A Secure Blockchain Enabled V2V Communication System Using Smart Contracts

Debashis Das, Sourav Banerjee, *Senior Member, IEEE*, Pushpita Chatterjee, *Senior Member, IEEE*, Uttam Ghosh, *Senior Member, IEEE*, and Utpal Biswas

***Abstract*— In recent years, the corporate and industrial sectors have been experiencing significant transformations in vehicle-to-vehicle (V2V) communication. It can improve vehicle safety by giving signals to other vehicles wirelessly. The latest software, hardware, and technologies are applied to develop trusted applications that make V2V communication more believable. Today, various technologies are incorporated into vehicles to remove the barrier to existing challenges. The connected vehicles in V2V communication use sensors, data storage, and communication devices. Vehicles can communicate using the latest secure and trusted Cellular Vehicle-to-Everything (C-V2X) technology using direct and network communication modes. Even connected vehicles suffer from data security, user privacy, reliable environment, and vehicle security. Blockchain can help to eliminate those issues in V2V communication systems. Herein, a secure blockchain-enabled V2V communication system (BVCS) is proposed to enhance the security of vehicles and secure data sharing and communication among vehicles. The developed smart contracts in this paper can authenticate users and their vehicles automatically. In this paper, the proposed algorithms can authenticate users, detect unauthorized access, and establish secure communication between vehicles. The proposed system can enhance data security, user privacy, and vehicle security and provide a trusted environment in V2V communication systems.**

***Index Terms*— Blockchain technology, blockchain in C-V2X, smart contracts, V2V communication, vehicle security.**

I. Introduction

V2V communication is one of the information-sharing technology to facilitate crash avoidance, vehicle speed detection, location tracking, and vehicle movement [1]. It is a wireless transmission of information between vehicles to prevent accidents by sharing their positions, speed, and heading. Vehicle-to-Vehicle (V2V) communication can help to design various vehicle applications in the Intelligent Transport System (ITS). Different existing communication technologies such as Dedicated Short-Range Communications (DSRC), Fourth Generation Long-Term Evolution (4G-LTE), and Cellular-Vehicle to Everything (C-V2X) can provide V2V communication facilities with a quick response time. Thus, vehicles can share information with others in dangerous situations on the road. V2V also enables vehicle safety and reduces traffic congestion. In short, V2V can provide dedicated and constant communication services with or without internet facilities [2].

The communication platform of V2V can convey various threats as there has no such protocol that can secure the data transmission between vehicles. V2V communication needs to share more information concerning traditional ones. All the sensitive data, firmware updates, and safety-related data are sent through the network [3]. Thus, different types of attacks in cyber-physical systems can harm the system and vehicles [4]. So, cyberattacks are primary issues in V2V communication for keeping safe data [5]. Attackers can manipulate the system data such as user data, vehicle data, and transaction data. Therefore, a secure communication system is required to overcome those issues. So, data can be exchanged securely and shared with the correct information [6].

The corporate and industrial sectors have been trying to incorporate reliable and low-risk technology for secure and trusted V2V communication. Meanwhile, Blockchain, a decentralized and reliable technology, [7] has taken a position as the fastest-growing technology for its intrinsic features. It can secure the data using cryptographic hash functions. Also, Blockchain has immutable data storage. Thus, Blockchain can fulfill the security requirements of V2V communication with its beneficial features such as data immutability, transparency, data security, and privacy of its users [8].

In this paper, a blockchain-enabled V2V communication system (BVCS) is proposed to facilitate significant features like data security, vehicle security, and user privacy. Vehicles can share verified and trusted data with others without concerning security aspects in V2V communication. The proposed system is divided into various components such as user authentication, vehicle authentication, unauthorized access detection to the user application and vehicle, and V2V communication. So, the proposed system can provide user privacy, vehicle security, data security, transparency of transactions, and a secure communication environment.

A. Main Contributions of This Paper

This paper presents a V2V communication system using blockchain and smart contracts. The main contributions of the proposed work are stated in the following:

- A secure BVCS is designed and implemented in detail step by step.
- User authentication, vehicle validation, and secure V2V communication algorithms are described.

Manuscript received 10 December 2021; revised 6 May 2022 and 19 August 2022; accepted 11 November 2022. This work was supported by University Research Scholar (URS-SRF), through the University of Kalyani, Kalyani, India. The Associate Editor for this article was J. C.-W. Lin. *(Corresponding author: Uttam Ghosh.)*

Debashis Das and Utpal Biswas are with the Department of CSE, University of Kalyani, Kalyani 741235, India (e-mail: debashisdascse21@klyuniv.ac.in; utpalbiswas@klyuniv.ac.in).

Sourav Banerjee is with the Department of CSE, Kalyani Government Engineering College, Kalyani 741235, India (e-mail: mr.sourav.banerjee@ieee.org).

Pushpita Chatterjee is with the Department of EE and CS, Howard University, Washington, DC 20059 USA (e-mail: pushpita.c@ieee.org).

Uttam Ghosh is with the Department of CS and DS, Meharry Medical College (MMC), Nashville, TN 37208 USA (e-mail: ghosh.uttam@ieee.org).

Digital Object Identifier 10.1109/TITS.2022.3226626

- All the designed algorithms are implemented and tested using smart contracts.
- The performance analysis of the proposed system is discussed in detail and a theoretical comparison is presented in a tabular form.

B. Organization of the Paper

Section II explains the fundamentals of C-V2X technology and its limitations and solutions, blockchain technology, and smart contracts. In section III, the related existing works are discussed. Section IV presents the proposed system's architecture and its implementation procedure. In section V, tested results are given with a clear discussion. Section VI analyzes the security achievements of the proposed system with a detailed discussion. Finally, section VII concludes the paper by providing related information on future works.

II. Background and Overview

A. V2V Communication

V2V communication can use many wireless access methods to establish communications between vehicles. These communications technologies can enhance road safety and traffic efficiency and provide passenger and driver comfort through conferring security and safety applications. A few such technologies are C-V2X [9], DSRC [10], 4G-LTE [10], Wireless Local Area Network (WLAN)/ Wireless Fidelity (WI-FI) [11], ZigBee (IEEE 802.15.4) [11], Ultra-Wide Band (IEEE 802.15.3a) [11], and BLUETOOTH (IEEE 802.15.1) [11]. C-V2X is a communication technology that can share information (i.e., road conditions, movement alerts, vehicle speed, vehicle heading, vehicle position) among vehicles in a high-frequency data transferring mode within 300-400 meters [12]. C-V2X provides services in two modes: direct communication mode and network communication mode. Vehicles need not connect with a cellular network as no SIM card is required in direct communication modes. C-V2X can be used in commercial applications through connecting network communication modes. This mode enables C-V2X to take advantage of data security and privacy in mobile communication networks.

Security Requirements of the V2V Communication: Since vehicles are rapidly connected to the internet using the Internet of Things (IoT), V2V communication has notable limitations. It is difficult to assure the security of vehicles due to their high connectivity. However, a sensitive information transfer can lead to privacy issues also. Table I demonstrates the security requirements for acquiring reliable services in the V2V communication system [13]. Several applications are developed to enhance the security of the V2V communication system. Though, several requirements are not met due to the infrastructure of existing methodology and the nature of existing technologies. There is a need for a secure solution for V2V communication to fulfill the security requirements. Blockchain is a much more secure technology that can satisfy the security requirements of V2V communication.

TABLE I
Security Requirements of the V2V Communication

Security Requirements	Description
Data Authenticity	The source of information should be genuine and trustworthy.
Integrity	The information should not be adjusted when exchanging.
Anonymity	The entity information should be trusted.
Confidentiality	The information should only be accessed by authorized entities.
Availability	The implemented services should be operational.
Non-repudiation	An entity's action should be indisputable.
Access Control	Entities should be authorized before accessing the information.
Freshness	Real-time information should be refreshed in time.

B. Blockchain Technology

Blockchain is a shared distributed ledger issued by Nakamoto in 2008 [14]. It uses a cryptographic hash function, signature-based authentication scheme, and consensus protocols to communicate with each other. It is a cryptographically linked and secured ever-expanding record list known as blocks. The blockchain has the longest chain of blocks that store transactions. Transactions can be created by different nodes connected from several geographical locations. Consensus mechanisms take the role of establishing a trusted relation between various nodes. Blockchain has recorded and transmitted data across thousands of nodes. Each user in the blockchain network has a private and public key to make transactions securely and anonymously. Using Proof of Work (PoW), Proof of Stake (PoS), and other consensus techniques [15], blockchain provides a trustworthy network in which any member may acquire block information without relying on a single node. At first, blockchain is applied in Bitcoin, a cryptocurrency exchange platform, due to its reliable features such as decentralization, immutability, availability, and transparency [16]. Therefore, it is incorporated into various domains and applications for its intrinsic characteristics.

C. Smart Contracts

A Smart contract [17], [18] is a digital agreement to create an automatic verifiable transaction among blockchain nodes without involving third parties. The contract is saved in the blockchain to make it tamper-proof. The smart contract is saved in the blockchain to make it tamper-proof. The smart contract is deployed by authorized nodes and executed automatically based on predefined logic and conditions. It is nothing but computer programs that are saved in the form of codes in blocks. After getting triggered by any events, it can execute automatically. The smart contract is a verifiable digital contract that can deploy to a data-storage virtual machine like Ethereum Virtual Machine (EVM) [19]. Solidity language can be used to write a smart contract [20]. Ultimately, a user can call the smart contact's function for executing required events [21].

III. Literature Review

Table II presents a comparative analysis of several existing works with the proposed work. Demba and Möller [1] proposed an upgraded architectural approach that might assist in the secure system functioning without interruption and increased physical safety. They used DSRC technology for V2V communications. Ali [2] proposed three methods to

TABLE II
COMPARATIVE ANALYSIS OF EXISTING WORKS WITH THE PROPOSED WORK

Method	Proposed Method	Technology Used	Environment	Findings	Limitations
[1]	The architectural system of status checking application for increasing vehicle safety.	DSRC	Centralized	Increased physical safety.	Secure Authentication. User Privacy. Vehicle Security.
[2]	Physical adaptive data transmission and V2V communication scheme.	Adaptive Modulation and Coding mechanism with DSRC, C-V2X, and 4G-LTE	Centralized	Increased throughput. Reliable data transmission.	Secure Authentication. Data Security.
[22]	A graph-based multilayer network model for V2V enabled ATIS.	A graph-based reverse search algorithm	Centralized	Faster data transmission. Route finding strategies for traffic conditions.	Data Security. User privacy.
[23]	Fingerprint generation for vehicle authentication using channel characteristics of wireless networks.	Blockchain technology.	Decentralized	Real-time advisory detection within the network. Lower computational complexities. Free from m latency issues.	User authentication. Vehicle safety. No recovery mechanism is given after vehicles are attacked by hackers.
[24]	Blockchain-enabled IoT solution for V2V communication.	Blockchain technology, IoT, Ethereum	Decentralized	Security. Centralization. Privacy.	User and vehicle Authentication. Computational Complexities.
[25]	Data sharing mechanism for vehicles.	Blockchain technology.	Decentralized	Established a trusted platform for vehicles.	Lack of user and vehicle authentication. Validation of users and vehicles.
[26]	VehicleChain is proposed for V2V and V2I communication.	Blockchain technology.	Decentralized	Validation of vehicles at the time of communication. Protects cyber-physical attacks.	Vehicle data authentication. Data can be sent before the validation of the receiver.
[27]	Blockchain-enabled authentication scheme for vehicular networks.	Blockchain technology	Decentralized	Identity verification of vehicles.	Computational cost. Lack of automated authentication.
Proposed Work	Blockchain and smart contract-based V2V communication system with secure authentication and validation of users and vehicles.	Blockchain technology, C-V2X, Smart Contracts	Decentralized	Secure Authentication. Data Security. Vehicle Security. User privacy. Secure V2V Communication.	-

provide high-speed mobility and an intricate channel formation for the V2V communication network. Kim and Peeta [22] presented the V2V-based Advanced Traveler Information System (ATIS) network modeling framework. This model has three layers the physical layer, the data flow layer, and the communication layer. The proposed approach also offers responsive modeling capabilities to explain the evolution of information. Hu and Luo [4] presented the fundamental ideas for safe communication. And, then they provided secure communication mechanisms, including information authentication, information encryption, and security against infiltration. Kamal et al. [25] proposed wireless-based fingerprint generation methods to authenticate vehicles in real time. The proposed scheme has been developed using blockchain technology to enhance the complexity and delays of the network. Jabbar et al. [26] developed a blockchain-enabled real-time application for secure and easy communications between vehicles and connected entities in the V2X communication system. They have also developed a Decentralized Application (Dapp) contract. Singh et al. [27] suggested and developed a method for communication between vehicles using blockchain. They offered an incentive-based Intelligent Vehicle-Trust Point (IV-TP) scheme to encourage vehicles for trusted communication. Patel et al. [28] suggested a blockchain-based application named VehicleChain that is dependable and cost-effective for sharing data in V2V and Vehicle-to-Infrastructure (V2I) communication modes. This method can secure data from any cyber-physical attacks. Malik et al. [29] established a blockchain-based retraction and authentication framework to overcome two types of cost: communication and computational in V2V communications by eliminating third parties from the system using Road Side Units (RSUs) for vehicle identification. Table III represents the differentiation of proposed work with IoT [23] and Artificial Intelligence (AI)-based IoT [24] works based on various characteristics.

IV. PROPOSED SYSTEM

In this paper, a secure Blockchain-enabled V2V Communication System (BVCS) is proposed to enable secure communication between vehicles by sharing the correct information. Fig. 1 shows the system model of the proposed method, which consists of the two-layer model. On the top layer, blockchain nodes are present, and vehicles are attending on the ground

TABLE III
COMPARISON OF AI AND IOT-BASED APPROACHES WITH OUR WORK

Characteristics	IoT-based approach [23]	AI-based IoT approach [24]	Proposed Work
Privacy	Less	Less	High
bandwidth	Limited	Limited	High
Environment	Centralized	Centralized	Decentralized
Resources	Restricted	Restricted	Consuming
Availability	Can't access data if server node is crashed	Can't access data if server node is crashed	High
Scalability	Considering the large number of devices	Considering the large number of devices	Poor with larger networks
Security	Less	Less	High
Fault tolerance	Doesn't support	Doesn't support	Support
Immutability	No	No	Yes
Interoperability	Medium	Medium	High
Anonymity	Less	Less	High
Confidentiality	Less	Less	High
Reliability	Data can be tempered	Data can be tempered	Data is tamper-proof.
Authenticity	No	No	Yes
Transparency	No	No	Yes
Energy Consumption	Least/Medium	Optimum	High
Information Sharing	Data monitoring and processing	Data processing	Peer-to-Peer data sharing
Automated Decision-making protocol	No	No	Yes
Access control	Medium	Medium	High

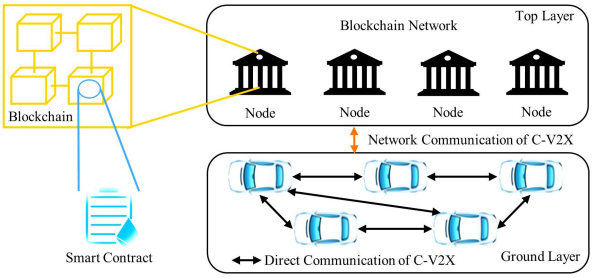

Fig. 1. System model of the BVCS.

layer. Two layers are connected using the network connection mode of C-V2X. More than one node can be chosen as an authenticated node. The authenticated node(s) are responsible for controlling the blockchain application, deploying smart contracts, and vehicle registration. It assumes that registered vehicles can only take part in the blockchain network. Each vehicle should have a tamper-proof device for storing communication data securely. In addition, vehicles are equipped with a C-V2X-supported onboard unit called Connectivity Control Unit (CCU). Only authenticated vehicles are allowed to interact with each other. The Authentication of users and vehicles is an automated process and is done by using smart contracts automatically. The BVCS can help to obtain an authentication-based information-sharing mechanism. The proposed system is divided into four stages: the initial stage, the registration stage, the authentication stage, and the communication stage.

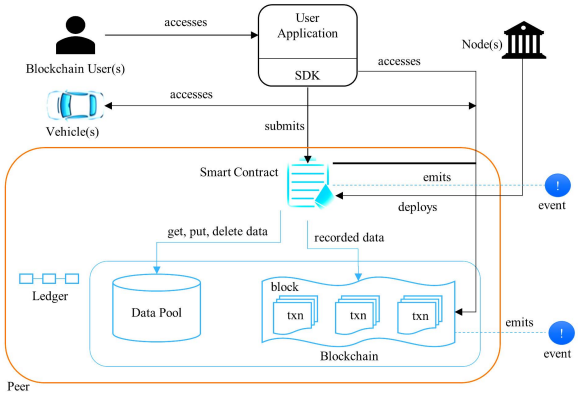

Fig. 2. Interaction between various entities of the BVCS.

A. Initial Stage

In the BVCS, various entities are introduced: user, vehicle, blockchain node, and smart contract. The interaction between these entities is shown in Fig. 2, in which each of them has an important role. A user provides the required credentials while buying a vehicle. An authorized node is responsible for collecting the user credentials. An authenticated blockchain node verifies the user data and then provides the vehicle's data, such as vehicle number, engine number, and chassis number. Given data will be stored in the blockchain data pool by the corresponding node. The user can verify the data through the user application to ensure that the correct data is stored or not. After user confirmation, the minor node puts the data in the blockchain. In such a way, the appropriate data will be stored in the blockchain. The authentication of the user will be performed by the smart contracts automatically. A blockchain node deploys smart contracts to the blockchain. The vehicle of the corresponding user can access the data after being authenticated by the smart contracts. Each transmitted data in V2V communication will be verified automatically using smart contracts and stored on the blockchain.

B. Registration Stage

An identification key is essential for identifying a vehicle and the vehicle's user. Thus, a unique Id (UI) is introduced to identify a vehicle and the vehicle's user. A UI should be unique and is only accessible by the application only. The UI is a hash value generated by smart contracts using the user blockchain account address. The blockchain account address is needed to identify the particular vehicle and the user. A UI uniquely can specify a vehicle number and a user license number with the vehicle chassis number, the engine number, and the user information. UI will be generated by applying the SHA-512 hash generation function [30]. It is an efficient algorithm to guarantee data integrity as it always returns the identical output for the corresponding assigned input value. It is also a modern cryptographic hash generation function and is considered highly secure [31]. Thus, a UI always contains the same hash value, and it will be unique. The UI generation process is shown in "equation (1),". In the BVCS scheme, the user can obtain multiple UIs for using more than one vehicle. The user can get a UI after login into the application. Therefore, the UI will be saved to the blockchain for future

TABLE IV
USEFUL NOTATIONS AND DEFINITIONS

Notation	Description
Vx, Vy	Vehicle x, Vehicle y
Ux, Uy	The user of Vx, Vy
UIx, UIy	Unique Id of Vx, Vy
BACx	Blockchain account address of Ux of Vx
ULx	The license number of Ux of Vx
VEx	Engine number of Vx
VCx	Chassis number of Vx
VNx	Vehicle number of Vx
||	Concatenated with
H	Hash
T	Time Stamp

verification of vehicles and users. In such a way, the vehicle will be registered completely. Table IV shows some notations used in this work.

C. Authentication Stage

A vehicle can only communicate after it will be verified. The communication process will be available and activated from the user application through smart contracts. Thus, user authentication is more important. Vehicle authentication is also much more needed to establish secure communication between vehicles. The authentication process of the user and vehicle is described in the following:

1) User Authentication: A 2-step authentication scheme (2-SAS) is designed for the authentication of a genuine user. In the 1st step, the user can log in using the received login credentials at the time of registration. In the 2nd step, the user has to set a token called user token (UT) that is permanent and changeable if required. This token will be stored in the blockchain, and it is an alphanumeric value. At the same time, the smart contract creates a random token (RT) for the user. This token is a hash value generated using the SHA-

$$UIx = H(BACx \parallel ULx \parallel VEx \parallel VCx \parallel VNx) \quad (1)$$

512 as shown in "equation (2),".

$$RTx = H(BACx \parallel ULx \parallel T \parallel VNx) \quad (2)$$

where RTx is the random token of Ux. It will be different and unique for each login session. Therefore, the user has to provide the correct UTx (UT of Ux) and RTx to the application for becoming authenticated. In such a way, 2-SAS can validate a user automatically. The workflow diagram of the 2-SAS for user Ux is shown in Fig. 3.

2) Vehicle Authentication and Unauthorized Access Detection: Once the user successfully becomes authenticated, he can operate the vehicle. The user can manage all vehicle functions (i.e., activate vehicle authentication and communication features, add driver data, and driver verification) from the application interface. A vehicle's data (i.e., registered or unregistered vehicle, the vehicle user authenticated or not) should be verified before it runs on the road. Vehicle authentication will be done by the application using smart contracts automatically. This event will be triggered after getting a request for running the vehicle from the user. He should provide the UTx and RTx to the application for authentication. If the user provides the correct credentials, he will be authenticated successfully. Therefore, he will give the UIx for vehicle authentication. The smart contract checks the given UIx with the stored UIx of the vehicle. In this way, the vehicle will be validated. If the

Algorithm 1 User Authentication (2-SAS)

Input: UTx, RTx
Output: successful or unsuccessful authentication

```
Ux logged in using the user Id and password;
if (Ux is valid) then
    1st step authentication of Ux is completed;
    if (UTx is not available) then
        Ux sets the UTx // it will be saved to the
        blockchain;
    end
    else
        do not need to set the UTx;
    end
    for (each login session) do
        Smart contact generates a RTx and sends it to Ux;
        Ux provides the UTx, RTx to the application;
        while (UTx == true && RTx == true) do
            Ux is authenticated successfully // 2nd step
            authentication is completed;
        end
    end
end
else
    if (Ux is registered) then
        provides the correct user Id and password;
    end
    else
        do the registration;
    end
end
```

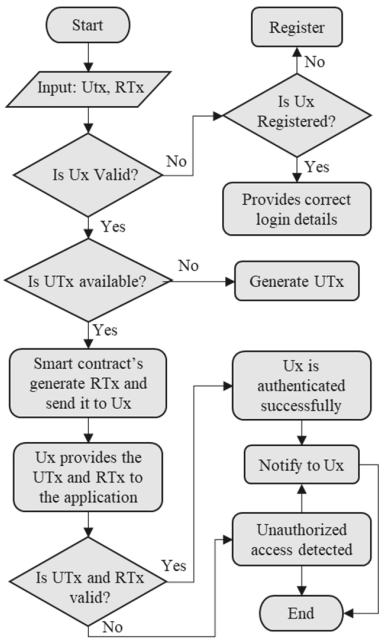

Fig. 3. Workflow diagram of the 2-SAS (user authentication process).

Algorithm 2 Vehicle Authentication and Unauthorized Access Detection

Input: UTx, RTx, UIx
Output: Unauthorized access detection;
Ux logged in using the user Id and password;
if (Ux is registered) **then**
  The application asks to provide UTx and RTx;
  if (UTx == true && RTx == true) **then**
    Ux is authenticated;
    if (UIx == true) **then** // smart contract checks the given UIx by Ux with the stored UIx in the vehicle device;
      Vx is authenticated;
    end
  end
  else
    Ux isn't authenticated;
    unauthorized access is detected and notified to Ux;
  end
end

Algorithm 3 Communication Establishment Between Vx and Vy

Input: UIx, UIy
Output: SKx, SKy
After the successful authentication of Ux and Uy;
The application creates SKx and SKy;
if (UIx is valid) **then**
  SKx is stored in the vehicle device of Vx;
  Vx sends SKx to Vy;
  Vy sends back it to smart contracts;
  if (SKx is true) **then** // smart contract checks SKx with the stored SKx in the blockchain;
    Vx is validated;
    Vy ensures that Vx is authenticated;
  end
end
if (UIy is valid) **then** //this instruction will be executed while the instruction of line no. 3 will be executed;
  SKy is stored in the vehicle device of Vy;
  Vy sends it to Vx;
  Vx sends back it to smart contracts;
  if (SKy is true) **then** // smart contract checks SKy with the stored SKy in the blockchain;
    Vy is validated;
    Vx ensures that Vy is authenticated;
    Now, secure communication is established between Vx and Vy;
  end
end

validation of the vehicle is failed, it means unauthorized access is detected. Finally, an unauthorized accesses detection message will be delivered to the user and the concerned authority.

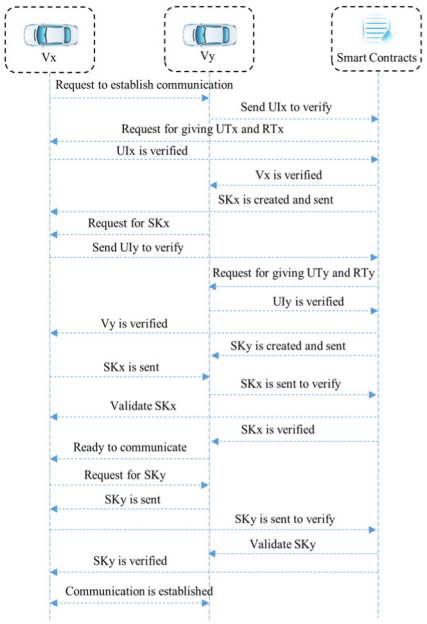

Fig. 4. Sequential diagram of the interaction between two vehicles and smart contracts for establishing secure communication.

D. Communication Stage

After the completion of the user and vehicle authentication, the vehicle can share information. For V2V communication, vehicles use their secret key created using SHA-512 because of its faster execution. They store their key in their tamper-proof device. They can communicate securely with each other using their secret key. The secret key will be generated using smart contracts, as shown in "equation (3),".

$$SKx = H(UIx \parallel RTx \parallel VNx \parallel T) \tag{3}$$

V2V Communication: Secure V2V communication between vehicles is proposed for the intelligent transport system to achieve efficient and secure communication using blockchain and more high-speed and secure communication technology like C-V2X. Here, vehicles should be validated before establishing communication with other vehicles. C-V2X is a platform that integrates with the LTE-V2X PC5 interface for short-range and network-less V2V communications. The communication process between Vx and Vy is presented in "Algorithm (3)". However, user and vehicle authentication of Vx and Vy is required before establishing secure communication. So, secure communication will be established between Vx and Vy. Fig. 4 shows the sequential interaction between two vehicles and smart contracts for establishing secure communication. Smart contracts verify users and vehicles to achieve the trustworthiness of the communication system. However, the communication data should be verified by smart contracts, and then data will be shared between Vx and Vy. Thus, encrypted [31] data will be shared for achieving data security. Vx encrypts data with SKx and sends the encrypted data for decryption to Vy. In such a way, Vy also encrypts data with SKy and sends the encrypted data for decryption to Vx. The encryption method of a secret key is not like symmetric encryption. But in our proposed work, a session-wise secret key is used to establish secure communication and

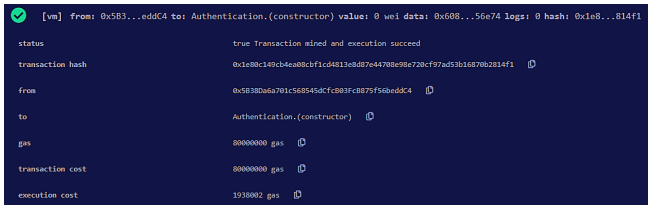

Fig. 5. The smart contract is deployed successfully.

to share data between vehicles. A secret key is different for each vehicle in each session. Thus, while a communication process will be initiated, the secret key will be generated by the smart contract and shared with the corresponding vehicle. For example, SKx will be shared with Vy, and Sky will be shared with Vx. The data is sent by Vx as $Data_{Vx} = UIx \parallel T \parallel Message$. Vx signs the data using SKx and sends it to Vy, where $Signed_{Vx}\ (Data_{Vx}) = E_{Vx}\ (H(Data_{Vx}))$. Vy received the message and will verify the signature, the generated hash, and the data components (i.e., UIx, SKx) with the received information from smart contracts. Vy will decrypt the message using the SKx and access data. Another side, Vy will send back the data as per the request of Vx if required. In this way, secure communication will be established, and data will be shared securely between Vx and Vy.

V. Testing Results

In the BVCS, three algorithms are developed to authenticate the user and vehicle and establish secure communication. These algorithms are implemented using smart contracts. The code is written in solidity language through a web-based platform named Ethereum Remix IDE (v0.24.1) [32]. Smart contract codes can implement and run on the Ethereum Virtual Machine (EVM). The solidity compiler version is 0.8.7, and the EVM version is assigned to the compiler default. JavaScript VM (v4.2.0) environment is selected for deploying and executing codes. The input data (*BAC: 0x5. 38Da6a701c568545dCfcB03FcB875f56beddC4, UL: BP2134, VE: ABCD123, VC: 3456MH4, VN: IN0009U, and UT: ABCD1234*) is chosen randomly for only testing purposes. The output data will be created using those input values through the smart contract. The UI, RT, and SK are generated using "equations (1), (2), and (3)," respectively. The smart contract executes these parameters using the keccak256 cryptographic hash function [33] as it is used in Ethereum. Fig. 5 shows that the smart contract's code is compiled, run, and executed successfully from account address "0x5. 38Da6a701c568545dCfcB03FcB875f56beddC4". This address is considered a user BAC. All implemented scenarios are tested using this address. Herein, the user stores his credentials and vehicle-related data from this address. Fig. 6 shows that the user stores required data using the *SetData* () function, similar to a registration scenario. Fig. 7 shows that the user or vehicle of BAC: "0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c" is not registered.

A. User Authentication

After logging in to the application, the user has to a UT using the *SetUserToken()* function shown in Fig. 8. Therefore,

Fig. 6. User and vehicle data is stored successfully.

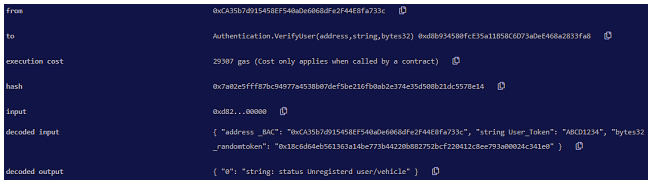

Fig. 7. The vehicle is not registered.

Fig. 8. UT is set successfully by the user of the BAC.

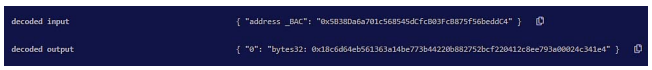

Fig. 9. RT is created successfully for the user.

Fig. 10. The user is authenticated successfully.

Fig. 11. The user cannot be authenticated by providing the wrong token.

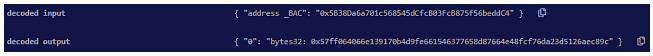

Fig. 12. UI is created successfully for the user.

the user calls the *GenerateRandomToken* () function to get the RT recording in Fig. 9. Now, the user has both token UT and RT to authenticate himself. The user provides these tokens and is authenticated successfully using the *VerifyUser()* function shown in Fig. 10. If any of these provided tokens is wrong, as shown in Fig. 11, authentication will be rejected.

B. Vehicle Authentication

The smart contract generates a UI for the user using the *UIgenerator()* function shown in Fig. 12. The UI will be stored in the vehicle device for communication purposes. Before establishing V2V communication, the smart contract verifies that the UI is associated with an authenticated user. So, the vehicle is validated using the *VerifyVehicle()* function shown in Fig. 13. Fig. 14 shows that the vehicle is not authenticated for giving false data, and unauthorized access is detected.

C. Secure Communication Establishment

Therefore, the vehicle will be eligible to establish V2V communication. Each vehicle has the SK using *GenerateSecretKey()* function shown, in Fig. 15. The vehicle can

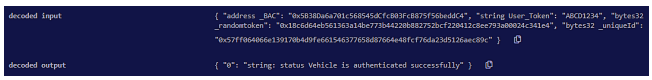

Fig. 13. The vehicle is authenticated successfully.

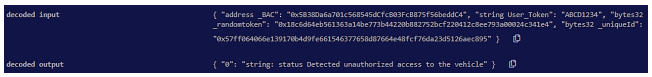

Fig. 14. Unauthorized access detection to the vehicle.

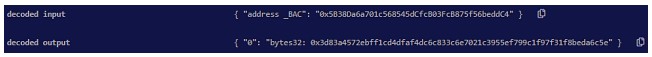

Fig. 15. A secret key is generated for the user.

Fig. 16. Data is sent from BAC: 0xAb8483F64d9C6d1EcF9b849Ae677dD 3315835cb2.

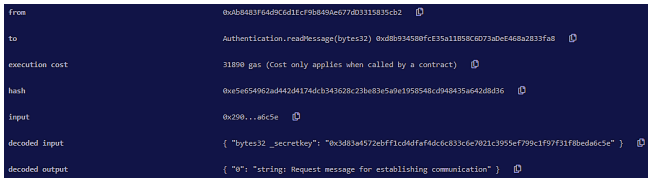

Fig. 17. The message is read by the recipient using the secret key of the sender.

send messages to other vehicles after establishing successful communication. The sent messages only can be read by those recipients who have SK of the sender vehicle. As shown in Fig. 16, a vehicle sends a message from address 0x5.38Da6a701c568545dCfcB03FcB875f56beddC4 to address *0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2* of another vehicle. The recipient has accessed the message after providing the right SK of the sender vehicle shown in Fig. 17.

VI. Performance Analysis of the BVCS System

Data security has been a top priority for organizations in recent years, and they're looking for new ways to protect their data. Recently, blockchain technology has emerged as one of the most creative options for securing data exchange. Hashing and digital signatures in blockchain bring to the forefront through the application of cryptography because both these play a significant role in the blockchain environment. In this paper, the BVCS is presented for securing the transmitted data while exchanging it between vehicles and establishing a trusted environment for V2V communication. A comparative analysis of the BVCS with other methods is provided in Table V.

A. User Privacy

In traditional V2V communication systems, user data is stored in a centralized environment. A single node is responsible for making changes in data. So, data manipulation can be possible here. A secure and transparent database is required to increase user privacy. Blockchain can provide a decentralized, transparent, and privacy-preserving environment. In this paper, a V2V communication system, the BVCS, is designed using blockchain for its intrinsic features. User data cannot be compromised using the BVCS application. "Algorithm (1)" shows how smart contracts authenticate users automatically. Herein, users are authenticated without sharing data with third parties. Unauthorized access can be detected by introducing the token generation policy for verifying genuine users. Thus, the BVCS can keep user data secure and enhance user privacy.

TABLE V
Performance Comparison of the BVCS With Other Existing Methods

Characteristics	Methods and Technologies				
	[18]	[22]	[25]	[26]	BVCS
Privacy	√	√	√	√	√
Confidentiality	√	√	×	×	√
Access Control	×	×	×	×	√
Anonymity	√	√	√	√	√
Integrity	√	×	√	√	√
Mobility	√	×	√	√	√
Freshness	√	×	√	√	√
Data Authenticity	√	√	×	×	√
Vehicle Authentication	√	×	×	×	√
Vehicle Security	×	×	×	×	√
Key Management	√	×	×	×	√
Unauthorized Access Detection	×	×	×	×	√

B. Data Security

The importance of data security is essential for accessing and analyzing the correct data. Data security is crucial for different reasons in private and public organizations. The main elements of data security are confidentiality, availability, and integrity. Data integrity ensures that data will be stored securely and reliably. Data availability ensures that data always be accessed safely. Using precise data security measures can prevent data hacks and reduce risk. In the BVCS system, blockchain data cannot be accessed and modified by malicious nodes. Since smart contracts authenticate vehicles before establishing communication, data cannot be shared with unauthorized vehicles. Data security is provided in the BVCS system using a hashing algorithm (SHA512) and a digital signature (by creating a secret key). The hashing algorithm is used to protect data from cyber-attacks. The secret key is introduced for securing the transmitted data between the sender and receiver nodes. So, data will be secured in the BVCS system.

C. Vehicle Security

In the V2V communication system, vehicle security is essential to communicate with each other. Vehicles should be verified for establishing communication securely with each other. At the same time, users should be authenticated before establishing communication to enable V2V communication. In the BVCS system, vehicles will be validated automatically using smart contracts. Smart contacts verify the stored

data in vehicles before establishing communication. Vehicle data will be shared through the network communication of C-V2X technology. "Algorithm (2)" shows the full details of the verification of genuine users and the detection of any unauthorized access. So, vehicle theft is not possible here. Vehicle data will be validated and shared in encrypted mode at the time of transferring data with each other. A secret key is introduced here to encrypt data. Thus, data cannot be accessed by others except recipients. Smart contracts are responsible for validating the secret key. "Algorithm (3)" shows the full details of the vehicles' verification process to establish secure communication. So, data can be shared among vehicles after secret key verification in a secure way. Therefore, data security of vehicles can be achieved in the BVCS system.

D. Platform Security

A decentralized platform is more reliable and cost-effective than a centralized-based platform in vehicular communications. A single node is responsible for maintenance in a centralized system. The whole system will be a failure if the central node is crashed. Herein, blockchain is combined with C-V2X technology for realizing a secure V2V communication system. As it is a decentralized system, no communication system will be broken by crashing or disconnecting a single node. Blockchain is a secure platform to develop and manage applications in which multiple nodes can share and track information without involving intermediaries. Every connected node in the blockchain is verified before joining the network. Thus, the BVCS system can provide a decentralized, transparent, and secure platform for sharing information.

E. Communication Security and Privacy

Data stored in-vehicle devices would also be secured with a secure communication system. Blockchain data is always verifiable and cannot be altered. So, verified data can be shared between vehicles and can be secured with transparent transactions using Blockchain in the V2V communication system. Today, blockchain is a secure technology for its intrinsic characteristics. Data stored in the blockchain is safe and protected using cryptography. Encryption and decryption methods are used to protect communicated data from unauthorized access. Data can be shared among vehicles after secret key verification in a secure way. Thus, communication data will be secured in this system. Thus, the BVCS system can provide a secure communication interface.

F. Limitations of the Proposed System

The proposed work has some minor limitations that are described in the following:

–First, Unregistered vehicles cannot access the benefits of the proposed system. In this paper, no policy has been mentioned for unregistered vehicles.

–Second, the generation of UI, SK, and RT is automated and given to users after 1st step authentication. Users must have to remember the UT for getting UI, SK, and RT. If a user cannot remember his UT, it is not possible to get that key immediately to access his vehicle.

–Third, no penalty scheme has been discussed for unregistered vehicles.

VII. Conclusion

A secure V2V communication platform is essential to safeguard the processing and sharing of data without hampering the data. In this paper, the challenges of V2V communication are provided. The BVCS is a blockchain-enabled secure communication system that can enhance vehicle security, data security, and user privacy and provide a secure decentralized, and trusted environment for V2V communication. The proposed algorithms ensure how the BVCS can improve the above-specifying concerns. Smart contracts eliminate the barrier of the key-based and trust-based authentication problems using proposed algorithms for users and vehicles. The BVCS is an identity-based, trust-based, and key-based solution for ensuring a safe and secure V2V communication system. The testing results and security analysis assures the realization of BVCS for secure V2V communication. The security requirements of a secure and trusted communication system are present in this proposed system. In the future, the BVCS will be extended and implemented with autonomous vehicles and intelligent transport systems. So, autonomous vehicles can recognize faster and achieve more security in vehicular communications with a more immediate data-sharing mechanism.

References

[1] A. Demba and D. P. F. Moller, "Vehicle-to-vehicle communication technology," in *Proc. IEEE Int. Conf. Electro/Inf. Technol. (EIT)*, May 2018, pp. 459–464, doi: 10.1109/EIT.2018.8500189.

[2] S. Ali, "Vehicle to vehicle communication," Netw. Mobile Robots Res., Tech. Univ. Dortmund, Dortmund, Germany, 2019, doi: 10.13140/RG.2.2.24951.88487.

[3] U. Ahmed, J. C.-W. Lin, and G. Srivastava, "Privacy-preserving deep reinforcement learning in vehicle ad hoc networks," *IEEE Consum. Electron. Mag.*, vol. 11, no. 6, pp. 41–48, Nov. 2022, doi: 10.1109/MCE.2021.3088408.

[4] Q. Hu and F. Luo, "Review of secure communication approaches for in-vehicle network," *Int. J. Automot. Technol.*, vol. 19, no. 5, pp. 879–894, Oct. 2018, doi: 10.1007/s12239-018-0085-1.

[5] J. M.-T. Wu, G. Srivastava, A. Jolfaei, M. Pirouz, and J. C.-W. Lin, "Security and privacy in shared HitLCPS using a GA-based multiple-threshold sanitization model," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 6, no. 1, pp. 16–25, Feb. 2022, doi: 10.1109/TETCI.2020.3032701.

[6] J. C. Lin, P. Fournier-Viger, L. Wu, W. Gan, Y. Djenouri, and J. Zhang, "PPSF: An open-source privacy-preserving and security mining framework," in *Proc. IEEE Int. Conf. Data Mining Workshops (ICDMW)*, Nov. 2018, pp. 1459–1463, doi: 10.1109/ICDMW.2018.00208.

[7] D. Das, S. Banerjee, and U. Biswas, "A secure vehicle theft detection framework using blockchain and smart contract," *Peer Peer Netw. Appl.*, vol. 14, no. 2, pp. 672–686, Mar. 2021, doi: 10.1007/s12083-020-01022-0.

[8] W. Wang et al., "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2018, doi: 10.1109/ACCESS.2019.2896108.

[9] A. Papathanassiou and A. Khoryaev, "Cellular V2X as the essential enabler of superior global connected transportation services," *IEEE Future Netw.*, vol. 1, no. 2, pp. 1–2, Jun. 2017.

[10] Z. Xu, X. Li, X. Zhao, M. H. Zhang, and Z. Wang, "DSRC versus 4G-LTE for connected vehicle applications: A study on field experiments of vehicular communication performance," *J. Adv. Transp.*, vol. 2017, pp. 1–10, Aug. 2017, Art. no. 2750452, doi: 10.1155/2017/2750452.

[11] V. Khairnar and S. Pradhan, "V2V communication survey wireless technology," *Int. J. Comput. Technol. Appl.*, vol. 3, pp. 1–4, Mar. 2014.

[12] D. Gettman. (2020). *DSRC and C-V2X: Similarities, Differences, and the Future of Connected Vehicles*. [Online]. Available: https://www.kimley-horn.com/dsrc-cv2x-comparison-future-connected-vehicles/

[13] A. Ruddle et al., "Deliverable D2. 3: Security requirements for automotive on-board networks based on dark-side scenarios," in *E-Safety Vehicle Intrusion Protected Applications*. Karlsruhe, Germany: Fraunhofer ISI, 2009.

[14] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Dec. 6, 2022. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[15] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Jun. 2017, pp. 557–564, doi: 10.1109/BigDataCongress.2017.85.

[16] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 49, no. 11, pp. 2266–2277, Nov. 2019, doi: 10.1109/TSMC.2019.2895123.

[17] D. Das, S. Banerjee, U. Ghosh, U. Biswas, and A. K. Bashir, "A decentralized vehicle anti-theft system using blockchain and smart contracts," *Peer Peer Netw. Appl.*, vol. 14, no. 5, pp. 2775–2788, Sep. 2021, doi: 10.1007/s12083-021-01097-3.

[18] J. Liu and Z. Liu, "A survey on security verification of blockchain smart contracts," *IEEE Access*, vol. 7, pp. 77894–77904, 2019, doi: 10.1109/ACCESS.2019.2921624.

[19] Endorphin. *Ethereum Virtual Machine (EVM)*. Accessed: Dec. 6, 2022. [Online]. Available: https://ethereum.org/en/developers/docs/evm/

[20] M. G. Solomon. Ethereum Smart Contracts: Tips for Handling Data in Solidity. Ethereum for Dummies. Accessed: Dec. 6, 2022. [Online]. Available: https://www.dummies.com/personal-finance/ethereum-smart-contracts-tips-for-handling-data-in-solidity/

[21] Minimalism. *Introduction to Smart Contracts*. Accessed: Dec. 6, 2022. [Online]. Available: https://ethereum.org/en/developers/docs/smart-contracts/

[22] Y. H. Kim and S. Peeta, "Graph-based modeling of information flow evolution and propagation under V2 V communications-based advanced traveler information systems," *Comput.-Aided Civil Infrastruct. Eng.*, vol. 31, no. 7, pp. 499–514, Jul. 2016, doi: 10.1111/mice.12188.

[23] D. N. Chowdhury, N. Agarwal, A. B. Laha, and A. Mukherjee, "A vehicle-to-vehicle communication system using IoT approach," in *Proc. 2nd Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA)*, Mar. 2018, pp. 915–919, doi: 10.1109/ICECA.2018.8474909.

[24] P. Goswami et al., "AI based energy efficient routing protocol for intelligent transportation system," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 2, pp. 1670–1679, Feb. 2022, doi: 10.1109/TITS.2021.3107527.

[25] M. Kamal, G. Srivastava, and M. Tariq, "Blockchain-based lightweight and secured V2 V communication in the internet of vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 3997–4004, Jul. 2021, doi: 10.1109/TITS.2020.3002462.

[26] R. Jabbar, M. Kharbeche, K. Al-Khalifa, M. Krichen, and K. Barkaoui, "Blockchain for the internet of vehicles: A decentralized IoT solution for vehicles communication using ethereum," *Sensors*, vol. 20, no. 14, 2020, p. 3928, doi: 10.3390/s20143928.

[27] M. Shing and S. Kim, "Blockchain based intelligent vehicle data sharing framework," 2017, *arXiv:1708.09721*, doi: 10.48550/ARXIV.1708.09721.

[28] A. Patel, N. Shah, T. Limbasiya, and D. Das, "VehicleChain: Blockchain-based vehicular data transmission scheme for smart city," in *Proc. IEEE Int. Conf. Syst., Man Cybern. (SMC)*, Oct. 2019, pp. 661–667, doi: 10.1109/SMC.2019.8914391.

[29] N. Malik, P. Nanda, A. Arora, X. He, and D. Puthal, "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 674–679, doi: 10.1109/TrustCom/BigDataSE.2018.00099.

[30] A. Sengupta and M. Rathor, "Security of functionally obfuscated DSP core against removal attack using SHA-512 based key encryption hardware," *IEEE Access*, vol. 7, pp. 4598–4610, 2019, doi: 10.1109/ACCESS.2018.2889224.

[31] J. Lake. (2019). *Understanding Cryptography's Role in Blockchains*. Accessed: Dec. 6, 2022. [Online]. Available: https://www.comparitech.com/crypto/cryptography-blockchain/

[32] Remix 0.18.0. *Remix Ethereum IDE*. Accessed: Dec. 6, 2022. [Online]. Available: https://remix.ethereum.org/

[33] H. Jameson. *Which Cryptographic Hash Function Does Ethereum Use?* Accessed: Dec. 6, 2022. [Online]. Available: https://ethereum.stackexchange.com/questions/550/which-cryptographic-hash-function-does-ethereum-use

Debashis Das received the B.Tech. degree in computer science and engineering from the Government College of Engineering and Leather Technology in 2015, the M.Tech. degree in computer science and engineering from Kalyani Government Engineering College in 2018, and the Ph.D. degree from Kalyani University. He is currently working as a University Research Scholar with Kalyani University. Currently, he is working on blockchain technology for ITS and its applications. His research interests include the Internet of Vehicles (IoV), distributed computing, cyber-physical systems, intelligent transportation systems (ITS), and blockchain technology.

Sourav Banerjee (Senior Member, IEEE) received the Ph.D. degree from the University of Kalyani in 2018. He is currently an Assistant Professor with the Department of Computer Science and Engineering, Kalyani Government Engineering College, Kalyani, West Bengal, India. He has authored numerous reputed journal articles, book chapters, and international conferences. His research interests include big data, cloud computing, cloud robotics, distributed computing, mobile communications, and the IoT. He is a Senior Member of ACM, IAE, and the MIR Laboratories. He is a SIG Member of the MIR Laboratory, USA. He is an Editorial Board Member of *Wireless Communication Technology*.

Pushpita Chatterjee (Senior Member, IEEE) received the Ph.D. degree from IIT Kharagpur, India. She is working with the Department of Electrical Engineering and Computer Science, Howard University, Washington, DC, USA. Her research interests include machine learning, smart health, wireless sensor networks, distributed and trust computing, software-defined networking, and information-centric networking.

Uttam Ghosh (Senior Member, IEEE) received the Ph.D. degree in electronics and electrical engineering from IIT Kharagpur, India, in 2013. He was an Assistant Professor at the Department of Computer Science, Vanderbilt University. He was a Post-Doctoral Researcher at the University of Illinois in Urbana–Champaign, Fordham University, and Tennessee State University. He is an Associate Professor of cybersecurity with the Department of Computer Science and Data Science, Meharry Medical College (MMC), Nashville, TN, USA. His main research interests include cybersecurity, computer networks, wireless networks, machine learning, health informatics, and software-defined networking. He is a member of Sigma Xi and ACM.

Utpal Biswas received the B.E., M.E., and Ph.D. degrees in computer science and engineering from Jadavpur University, India, in 1993, 2001, and 2008, respectively. He was a Faculty Member at the Department of Computer Science and Engineering NIT, Durgapur, India, from 1994 to 2001. Currently, he is working as a Professor with the Department of Computer Science and Engineering, University of Kalyani, West Bengal, India. He has over 130 research articles in different journals, book chapters, and conferences. His research interests include optical communication, ad-hoc and mobile communication, semantic web services, e-Governance, and cloud computing.