Probit Cryptographic Blockchain for Secure Data Transmission in Intelligent Transportation Systems

Rajesh Kumar Dhanaraj[1], Seifedine Kadry[2,3,4], Byeong-Gwon Kang[5], Yunyoung Nam[6*]

[1] School of Computing Science and Engineering, Galgotias University, India
[2] Department of Applied Data Science, University College, Norway
[3] College of Engineering and Information Technology, Ajman University, United Arab Emirates
[4] Department of Electrical and Computer Engineering, Lebanese American University, Lebanon
[5] Department of Information and Communication Engineering, Soonchunhyang University, Korea
[6] Department of Computer Science and Engineering, Soonchunhyang University, Korea
sangeraje@gmail.com, skadry@gmail.com, bgkang@sch.ac.kr, ynam@sch.ac.kr

Abstract

To address the current security challenges, Digital Twin (DT) models and strategies are to be applied to improve security, privacy, and safety in intelligent transportation systems. However, the existing algorithm was failed to address the security and privacy issues for data between the vehicles. To enhance the security of data transmission, a novel Probit Regressive Davis Mayer Kupyna Cryptographic Hash Blockchain (PRDMKCHB) technique is proposed. Initially, the source vehicle finds the nearest vehicle to transmit the data based on the trust value using the probit regression function. After finding the neighboring nodes, the Blockchain is constructed to improve the security of data transmission from the source to the destination. The Blockchain uses the Kupyna Cryptography to generate the hash value for each data. Davis Mayer compression function is to improve the security of data delivery and to minimize packet loss. The comprehensive simulation is carried out to validate the performance of the proposed PRDMKCHB technique and existing Blockchain technology in terms of packet delivery ratio, packet loss rate, and execution time. Simulation results show the performance improvement of the proposed PRDMKCHB technique compared to the previous Blockchain technology in terms of higher packet delivery ratio, minimum packet loss, and execution time with respect to the number of data packets.

Keywords: Digital Twin (DT), IoVT, Secure data transmission, Probit regression, Blockchain

1 Introduction

Intelligent transportation is a major task since voluminous data is collected while vehicles are on the go. To protect these sensitive data from unauthorized access, security systems are to be hardened [31]. To virtually represent the physical assets, Digital Twin (DT) technology is used since this software makes the asset more valuable with a huge size of data [32]. The Digital Twin technique can be able to simulate real situations precisely which helps to observe and predict the security challenges for gathered data. Most of the transport organizations which apply IoVT have started using the DT to improve the reliability and security of the voluminous data. With the help of DT, doorstep transportation is possible, and people can be able to bring the digital link in real-time to associate the services. All the components which create data while the vehicle is moving are connected through DT and this enables to use of integrated cloud and platform services to store and analyze the secured data.

Internet of Vehicles (IoV) is a novel paradigm that converges the Internet of things (IoT) into vehicular networks to benefit from everywhere through internet connectivity [33]. Vehicles that are equipped with automotive electronics devices communicate with other vehicles and roadside units (RSUs) to get information about the real-time traffic states. IoV is widely used in several applications such as communications, transportation, automotive technology, and so on [34]. To address the current security challenges, AI-based Machine Learning/Deep Learning techniques are applied preferably as the operational data stored in the cloud.

With the rapid growth of computation and communication technologies, secure data sharing is the primary function of IoV. In IoVT, data transmission between the vehicles for collaborative analysis improves the driving skill and service authority. An intelligent transportation system is a highly developed application that helps to provide information about traffic, road accidents, and emergency information to other vehicles. These kinds of sensitive data are easy to leak, and the whole network is vulnerable to some attacks. Therefore, in the process of vehicle communication for IoV, it is essentially required to protect the communication contents. However, in an IoV, which is a highly dynamic environment due to the mobility of vehicles, secure inter-vehicle communications are the significant challenges that need to be solved.

A Blockchain-based decentralized structural design was introduced in [1] for distributing the event-information between the road-side units and vehicles. The design minimizes the computation and storage overhead, but it failed to increase security in vehicular ad-hoc networks. A Blockchain Empowered Asynchronous Federated Learning scheme was developed in [2] for increasing the security and efficiency of data sharing between the vehicles. However, an efficient cryptography technique was not implemented to improve the security level further and reduce packet loss. A Blockchain-based asymmetric group key agreement protocol (B-AGKA) was introduced in [3] for IoV to protect the

*Corresponding Author: Yunyoung Nam; E-mail: ynam@sch.ac.kr

DOI: 10.53106/160792642022112306013

security of data transmission. However, the designed protocol failed to achieve a higher security level.

In IoV environments, security is a main important issue. Numerous conventional methods are developed for secure data transmission based on Blockchain technology. However, the security level was not enhanced. In traditional methods, error rate and space complexity were not minimized. In many existing methods, the execution time was not minimized for secure communication. Motivated by this, the proposed PRDMKCHB technique is chosen based on our objective. This work's aim is to enhance the security level of data transmission based on Blockchain technology.

The proposed PRDMKCHB technique is designed with the novelty of Probit regression and Davis Mayer Kupyna cryptographic hash function. The probit regression function is used to select the neighboring node based on the threshold value for lowest distance and highest trust. Probit regression function is provided the value either 0 or 1. If the value is 1, the neighboring node is chosen. Otherwise, if the value is 0, the neighboring node is not selected. Secured transmission is attained through the chosen nodes for enhancing secure data transmission with minimum time consumption. In contrast to existing works, the root hash is created with the aid of Davis Mayer hash function. Davis Mayer hash function is one-way compression function to protect unauthorized access for improving data confidentiality. In contrast to conventional methods, a one-way compression function is used in cryptography to converts two fixed-length inputs into a fixed-length output.

The rest of this article is arranged into different sections as follows. Related works are discussed in Section 2. The description of PRDMKCHB is presented in section 3. Section 4 provides a simulation setting. Followed by the performance of proposed and existing methods is discussed with different metrics in section 5. At last, the conclusion of the article is presented in section 6.

2 Related Works

A Similarity Aware Safety Multimedia Data communication approach was developed in [4] for the Internet of Vehicles. Vehicle attribute was introduced for producing the communication keys to enhance the network security. The designed approach minimizes the delay and maximizes the network performance, but the performance of the packet delivery ratio was not analyzed. An effective and secure data communication method was introduced in [5] for the Internet of vehicles. Multiple blockchain networks were developed to identify the data blocks of IoV. The method reduces the transmission delay and packet loss, but higher packet delivery was not achieved. A secured and efficient communication method was developed in [6] for the internet of vehicles. Three-level security architecture was designed in [7] to increase reliability and minimize the time overhead. The architecture minimizes the execution time and delay, but it failed to achieve a high-security level. A two-stage soft security enhancement approach was introduced in [8] to improve the security of data transmission. However, the trust assessment was not performed. A secure and efficient message authentication protocol was presented in [9] for IoV based secure communication. The protocol minimizes the performance of computation, but it failed to evaluate the performance of delay. SDN based reliable and secure data distribution architecture was developed in [10]. Multi-Generation Mixing (MGM) based network coding algorithm maximizes the reliability. The method increases the successful delivery ratio and minimizes delay, but it failed to evaluate the performance results of packet loss. Security and privacy preservation mechanism was introduced in [11] depend on crowdsensing for the internet of vehicles. An angular inclination routing was maximized the packet collection rate. The mechanism reduces time consumption, but it failed to minimize packet loss.

Lightweight cryptography was introduced in [12] for increasing security while preserving communication. The technique improves the security in terms of communication efficiency, but the packet loss rate was not minimized. A lightweight mutual authentication method was applied to perform data communication. The designed approach increases the packet delivery and reduces packet loss, but the execution time of secure transmission was not minimized. A lightweight mutual authentication protocol was developed in [13] for IoV through cryptographic procedures. The proposed protocol facilitates secure communication and reduces the computational cost, but the higher packet delivery ratio was not achieved. A Paillier Cryptosystem was developed in [14] to accomplish the secure data aggregation between the multiple vehicles. The designed technique minimizes the computational complexity, but it failed to implement the Blockchain technology to achieve privacy protection. Ciphertext-policy attribute-based encryption and elliptic curve cryptography were developed in [15] to ensure the security of data transmission. The technique obtains data distribution between dissimilar fields and minimizes the execution time of secure data transmission. But it failed to select vehicles with high trust for secure transmission. A dynamic scalable elliptic curve cryptosystem was developed in [16] to guarantee the in-vehicle security level. The technique increases the performance of security level, computation efficiency, and minimizes the power consumption. But it takes more execution time for secure transmission between the vehicles.

In [17], Blockchain technology was applied to vehicle networking for security management. The designed technology minimizes the average transmission delay, but it failed to increase the packet delivery ratio. A novel type of Blockchain technology was developed in [18] for significant message distribution between the vehicles. Local blockchain was applied for increasing the scalability of the blockchain. The technology minimizes the message overhead, but it failed to implement a type of Blockchain to deal with critical event message dissemination with less delay in the VANET environment. A Blockchain-based IoT system was developed in [19] to construct secure communication. The designed system minimizes the execution time, but the higher data delivery ratio was not achieved.

In [20], a Blockchain framework was developed to attain the secured transmission between the vehicles using a smart contract. The designed framework enhances the effectiveness and transparency of vehicle collaborations. The framework minimizes the running time, but it failed to achieve a higher packet delivery ratio. A Blockchain-based decentralized trust appraisal method was developed in [21] for increasing the vehicle's secure communication. The method minimizes the response time between the vehicles, but the delay was not minimized. A Blockchain-enabled privacy-preserving batch authentication scheme was developed in [22] for IoT based smart city environment. Voting-based Practical Byzantine Fault Tolerance (PBFT) consensus algorithm was utilized to blocks transactions. The designed scheme reduces the computation time, but it failed to improve the security of data delivery. A Blockchain-based secure data sharing system was introduced in [23]. The system minimizes the total delay, but it failed to improve the packet delivery ratio. A Blockchain-based lightweight and secure communication were performed in [24] for data authentication amid vehicles. The designed scheme minimizes the time complexity, but the delay was not reduced. An authentication-based protocol (A-MAC) was developed in [25] for vehicular communication. The protocol reduces the execution time of communication but the delay as well packet loss ratio was not minimized. Authenticated Key Management Protocol was developed in [26] to guarantee traffic security and effectiveness. AKM-IoV finds the dissimilar attack. The protocol minimizes the delay as well as packet loss, but the execution time was not reduced.

A Blockchain-based privacy protection method was presented in [27] for IoV communication. Angular routing was developed for attaining multihop routing of packets. The method reduces the delay, but the packet delivery was not increased. An IoV double-layered chain method was developed in [28] for increasing the privacy protection model of the vehicle network. The model reduces the computational complexity and increases the throughput, but the delivery ratio was not improved. An efficient signcryption method was introduced in [29] for heterogeneous IoV to achieve high-level security features. Signcryption was applied for producing a security level. But the execution time for secure communication was not minimized. An identity-based signcryption was developed in [30] for secure communication between the vehicles with high confidentiality. Identity-based mechanism enhances efficiency. However, the delay in secure communication was not minimized. Even though the significant contributions were given by many authors [10-30], the balancing between the parameters addressed like delay, packet loss, computational time and secure data transmission is a quite challenging task.

2.1 Contributions of This Work

The contribution of the proposed PRDMKCHB technique is summarized as follows,

- To improve the security level of data transmission in IoVT, a novel PRDMKCHB is introduced based on Blockchain technology.
- To improve packet delivery and reduce packet loss, PRDMKCHB uses the Davis Mayer Kupyna Cryptography based Blockchain technology. The Davis Mayer compression function generates the hash for each data. This helps to avoid the unwanted access and data packets lost during the transmission between the source vehicles to the destination vehicles.
- To minimize the execution time on secure communication, a probit regression function is applied in PRDMKCHB. The regression function analyzes the node's trust and selects the best neighboring node. Then, the secured transmission is performed via the selected nodes to improve the secure transmission with lesser time consumption.
- Finally, security investigation and extensive simulation estimation are performed with various performance metrics to underline the advantage of the proposed PRDMKCHB technique over conventional Blockchain techniques.

3 Methodology

Internet of Vehicles (IoV) connects the intelligent transportation system (ITS) along with the Internet of Things (IoT) technology. IoVT permits the vehicles to transits the data with its surroundings to enhance traffic safety and offer digital services to road users. IoVT plays a vital role in the recently developed smart city applications. The concept of smart cities has become well-known in modern metropolises due to the appearance of implanted and connected smart devices. It facilitates the connection of everything to the Internet. A major aspect of a smart city is the forthcoming generation and smart devices such as vehicles integrate into the IoT technology for sensing, communication, and social capabilities as part of the extensive IoT concept. Security presents big challenges for IoV environments. Due to the high mobility of vehicles, a very huge number of transmissions is performed in IoV. In such an event, an attacker may constitute a big risk for vehicular networks during the communication between the devices. Therefore, a novel and efficient solution is required to guarantee the security of information. Based on the motivation, a new technique called PRDMKCHB is introduced for improving security.

3.1 System Model

This section describes the system model of an IoV. This system model helps to understand that the proposed PRDMKCHB is how to achieve secure data transmission between the devices through IoT. The architecture of IoV enabled data communication is illustrated in Figure 1. The architecture consists of the internet, RSU, and vehicles. The IoT devices such as sensor nodes in the VANET can sense information such as traffic congestion information, road accidents, and emergency information, and so on. This information transmission is responsible for integrating the communications between the vehicle devices.

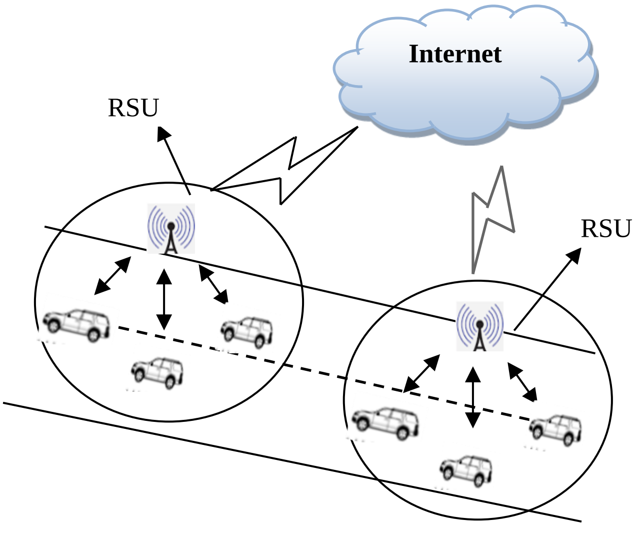

Figure 1. IoV architecture based data transmission

Figure 1 illustrates an IoV architecture consists of the internet of things (IoT), Roadside unit (RSU), and vehicles $V_1, V_2, V_3, \ldots. V_n$. In the network, the RSUs connect to the internet through uplink communication and connect to the vehicles along the road within their range through downlink communication. Therefore, the RSU act as a central coordinator between the vehicle and the internet. The secure data communication between the vehicles and vehicles to RSU is performed based on the Probit Regressive Davis Mayer Kupyna Cryptographic Hash Blockchain. Among the distributed vehicles, the source vehicle $(Sv)$is identified and it transmits the data packets $p_i = p_1, p_2, p_3, \ldots p_n$ to destination through the neighboring nodes $In_1, In_2, In_3,, \ldots. I_m$ based on Blockchain technology. The vehicles are untrusted in our system, which means that a vehicle may turn malicious and plan to obtain data from others. Based on the above system model, the proposed PRDMKCHB technique is designed, and the architecture is shown in Figure 2.

Figure 2 illustrates the flow process of the PRDMKCHB technique to improve the secure transmission between the vehicles in the network. The source vehicle 'Sv'initially finds the neighboring vehicle node for secure data transmission.

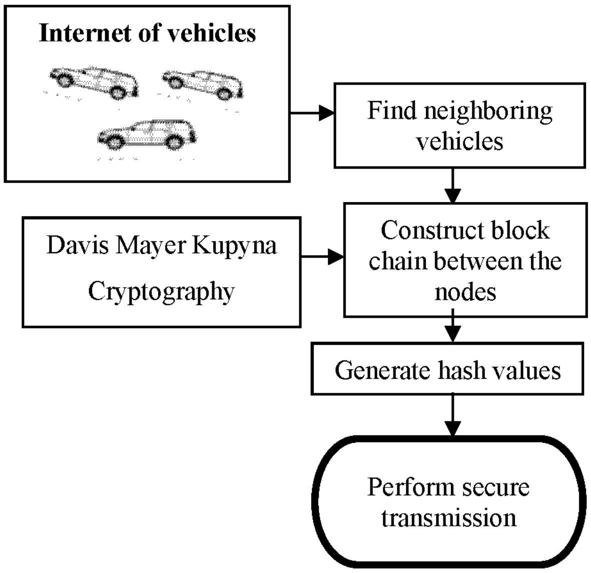
Internet of vehicles
Find neighboring vehicles
Davis Mayer Kupyna Cryptography
Construct block chain between the nodes
Generate hash values
Perform secure transmission

Figure 2. Flow process of the PRDMKCHB technique

The node which has a higher trust value, and the minimum distance is selected as neighboring nodes. By using Davis Mayer Kupyna Cryptographic, the Blockchain is constructed. Then, the hash value of every block is generated for enhancing the security level to avoid third-party access. Finally, proposed PRDMKCHB technique performs secure transmission between the vehicle nodes. A brief description of the proposed PRDMKCHB technique is explained in the following section.

3.1.1 Probit Regression-based Neighboring Node Discovery

Initially, the vehicle nodes are deployed in the network for transmitting the data. The source node initially starts to find the neighboring node using probit regression. Probit regression is the statistical method used to analyze the variables and returns the outcomes based on the probability of either 0 or 1. Let us consider the current coordinate of the vehicle node 'i' is (a_1, b_1) and the coordinate of another node 'j' (a_2, b_2) in two-dimensional space. Therefore, the distance between the two nodes is computed as follows,

$$D_{ij} = \sqrt{(a_2 - a_1)^2 + (b_2 - b_1)^2}. \qquad \textbf{(1)}$$

Where, D_{ij} stands for the distance between the two nodes. For each node, the trust value is measured as follows,

$$Trustvalue, \psi = \left[\frac{P_f}{T_f}\right]. \qquad \textbf{(2)}$$

From equation (2), ψ denotes the trust value, P_f represents the number of packets correctly forwarded, T_f denotes the total no of packet forwarded. The probit regression function is then applied to select the neighboring vehicle towards the destination for secure data transmission. The regression analysis is expressed as follows,

$$Y = \emptyset\ [X\beta + \varepsilon]. \qquad \textbf{(3)}$$

$$\emptyset^{-1}(Y) = X\beta + \varepsilon. \qquad \textbf{(4)}$$

$$F(Y) = Y' = X\beta + \varepsilon. \qquad \textbf{(5)}$$

$$F(Y) = \emptyset^{-1}(Y). \qquad \textbf{(6)}$$

Where, $F(Y)$ denotes an output of probit regression function which provides the values either 1 or 0, X denotes an input (i.e., vehicle nodes), β denotes a parameter,ε is a variable [0,1], $\emptyset$ denotes a Cumulative Distribution Function. The regression function analyzes the vehicle node with minimum distance and higher trust is chosen as the neighboring node.

$$\begin{gathered} F(Y) = \{arg\ argD(trustTH) \quad ; \\ returns\ 1\ otherwise\ ;\ returns\ 0 \\ F(Y) = \{arg\ argD(trust > TH); \\ returns\ 1\ otherwise\ ;\ returns\ 0. \end{gathered} \qquad \textbf{(7)}$$

Where, $F(Y)$ denotes an output of regression function, $arg\ argD$denotes an argument of the minimum function, D denotes a distance, T_n denotes a trust value, THdenotes a threshold. The node with minimum distance and higher trust than the threshold is chosen as the neighboring node. In this way, all the neighboring nodes from source to destination are selected. Otherwise, the node with minimum distance and higher trust than the threshold is neglected.

3.1.2 Davis Mayer Kupyna Cryptographic Hash Based Blockchain Technology

In IoVT, all the nodes move independently within the network in a dynamic manner. Security plays a noteworthy factor due to a lack of centralization, dynamic topology. Due to this, it is hard to discover the malicious and faulty nodes in the network. Data sharing communication are the main function of IoVT. It has a few noticeable characteristics, such as the sensitive information is easy to leak, and the entire network is vulnerable to various attacks. Therefore, in the process of vehicle communication for IoV, it is hard to construct an efficient technique for protecting the security of transmission contents. In this case, the secure transmission of data in the vehicle to the vehicle environment is performed by applying Davis Mayer Kupyna cryptographic hash based Blockchain technology. A Blockchain consists of several blocks that are connected using cryptographic hash functions to avoid unauthorized access. Every block includes a cryptographic hash of the previous block, a timestamp, transaction data, and Root hash. Consensus mechanism is used for authentication and verification purpose in the Blockchain. Therefore, it also helps to secure a way to distribute the data between vehicle nodes. On the contrary to conventional Blockchain technology, the proposed technique uses the Davis Mayer Kupyna cryptographic hash for secure data transmission between the vehicles. A Davis Mayer Kupyna cryptographic hash-based Blockchain provides more security without including any trusted-third party. The construction of Blockchain technology is illustrated in Figure 3.

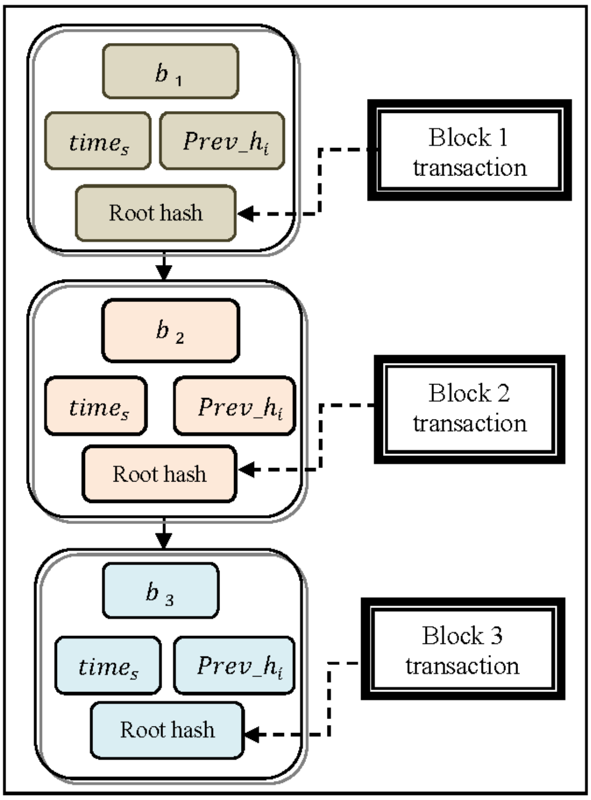

Figure 3. Construction of blockchain

Figure 3 reveals the Blockchain construction based on the different blocksb_1,b_2, b_3. Each block comprises the timestamp, previous block hash, and root hash. Each block includes a hash of the previous block ($Prev\_h_i$) used for verification. Time steps ($time_s$) indicates the time when the block was constructed. Each block comprises the transaction that includes the number of data $p_i = p_1, p_2, p_3, \dots p_n$ gathered from the environment such as traffic congestion information, road accidents, and emergency information. The root hash value of each block is generated using the Davis Mayer Kupyna cryptographic hash function. It is used to improve security by avoiding unauthorized access. A hash function is a cryptographic algorithm that takes input strings of arbitrary length and maps these to small fixed-length output.

Figure 4 given above illustrates the hash function generation. The collected information is given to the data block. Then the kupyna cryptographic hash function uses the Davis Mayer compression function to generate a hash value of each data and it is represented as β(p),β (q). Then the concatenation of these two generates hash values (β (pq)) is given to the root hash of the block. The Davis Mayer compression function generates the fixed size of the hash value.

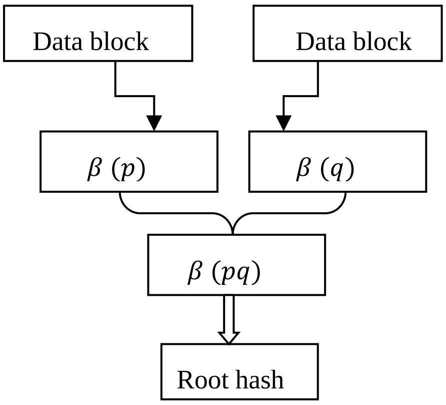

Figure 4. Hash generation

The compression function operation is shown in the following Figure 5.

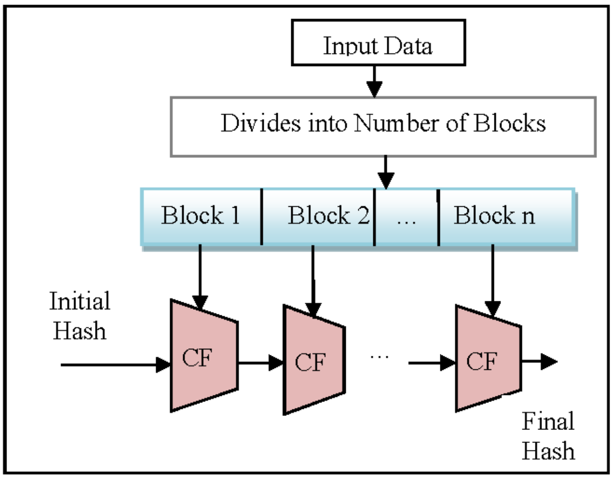

Figure 5. Davis Mayer Kupyna cryptographic hash function

Figure 5 displays the Davis Mayer Kupyna cryptographic hash function. Initially, the input data $p_i = p_1, p_2, p_3, \dots p_n$ are given as input. Each data are divided into a number of blocks that is $c_i = c_1, c_2, c_3, \dots c_b$ with a fixed size. Then the input message block is given to the Davis Mayer Compression Function (CF) which takes an input message block (c_1) and previous hash and finally generating the hash value (β_h). The operation of the Davis Mayer compression function is illustrated in Figure 6.

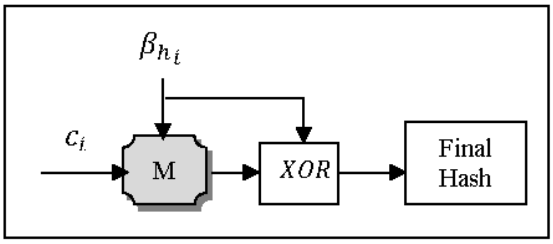

Figure 6. Davis Mayer compression function

Figure 6 illustrates the Davis Mayer compression function which receives the input message block 'c_i' and the previous hash value is initially preset. As shown in Figure 6, M denotes a block cipher. The message block (c_i) is the key to a block cipher 'M' and feeds the previous hash value (β_{h_i}) as the plaintext to be encrypted. The output ciphertext is then also XORed with the previous hash value and the message block (c_i) as the key to a block cipher. In the first round, when there is no previous hash value is set to a constant pre-specified initial value (β_h 0) in the form of binary (i.e., β_h0=010).

$$\beta_{h_i} = [M_{c_i}(\beta_{h_i}) \oplus \beta_{h_i}]. \qquad \textbf{(8)}$$

Where, β_{h_i} denotes a final hash value generated from the Davis Mayer compression function. The hash of one data block is not similar to another input block i.e., $\beta_{h_1} \neq \beta_{h_2}$. The final hash of kupyna cryptographic hash function is generated as the output of the final compression function. As a result, the hash value of each data is generated and is used to avoid the unauthorized entity. Only authorized vehicle nodes access the data, and it improves the data security level between the vehicle nodes. The step-by-step process of the Davis Mayer Kupyna cryptographic hash-based secure data transmission is described I algorithm 1.

Algorithm 1. Probit regressive Davis Mayer Kupyna cryptographic hash blockchain

```
Input: Number of vehicles $V_1, V_2, V_3, \dots . V_n$, data packets
$p_i = p_1, p_2, p_3, \dots p_n$, Source node '$Sv$', destination node '$Dv$'
Intermediate nodes $In_1, In_2, In_3, , \dots . I_m$, initial hash $\beta_h$0=010
Output: Improve secure data transmission

Begin
    for each vehicle node '$V$'
    Measure distance 'D' and trust '$T_n$'
      If $(arg\ argD_{ij} \&\& (trust > TH))$ then
    $returns$ '1'
    Select neighboring node
        else
    $returns$'0'
        end if
    End for
        For each data transmission
            Construct Blockchain
                For each $p_i$
                    Divide into message blocks $c_1, c_2, c_3, \dots c_b$
            End for
                for each block'$c$'
                    Generate hash value
            '$\beta_{h_i} = [M_{c_i}(\beta_{h_i}) \oplus \beta_{h_i}]$'
                    End for
            Obtain the final hash
                End for
            Perform secure transmission between '$Sv$' and '$Dv$'
End
```

The algorithmic process of Probit Regressive Davis Mayer Kupyna Cryptographic Hash Blockchain describes the secure data transmission between the source and destination. Firstly, probit regression is applied for discovering the neighboring node with minimum distance and higher trust. For each vehicle node, distance and trust value are computed. The regression function analyzes the node behaviors with the threshold value. The regression function is used to provide the values such as 0 or 1. When the value is 1, the neighboring node is selected. Otherwise, it is not selected the neighboring node. After finding the intermediate nodes, the Blockchain is constructed for secure data transmission. Each data is separated into several blocks with a fixed size. The kupyna cryptographic hash function is applied to Blockchain technology to generate the hash value for each data with the help of the Davis Mayer compression function. The Davis Mayer compression function is used for avoiding unwanted access. Before the transmission, the input data is hashed, and it sends to the next node for increasing security. As a result, the PRDMKCHB technique helps to protect the security of communication between the vehicle nodes.

4 Experimental Setup and Simulation

In this section, the proposed PRDMKCHB technique and the other three existing methods namely Blockchain-based Decentralized Structural [1], Blockchain Empowered Asynchronous Federated Learning [2], and B-AGKA [3] are implemented in the NS3 network simulator. The simulator is conducted with the software specification of Windows 10 Operating system, 3.0GHZ Processor type, 403MHZ RAM, 250 GB Hard disk, ASUSTek P5G41C-M Motherboard, Internet Protocol. The proposed PRDMKCHB technique is validated by using an NS3 network simulator for conducting the simulation. 500 vehicle nodes are mobile that move randomly over a squared area of A2 (1100 m * 1100 m). The various simulation parameters are listed below (Table 1).

Table 1. Simulation parameters

Simulation parameter	Value
Simulator	NS3
Number of vehicle nodes	50, 100, 150, 200, 250, 300, 350, 400, 500
Network area	1100m * 1100m
Simulation time	300s
Routing protocol	DSR
Nodes speed	0-20m/s.
Data packets	25, 50, 75, 100, 125, 150, 175, 200, 225, 250
Data packet size	10KB-100KB
Number of runs	10
Digest sizes of Kupyna hash function	256 bits
Compression function	Davis Mayer compression function

5 Performance Analysis

The simulation results of the three different methods such as the PRDMKCHB technique, Blockchain-based Decentralized Structural [1], Blockchain Empowered Asynchronous Federated Learning [2], B-AGKA [3] are discussed with respect to various performance metrics such as security level, packet loss rate, and execution time. These metrics are described as given below.

- **Security level**

The packet delivery ratio is measured based on the number of data packets correctly received at the receiver by avoiding unauthorized access. Here, the security level is measured in terms of packet delivery ratio. The transmitted data packets were successfully received without accessing unauthorized access. The formula for calculating the security level is expressed as follows,

$$PDR = \left[\frac{Np_{CR}}{N}\right] * 100. \quad \textbf{(9)}$$

Where PDR denotes a packet delivery ratio, N denotes the number of data packets, Np_{CR}denotes the number of packets correctly received. The packet delivery ratio is measured interms of percentage (%).

- **Data confidentiality rate**

The data confidentiality rate is defined as the number of data accessed by authorized access, and it is protected from unauthorized access. The data confidentiality rate is measured using the following equation,

$$DCR = \left[\frac{Numberofdataprotectedfromauthorizedaccess}{N}\right] * 100. \quad \textbf{(10)}$$

Where DCR indicates a data confidentiality rate, N denotes the number of data packets. The packet loss rate is measured in percentage (%).

- **Execution time**

Execution time is defined as the time taken by the algorithm to transmit the data packets from source to destination in a secure manner. It is measured in terms of milliseconds (ms).

$$ET = N * time(transmitonepacket). \quad \textbf{(11)}$$

$'ET'$ denotes an execution time, 'N' denotes the number of packets,

- **Packet delay**

It is measured as the difference between the actual arrival time of the data packets and the observed arrival time of the data packets at the destination. The overall delay is measured as follows,

$$D = [t_{act}] - [t_{ob}]. \quad \textbf{(12)}$$

Where 'D' represents the packets delay, t_{act} denotes an actual arrival time and 't_{ob}' symbolizes the observed arrival time. The overall packet delay is estimated in terms of milliseconds (ms).

The observed results indicate that the proposed PRDMKCHB technique increases the packet delivery ratio than the existing Blockchain-based Decentralized Structural [1], Blockchain Empowered Asynchronous Federated Learning [2], and B-AGKA [3]. This is proved through statistical analysis. By considering 25 data packets being sent from the source vehicle node, 23 data packets are correctly received at the destination vehicle using the PRDMKCHB technique, and the packet delivery ratio is 92%. Whereas 22, 22, and 21 data packets are successfully received by applying Blockchain-based Decentralized Structural [1], Blockchain Empowered Asynchronous Federated Learning [2], and B-AGKA [3], and the delivery ratio are 90%, 88%, and 84%, respectively. The average of ten comparison results indicates that the PRDMKCHB technique achieves higher packet delivery by 4% compared to [1], 7% compared to [2] and 12%when compared to [3].

Figure 7 shows the observed higher packet delivery ratio helps to improve the security of data transmission between the vehicles. According to the attained results, the proposed PRDMKCHB technique delivers more packets as compared to the conventional Blockchain techniques. This improvement is achieved by the PRDMKCHB technique initially measures the trust value of the node to construct the Blockchain. Since the conventional Blockchain technique was not used an efficient cryptographic hash function to hide the information. In the contrast, the PRDMKCHB technique uses the Davis Mayer Kupyna Cryptographic technique to convert the given input data into the hash value. The hash value is generated by using this technique for avoiding unauthorized access. This helps to provide higher security for data transmission. The number of data packets increased, and then the security level is increased. As a result, the proposed PRDMKCHB technique achieves a higher delivery ratio resulting in increases in the security level in IoV.

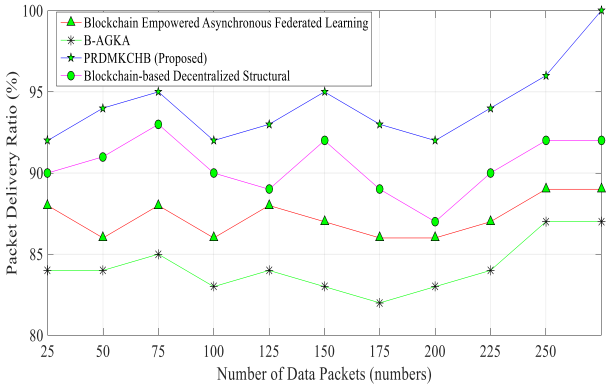

Figure 7. Performance analysis of packet delivery ratio

Figure 8 portrays the graphical results of the data confidentiality rate using three different methods PRDMKCHB technique, Blockchain-based Decentralized Structural [1], Blockchain Empowered Asynchronous Federated Learning [2], and B-AGKA [3]. The figure demonstrates the data confidentiality rate of the proposed PRDMKCHB technique whereas the red and green colored cone indicates the data confidentiality rate of existing [1-3], respectively. The numbers of data packets are taken in the range from 25 to 250. Let us consider 25 data packets, 24 data are protected by unauthorized access and the data confidentiality rate is 96%. Similarly, 21, 21, and 20 data are protected by unauthorized access and the data confidentiality rates are 86%, 84%, and 82% using Blockchain-based Decentralized Structural [1], Blockchain Empowered Asynchronous Federated Learning [2], and B-AGKA [3]. The average of the ten runs and the results are indicated by the data confidentiality rate is considerably increased by 7%, 10%, and15% when compared to existing methods. Among the three Blockchain technology, the proposed PRDMKCHB technique improves data confidentiality rate performance than the other two existing methods. The reason for achieving higher data confidentiality is to apply the Davis Mayer Kupyna Cryptography used in the proposed PRDMKCHB technique. When constructing the Blockchain between the vehicles. The hashed data transmission between the nodes avoids unwanted access to the data packets. This helps to improve the secure data confidentiality rate.

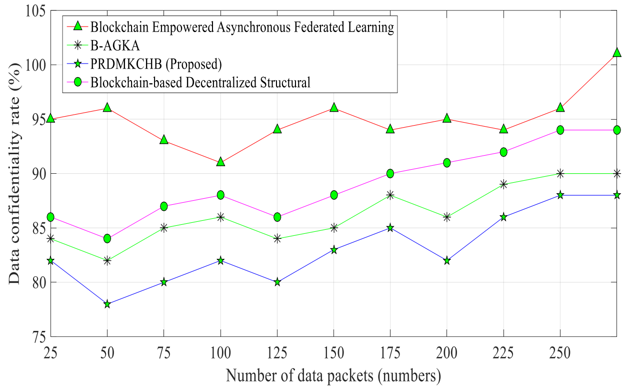

Figure 8. Performance analysis of data confidentiality rate

Figure 9 reveals the simulation of execution time over different numbers of data packets sent from source vehicle to destination considered in the ranges from 25 to 250 for 10 different runs. The simulations are conducted for 25 data packets being sent, the execution time of secure transmission is observed using the proposed PRDMKCHB is 27ms whereas the time consumption of secure transmission is 29ms, 30ms and 33ms observed using Blockchain-based Decentralized Structural [1], Blockchain Empowered Asynchronous Federated Learning [2], and B-AGKA [3].

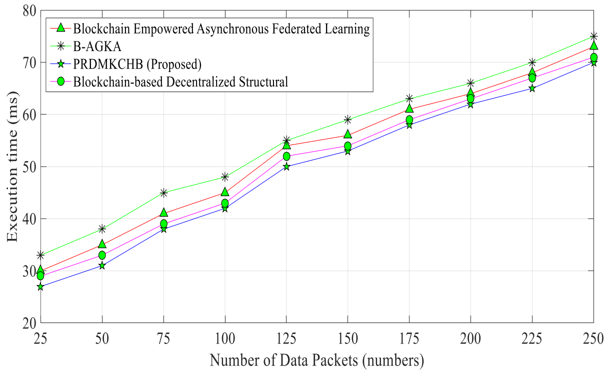

Figure 9. Performance analysis of execution time

Likewise, ten runs are performed, and the results are observed for each method. The execution time of secure data transmission from source to destination is minimized using PRDMKCHB is minimized to the existing methods. The existing methods neighboring node is not discovered for transmitting the data packets from source to destination. With the implementation of the probit regression function and Davis Mayer, compression functions are applied in PRDMKCHB technique. It selects the neighboring nodes with higher trust through the probit regression function. The neighborhood trusted nodes are discovered between the sources to destination efficiently transmit the data packets. Besides, the Davis Mayer compression function used in the proposed cryptography technique quickly generates the hash for each data. Then, the trusted node accurately performs data transmission with lesser time. From the observed results, the proposed PRDMKCHB technique outperforms well in terms of achieving lesser time. The average execution time of the PRDMKCHB technique is considerably reduced by 3%, 6% and 11% when compared to existing [1-3].

Figure 10 illustrates the performance of delay with respect to the number of packets being sent from the source node. While increasing the number of data packets, the packet delay of the data transmission gets increased for all the methods. But comparatively, the observed results indicate that the delay is minimized using the PRDMKCHB technique. This is due to the PRDMKCHB technique uses probit regression function and Davis Mayer compression function. Firstly, discovers the neighboring node with a high trust value receives the data packets and it forwards to the destination with minimum time. As a result, the average end-to-end delay of the PRDMKCHB technique is considerably reduced by 8%, 16%, and 23% when compared to Blockchain-based Decentralized Structural [1], Blockchain Empowered Asynchronous Federated Learning [2], and B-AGKA [3].

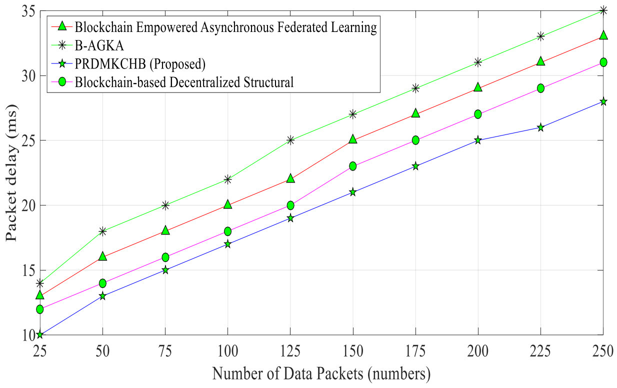

Figure 10. Performance analysis of the packet delay

6 Conclusion

In this work, the data security in Intelligent Transportation System is analyzed in the IoVT environment. To deal with these problems, a novel technique called PRDMKCHB is introduced, and it is better than the conventional Blockchain technology since it uses regression and cryptography based Blockchain. Initially, the probit regression is used to discover the neighboring vehicles with high trust. Also, it is used to choose the optimized participating nodes with minimum transmission time and delay. Next, the Blockchain is built to share the information among the nodes using the Artificial Intelligence technique. The Davis Mayer Kupyna Cryptography technique is employed to perform secure transmission amongst the participating nodes, depended on the

Blockchain technology. By integrating compression function into the Blockchain, the quality of data security gets improved by generating the hash value. Also, the compression function is used for avoiding unauthorized entity. Finally, it concluded that the proposed PRDMKCHB efficiently handles the secure information transmission reliably and securely with help of regression and cryptography based Blockchain Technology. A simulation is conducted with NS3 Simulator through the different metrics such as security level, packet delivery ratio, packet loss rate, and execution time. The performance results specify that the proposed PRDMKCHB achieved better performance through the security level in terms of high packet delivery ratio, and minimum packet loss as well as lesser execution time than the other conventional Blockchain methods. Blockchain technology is used to preserve the systems, and devices from attacks. The advantage of the proposed technique such as enhance traffic management, providing driver assistance, providing route optimization, preventing possible crashes, and avoiding security risks in the intelligent transportation system. The proposed PRDMKCHB technique is failed to measure the throughput, data integrity rate metric. For future research, propose technique is extended to provide a more secure framework which consists of secured data transmission for measuring throughput, data integrity rate VANET.

Acknowledgement

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the korea government (MSIT) (No. 2022H1D8A3038040) and the Soonchunhyang University Research Fund.

References

[1] S. Dwivedi, R. Amin, S. Vollala, R. Chaudhry, Blockchain-based secured event-information sharing protocol in internet of vehicles for smart cities, *Computers & Electrical Engineering*, Vol. 86, Article No. 106719, September, 2020.

[2] Y. Lu, X. Huang, K. Zhang, S. Maharjan, Y. Zhang, Blockchain Empowered Asynchronous Federated Learning for Secure Data Sharing in Internet of Vehicles, *IEEE Transactions on Vehicular Technology*, Vol. 69, No. 4, pp. 4298-4311, April, 2020.

[3] Q. Zhang, Y. Li, R. Wang, J. Li, Y. Gan, Y. Zhang, X. Yu, Blockchain-based asymmetric group key agreement protocol for internet of vehicles, *Computers & Electrical Engineering*, Vol. 86, Article No. 106713, September, 2020.

[4] D. Wu, L. Deng, H. Wang, K. Liu, R. Wang, Similarity Aware Safety Multimedia Data Transmission Mechanism for Internet of Vehicles, *Future Generation Computer Systems*, Vol. 99, pp. 609-623, October, 2019.

[5] W. Zhang, G. Li, An Efficient and Secure Data Transmission Mechanism for Internet of Vehicles Considering Privacy Protection in Fog Computing Environment, *IEEE Access*, Vol. 8, pp. 64461-64474, March, 2020.

[6] L. Wang, X. Liu, NOTSA: Novel OBU with Three-Level Security Architecture for Internet of Vehicles, *IEEE Internet of Things Journal*, Vol. 5, No. 5, pp. 3548-3558, October, 2018.

[7] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. Kim, J. Zhao, Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory, *IEEE Transactions on Vehicular Technology*, Vol. 68, No. 3, pp. 2906-2920, March, 2019.

[8] S. Yu, J. Lee, K. Park, A. Das, Y. Park, IoV-SMAP: Secure and Efficient Message Authentication Protocol for IoV in Smart City Environment, *IEEE Access*, Vol. 8, pp. 167875-167886, September, 2020.

[9] J. Bhatia, P. Kakadia, M. Bhavsar, S. Tanwar, SDN-Enabled Network Coding-Based Secure Data Dissemination in VANET Environment, *IEEE Internet of Things Journal*, Vol. 7, No. 7, pp. 6078-6087, July, 2020.

[10] L. Krishnasamy, R. Dhanaraj, D. Ganesh Gopal, T. R. Gadekallu, M. Aboudaif, E. A. Nasr, A Heuristic Angular Clustering Framework for Secured Statistical Data Aggregation in Sensor Networks, *Sensors*, Vol. 20, No. 17, Article No. 4937, September, 2020.

[11] A. Castiglione, F. Palmieri, F. Colace, M. Lombardi, D. Santaniello, G. D'Aniello, Securing the internet of vehicles through lightweight block ciphers, *Pattern Recognition Letters*, Vol. 135, pp. 264-270, July, 2020.

[12] H. Vasudev, V. Deshpande, D. Das, S. Das, A Lightweight Mutual Authentication Protocol for V2V Communication in Internet of Vehicles, *IEEE Transactions on Vehicular Technology*, Vol. 69, No. 6, pp. 6709-6717, June, 2020.

[13] K. Lalitha, R. Thangarajan, S. Udgata, C. Poongodi, A. Sahu, GCCR: An Efficient Grid Based Clustering and Combinational Routing in Wireless Sensor Networks, *Wireless Personal Communications*, Vol. 97, No. 1, pp. 1075-1095, November, 2017.

[14] J. Pan, J. Cui, L. Wei, Y. Xu, H. Zhong, Secure data sharing scheme for VANETs based on edge computing, *EURASIP Journal on Wireless Communications and Networking*, Vol. 2019, No. 1, pp. 1-11, June, 2019.

[15] J. Wang, J. Li, H. Wang, L. Zhang, L. Cheng, Q. Lin, Dynamic Scalable Elliptic Curve Cryptographic Scheme and Its Application to In-Vehicle Security, *IEEE Internet of Things Journal*, Vol. 6, No. 4, pp. 5892-5901, August, 2019.

[16] T. Jiang, H. Fang, H. Wang, Blockchain-Based Internet of Vehicles: Distributed Network Architecture and Performance Analysis, *IEEE Internet of Things Journal*, Vol. 6, No. 3, pp. 4640-4649, June, 2019.

[17] R. Shrestha, R. Bajracharya, A. Shrestha, S. Nam, A new type of blockchain for secure message exchange in VANET, *Digital Communications and Networks*, Vol. 6, No. 2, pp. 177-186, May, 2020.

[18] R. Jabbar, M. Kharbeche, K. Al-Khalifa, M. Krichen, K. Barkaoui, Blockchain for the Internet of Vehicles: A Decentralized IoT Solution for Vehicles Communication Using Ethereum, *Sensors*, Vol. 20, No. 14, Article No. 3928, July, 2020.

[19] B. Yin, Y. Wu, T. Hu, J. Dong, Z. Jiang, An Efficient Collaboration and Incentive Mechanism for Internet of Vehicles (IoV) With Secured Information Exchange Based on Blockchains, *IEEE Internet of Things Journal*, Vol. 7, No. 3, pp. 1582-1593, March, 2020.

[20] M. Cinque, C. Esposito, S. Russo, O. Tamburis, Blockchain-empowered decentralised trust management for the Internet of Vehicles security, *Computers & Electrical Engineering*, Vol. 86, Article No. 106722, September, 2020.

[21] P. Bagga, A. Sutrala, A. Das, P. Vijayakumar, Blockchain-based batch authentication protocol for Internet of Vehicles, *Journal of Systems Architecture*, Article No. 101877, February, 2021.

[22] P. Chinnasamy, S. Udgata, L. K, J. A, Multi-objective based deployment of throwboxes in Delay Tolerant Networks for the Internet of Things environment, *Evolutionary Intelligence*, Vol. 14, No. 2, pp. 895-907, June, 2021.

[23] M. Kamal, G. Srivastava, M. Tariq, Blockchain-Based Lightweight and Secured V2V Communication in the Internet of Vehicles, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 22, No. 7, pp. 3997-4004, July, 2021.

[24] N. Gupta, R. Manaswini, B. Saikrishna, F. Silva, A. Teles, Authentication-Based Secure Data Dissemination Protocol and Framework for 5G-Enabled VANET, *Future Internet*, Vol. 12, No. 4, Article No. 63, April, 2020.

[25] L. Krishnasamy, T. Ramasamy, R. Dhanaraj, P. Chinnasamy, A geodesic deployment and radial shaped clustering (RSC) algorithm withstatistical aggregation in sensor networks, *Turkish Journal of Electrical Engineering & Computer Sciences*, Vol. 29, No. 3, pp. 1464-1478, May, 2021.

[26] M. Saleem, K. Mahmood, S. Kumari, Comments on "AKM-IoV: Authenticated Key Management Protocol in Fog Computing-Based Internet of Vehicles Deployment", *IEEE Internet of Things Journal*, Vol. 7, No. 5, pp. 4671-4675, May, 2020.

[27] N. Wang, W. Yang, X. Wang, L. Wu, Z. Guan, X. Du, M. Guizani, A blockchain based privacy-preserving federated learning scheme for Internet of Vehicles. *Digital Communications and Networks*, In press, 2022. https://doi.org/10.1016/j.dcan.2022.05.020

[28] R. K. Dhanaraj, L. Krishnasamy, O. Geman, D. R. Izdrui, Black hole and sink hole attack detection in wireless body area networks*, Computers, Materials & Continua*, Vol. 68, No. 2, pp. 1949-1965, April, 2021.

[29] A. Elkhalil, J. Zhang, R. Elhabob, N. Eltayieb, An efficient signcryption of heterogeneous systems for Internet of Vehicles, *Journal of Systems Architecture*, Vol. 113, Article No. 101885, February, 2021.

[30] H. Xiong, Y. Hou, X. Huang, Y. Zhao, Secure message classification services through identity-based signcryption with equality test towards the Internet of vehicles, *Vehicular Communications*, Vol. 26, Article No. 100264, December, 2020.

[31] A. Mahmood, H. Zen, S. M. S. Hilles, Big Data and Privacy Issues for Connected Vehicles in Intelligent Transportation Systems, in: S. Sakr, A. Zomaya (Eds.), *Encyclopedia of Big Data Technologies*, Springer, 2018, pp. 196-203.

[32] A. Sharma, E. Kosasih, J. Zhang, A. Brintrup, A. Calinescu, Digital Twins: State of the Art Theory and Practice, Challenges, and Open Research Questions, *Journal of Industrial Information Integration*, Article No. 100383, November, 2020.

[33] F. Yang, S. Wang, J. Li, Z. Liu, Q. Sun, An Overview of Internet of Vehicles, *China Communications*, Vol. 11, No. 10, pp. 1-15, October, 2014.

[34] C. Chen, S. Quan, A Summary of Security Techniques-Based Blockchain in IoV, *Security and Communication Networks*, Vol. 2022, Article No. 8689651, February, 2022.

Biographies

Rajesh Kumar Dhanaraj is a Professor in the School of Computing Science and Engineering at Galgotias University, Greater Noida, India. He received the B.E. degree in Computer Science and Engineering from the Anna University Chennai, India in 2007 and the M.Tech from the Anna University Coimbatore, India in 2010 and Ph.D. degree in Computer Science from Anna University, Chennai, India, in 2017. He has contributed 30+ Authored and Edited books on various technologies, 21 Patents and 53 articles and papers in various refereed journals and international conferences and contributed chapters to the books. His research interests include Machine Learning, Cyber-Physical Systems and Wireless Sensor Networks. He is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE), member of the Computer Science Teacher Association (CSTA); and International Association of Engineers (IAENG). He is serving as an Associate Editor and Guest Editor for reputed journals. He is an Expert Advisory Panel Member of Texas Instruments Inc USA.

Seifedine Kadry received the bachelor's degree from Lebanese University, in 1999, the M.S. degree from the University of Reims, France, and the EPFL, Lausanne, in 2002, the Ph.D. degree from Blaise Pascal University, France, in 2007, and the H.D.R. degree from the University of Rouen Normandy, in 2017. He is currently a Full Professor of data science with the Noroff University College, Norway and Department of Electrical and Computer Engineering, Lebanese American University, Byblos, Lebanon. He is also an ABET Program Evaluator of computing and an ABET Program Evaluator of engineering technology. His current research interests include data science, education using technology, system prognostics, stochastic systems, and probability and reliability analysis.

Byeong-Gwon Kang received the B.S., M.S., and Ph.D. degrees in electrical engineering from Yonsei University, Korea in 1986, 1988, and 1993 respectively. He was a Senior Researcher at the Division of Mobile Communication System Development of ETRI (Electronics and Telecommunications Research Institute), Daejeon, Korea from 1993 to 1997. He is currently a Full Professor with Department of Information and Communication Engineering, Soonchunhyang University, Asan, Korea since 1997. He was a visiting scholar of Georgia

Institute of Technology, GA, USA from 2005 to 2006. His research interests include mobile communication systems, short range communication, regulations of wireless communication systems, RFID, signal processing, intelligent transportation system, and healthcare systems.

Yunyoung Nam received the B.S., M.S., and Ph.D. degrees in computer engineering from Ajou University, Korea in 2001, 2003, and 2007 respectively. He was a Senior Researcher with the Center of Excellence in Ubiquitous System, Stony Brook University, Stony Brook, NY, USA, from 2007 to 2010, where he was a Postdoctoral Researcher, from 2009 to 2013. He was a Research Professor with Ajou University, from 2010 to 2011. He was a Postdoctoral Fellow with the Worcester Polytechnic Institute, Worcester, MA, USA, from 2013 to 2014. He was the Director of the ICT Convergence Rehabilitation Engineering Research Center, Soonchunhyang University, from 2017 to 2020. He has been the Director of the ICT Convergence Research Center, Soonchunhyang University, since 2020, where he is currently an Associate Professor with the Department of Computer Science and Engineering. His research interests include multimedia database, ubiquitous computing, image processing, pattern recognition, context-awareness, conflict resolution, wearable computing, intelligent video surveillance, cloud computing, biomedical signal processing, rehabilitation, and healthcare systems.