user, it validates the authenticity of the user by using the session key.

Similarly, the user can validate the corresponding session key with the authenticated message for key agreement. The user can be considered an authenticated party if both keys are matched. To detect malicious activities on the network, the MGA-RF-based machine learning algorithm is employed to improve the security of smart city networks. Furthermore, the performance results of both existing and proposed techniques are evaluated and compared using the latency, TPR, accuracy, precision, recall and TTBM. Based on the obtained results, it is proved that the proposed CMA-MGA-RF technique outperforms the other techniques with improved performance values.

In the present work, the Collaborative Mutual Authentication (CMA) based blockchain mechanism is mainly developed to guarantee the security of smart city networks with proper registration, login, and authentication modules. It helps to filter the unauthenticated/malicious vehicle nodes in the network. In addition, an optimization integrated machine learning methodology, named as, MGA-RF is implemented to ensure the reliable data communication in the network by detecting the attacks in the network. In the proposed system, the distributed ledger – machine learning protocol is used to strengthen the security of smart city network. In future, the proposed distributed ledger blockchain framework can be implemented in a real-time scenario by getting funds.

ACKNOWLEDGMENT

The authors, therefore, acknowledge with thanks the Deanship of Scientific Research for technical and financial support.

REFERENCES

[1] P. K. Sharma, S. Rathore, and J. H. Park, “DistArch-SCNet: Blockchain-based distributed architecture with Li-Fi communication for a scalable smart city network,” IEEE Consum. Electron. Mag., vol. 7, no. 4, pp. 55–64, Jul. 2018.

[2] P. K. Sharma, S.-Y. Moon, and J.-H. Park, “Block-VN: A distributed blockchain based vehicular network architecture in smart city,” J. Inf. Process. Syst., vol. 13, no. 1, pp. 184–195, 2017.
A. O. Khadidos et al.: Intelligent Security Framework Based on CMA Model for Smart City Networks

[3] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, “Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework,” Inf. Syst. Frontiers, vol. 8, no. 1, pp. 1–22, Jan. 2020.

[4] J. Cha, S. K. Singh, T. W. Kim, and J. H. Park, “Blockchain-empowered cloud architecture based on secret sharing for smart city,” J. Inf. Secur. Appl., vol. 57, Mar. 2021, Art. no. 102686.

[5] S. Kisseleff, W. A. Martins, H. Al-Hraishiaw, S. Chatzinotas, and B. Ottersten, “Reconfigurable intelligent surfaces for smart cities: Research challenges and opportunities,” IEEE Open J. Commun. Soc., vol. 1, pp. 1781–1797, 2020.

[6] D. Wang, B. Bai, K. Lei, W. Zhao, Y. Yang, and Z. Han, “Enhancing information security via physical layer approaches in heterogeneous IoT with multiple access mobile edge computing in smart city,” IEEE Access, vol. 7, pp. 54508–54521, 2019.

[7] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, “Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles,” IEEE Access, vol. 8, pp. 43711–43724, 2020.

[8] S. Shitharth, P. K. Balachandran, K. H. Alyoubi, and S. J. Hussini, “An enriched RPCO-BCNN mechanisms for attack detection and classification in SCADA systems,” IEEE Access, vol. 9, pp. 156297–156312, 2021, doi: 10.1109/ACCESS.2021.3129053.

[9] S. Singh, P. K. Sharma, B. Yoon, M. Shojafar, G. H. Cho, and I.-H. Ra, “Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city,” Sustain. Cities Soc., vol. 65, Dec. 2020, Art. no. 102364.

[10] S. Yu, J. Lee, K. Park, A. K. Das, and Y. Park, “IoV-SMAP: Secure and efficient message authentication protocol for IoV in smart city environment,” IEEE Access, vol. 8, pp. 167875–167886, 2020.

[11] S. Sharma, K. K. Ghanshala, and S. Mohan, “Blockchain-based internet of vehicles (IoV): An efficient secure Ad hoc vehicular networking architecture,” in Proc. IEEE 2nd 5G World Forum (5GWF), Sep. 2019, pp. 452–457.

[12] J.-H. Park, M. M. Salim, J. H. Jo, J. C. S. Sicato, S. Rathore, and J. H. Park, “CloToNet: A scalable cognitive IoT based smart city network architecture,” Hum.-Centric Comput. Inf. Sci., vol. 9, no. 1, pp. 1–20, Dec. 2019.

[13] A. K. M. B. Haque, B. Bhushan, and G. Dhiman, “Blockchain-empowered cloud architecture based on secret sharing for smart city,” J. Inf. Secur. Appl., vol. 57, Mar. 2021, Art. no. 102686.

[14] S. Peneti, M. Sunil Kumar, S. Kallam, R. Patan, V. Bhaskar, and M. Ramachandran, “BDN-GWMNN: Internet of Things (IoT) enabled secure smart city applications,” Wireless Pers. Commun., vol. 119, no. 3, pp. 2469–2485, Aug. 2021.

[15] S. Shah, M. J. A. Anjum, and J. A. Shamsi, “SEAL: SDN based secure and reliable framework for protecting smart city applications from DDoS attacks,” J. Netw. Comput. Appl., vol. 145, Nov. 2019, Art. no. 102381.

[16] W. Chen, S. Xiao, L. Liu, X. Jiang, and Z. Tang, “A DDoS attacks traceback scheme for SDN-based smart city,” Comput. Electr. Eng., vol. 81, Jan. 2020, Art. no. 106503.

[17] D. Singh, B. Pati, C. R. Panigrahi, and S. Swagatika, “Security issues in iot and their countermeasures in smart city applications,” in Advanced Computing and Intelligent Engineering, vol. 1089. Singapore: Springer, 2020, pp. 301–313.

[18] A. Gharaiheb, M. A. Salahuddin, S. J. Hussini, A. Khreishah, I. Khalil, M. Guizani, and A. Al-Fuqaha, “Smart cities: A survey on data management, security, and enabling technologies,” IEEE Commun. Surveys Tuts., vol. 21, no. 2, pp. 1718–1743, 2nd Quart., 2019.

[19] S. Mallick, M. T. M. Faruque, and M. S. Ramzan, “A simple lightweight protocol for secure resource discovery in smart city,” in Proc. 22nd Int. Conf. Comput. Netw. Commun., Mar. 2019, Art. no. 102686.

[20] S. Pouryazdan, B. Kantarci, T. Soyata, and H. Song, “Anchor-assisted and vote-based trustworthiness assurance in smart city crowdsensing,” IEEE Access, vol. 4, pp. 529–541, 2016.

[21] M. Rahouti, K. Xiong, and Y. Xin, “Secure software-defined networking communication systems for smart cities: Current status, challenges, and trends,” IEEE Access, vol. 9, pp. 12083–12113, 2021.

[22] H. Yao, P. Gao, J. Wang, P. Zhang, C. Jiang, and Z. Han, “Capsule network assisted IoT traffic classification mechanism for smart cities,” IEEE Internet Things J., vol. 6, no. 5, pp. 7515–7525, Oct. 2019.

[23] S. Shitharth, P. R. Kshirsagar, P. K. Alalchandran, K. H. Alyoubi, and A. O. Khadidos, “An innovative perceptual pigeon galvanized optimization (PPO) based likelihood Naive Bayes (LNB) classification approach for network intrusion detection system,” IEEE Access, vol. 10, pp. 46424–46441, 2022, doi: 10.1109/ACCESS.2022.3171660.

[24] A. Dua, N. Kumar, A. K. Das, and W. Sasilo, “Secure message communication protocol among vehicles in smart city,” IEEE Trans. Veh. Technol., vol. 67, no. 5, pp. 4359–4373, Dec. 2017.

[25] M. Sookhak, H. Tang, Y. He, and F. R. Yu, “Security and privacy of smart cities: A survey, research issues and challenges,” IEEE Commun. Surveys Tut., vol. 21, no. 2, pp. 1718–1743, 2nd Quart., 2019.

[26] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, “A survey of blockchain technology applied to smart cities: Research issues and challenges,” IEEE Commun. Surveys Tut., vol. 21, no. 3, pp. 2794–2830, 3rd Quart., 2019.

[27] W. Li, H. Song, and F. Zeng, “Policy-based secure and trustworthy sensing for Internet of Things in smart cities,” IEEE Internet Things J., vol. 5, no. 2, pp. 716–723, Jun. 2017.

[28] A. A. Elsaiedy, N. Jagannath, A. G. Sanchis, A. Jamalipour, and S. K. Munasinghe, “Replay attack detection in smart cities using deep learning,” IEEE Access, vol. 8, pp. 137825–137837, 2020.

[29] Talwar Thakore & Associates. (2022). Data Protected—India.[Online]. Available: https://www.linkkaters.com/en/insights/data-protected/data-protected-india#:~:text=India%20has%20also%20also%20not%20yet%20implement%20the%20personal%20information.

[30] J. Li, H. Lu, and M. Guizani, “ACPN: A novel authentication framework with conditional privacy-preservation and non-reputation for VANETs,” IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 4, pp. 938–948, Feb. 2014.

[31] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, “2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET,” IEEE Trans. Veh. Technol., vol. 65, no. 2, pp. 896–911, Feb. 2015.

[32] H. Vasudev, D. Das, and A. V. Vasilakos, “Secure message propagation protocols for IoVs communication components,” Comput. Electr. Eng., vol. 82, Mar. 2020, Art. no. 106555.

ALAA O. KHADIDOS received the B.Sc. degree in computer science from King Abdulaziz University, Jeddah, Saudi Arabia, in 2006, the M.Sc. degree in computer science from the University of Birmingham, Birmingham, U.K., in 2011, and the Ph.D. degree in computer science from the University of Warwick, Coventry, U.K., in 2017. He is currently an Assistant Professor with the Faculty of Computing and Information Technology, King Abdulaziz University. His main research interests include the areas of computer vision, machine learning, optimization, and medical image analysis.
S. SHITHARTH (Senior Member, IEEE) received the B.Tech. degree in information technology from the KGIS Institute of Technology, Coimbatore, India, in affiliation with Anna University, Chennai, India, in 2012, the M.E. degree in computer science and engineering from the Thiagaraja College of Engineering, Madurai, India, in affiliation with Anna University, in 2014, and the Ph.D. degree from the Department of Computer Science and Engineering, Anna University. He is currently pursuing the Ph.D. degree with The University of Essex. He has worked in various institutions with a teaching experience of seven years. He is also working as an Associate Professor at Kabridahar University, Ethiopia. He has published in more than 45 international journals along with 20 international and national conferences. He has even published four patents in IPR. His current research interests include cyber security, blockchain, critical infrastructure and systems, network security, and ethical hacking. He is also an Active Member of the IEEE Computer Society and in five more professional bodies. In fact, he is also a member of the International Blockchain Organization. He is an active researcher, reviewer, and editor for many international journals.

HARIPRASATH MANOHARAN is currently working as an Assistant Professor with the Department of Electronics and Communication Engineering, Panimalar Institute of Technology, Poonamallee, Chennai, Tamil Nadul, India. He has completed 6.7 years of research experience and teaching experience. He has guided both B.Tech. and M.Tech. students for doing projects in the areas of wireless sensor networks. He has published more than 60 research articles which includes SCI, SCIE, ESCI, and SCOPUS indexed articles, and has presented papers in six international conferences. He has also published a book entitled Computer Aided State Estimation of Electric Power Networks which provides a complete guide to all research scholars in the field of electronics and communication engineering. His research interests include wireless sensor networks, data communications, and testing of communication devices.

AYMAN YAFOZ received the B.Sc. degree in information systems from King Khalid University, Abha, Saudi Arabia, the M.Sc. degree in web technology from the University of Southampton, Southampton, U.K., in 2015, and the Ph.D. degree in computer science from the University of Regina, Regina, SK, Canada, in 2021. He is currently an Assistant Professor at the Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia. His main research interests include data science, natural language processing, machine learning, and deep learning.

ADIL O. KHADIDOS received the B.Sc. degree in computer science from King Abdulaziz University, Jeddah, Saudi Arabia, in 2006, the M.Sc. degree in internet software systems from the University of Birmingham, Birmingham, U.K., in 2011, and the Ph.D. degree in computer science from the University of Southampton, Southampton, U.K., in 2017. He is currently an Assistant Professor at the Faculty of Computing and Information Technology, King Abdulaziz University. His main research interests include the areas of computer swarm robotics, entomology behavior, machine learning, self-distributed systems, and embedded systems.

KHALED H. ALYOUBI is currently an Associate Professor of computer science at the Faculty of Computing and Information Technology, King Abdulaziz University.