Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 7357820, 13 pages
https://doi.org/10.1155/2022/7357820

Research Article

Blockchain-Based Trust Verification and Streaming Service Awareness for Big Data-Driven 5G and Beyond Vehicle-to-Everything (V2X) Communication

Iftikhar Rasheed,[1] **Muhammad Asif**,[2] **Wali Ullah Khan**,[3] **Asim Ihsan**,[4] **Kalim Ullah**,[5] **and Md. Sadek Ali**[6]

[1]*Department of Information and Communication Engineering, The Islamia University of Bahawalpur, Pakistan*
[2]*Guangdong Key Laboratory of Intelligent Information Processing, College of Electronics and Information Engineering, Shenzhen University, Shenzhen, Guangdong 518060, China*
[3]*Interdisciplinary Center for Security, Reliability and Trust (SnT), University of Luxembourg, 1855 Luxembourg City, Luxembourg*
[4]*Department of Information and Communication Engineering, Shanghai Jiao Tong University, Shanghai 200240, China*
[5]*Department of Electrical Engineering, University of Science and Technology Bannu, Khyber Pakhtunkhwa, Pakistan*
[6]*Communication Research Laboratory, Department of Information and Communication Technology, Islamic University, Kushtia-7003, Bangladesh*

Correspondence should be addressed to Md. Sadek Ali; sadek@ice.iu.ac.bd

Received 4 January 2022; Revised 4 February 2022; Accepted 11 March 2022; Published 1 April 2022

Academic Editor: Alessandro Bazzi

Vigorous security and transparency with minimum latency and a high data rate are some of the key requirements for 5G and beyond vehicular networks especially in case of big data-driven vehicle-to-everything (V2X) communication applications which plays an important role in enabling advance intelligent transportation systems (ITS) and Internet of Vehicle (IoV) based network. The trace-ability in blockchain makes it one of the vital options, back-boned by the decentralized network to ensure independent security and privacy by exploiting the hash of a previous transaction with the time stamp and announcing it publicly for rejection of possible adversary attack. Therefore, in this work, we have opted for blockchains for trusted authentication and service awareness in 5G and beyond vehicle-to-everything (V2X) communication-based vehicular networks to stream blocks by certifying privacy and security. Here, we have considered blockchain as intermediary trusted agent to witness communication between a vehicle node and edge node, where edge node also uploads microservices along with calling figure of microservices to the blockchain. Furthermore, to ensure vehicle privacy with joint verification of vehicular network and server, we have devised a mechanism in which every vehicle nodes anonymously ask for services from the edge server along with signing an individual's identity. Moreover, based on generated vehicle requests and service awareness, we devised an improved edge cache scheme for the prior compilation of services at each edge. In comparison to the previous state-of-art work, the result shows that our proposed work handles the requests more efficiently to achieve a better service request cache hit rate generated by vehicles at the edge server.

1. Introduction

The existing communication technologies like multiple input-multiple output (MIMO), channel coding, cooperative communication, and Internet of Vehicles (IoV) have played an important role towards the development of upcoming next-generation communication systems [1–8]. Furthermore, wireless communication is one of few domains where major developments have been observed within the last few decades. Hence, literature in this domain anticipates channel models to elicit higher data rates at each wireless node. The development of 1stG to 5thG wireless standards is the

practical example of theoretical proposals; subsequently, current research has now entered in formulating theoretical phase of 6th generation network [9].

Besides higher data rate for supporting various advance communication applications like IoT (Internet of Things) to the Internet of Everything, especially vehicle-to-everything (V2X) communication applications the reliability, robustness, security, privacy, and big data, are some of the essential requirements needed to support diverse utilities for the increasing number of wireless nodes [10]. As a forthcoming communication protocol, 5thG and beyond presume to be indefectible in communication, processing, targeting more industrial solutions, smart cities, and autonomous transport structure like ITS [11, 12]. Moreover, the concept of autonomous vehicles connected through 5G links will be using multiple gigabytes (GB) of data per second, which means big data analysis incorporated with 5G V2X will play an important role in Intelligent transport systems (ITS) [13].

The intelligent transport systems (ITS) are an emerging area of research. Hence, for accuracy and robustness, all vehicles within the network are interconnected with each other and mobile devices for communication to avoid a collision, this type of network intend for safe, efficient, and environment-friendly transportation, thus, in all of these applications, the V2X communication plays a vital role in realizing the concept of ITS. Therefore, usually intelligent transportation can be discerned as parallel management of vehicle and cloud edge, which requires connected sensors and cameras to work jointly with mobile edge computing for attaining accuracy and efficiency [14, 15]. Here in these scenarios acquired and computed data transmitted using block-streams and on-demand request handling mode [16], this technique helps to avoid downloading the full application from the play store rather it uses the concept of splitting the application into microservices.

Second, the operating system (OS) or program is loaded into the program memory of 5G-enabled vehicle through block-streaming only on receiving client service or resource requests [17]. Therefore, block streams have several advantages in mobile edge computing especially in 5G-V2X network but with a limited number of resources [18].

Due to the availability of a high data rate in 5G, a new race has been evolved in 5G-V2X communication applications. Hence, the 5th generation and beyond standard targets to achieve high-speed communication link with least latency, due to which high precision and accuracy in the vehicular network for intelligent transportation can be achieved [19]. But in parallel security and privacy-related concerns limit full industrial implementations of such schemes. Thus, for building a strong cooperative interconnected network, new techniques like cloud computing, mobile crowdsensing, edge computing, big data, and artificial intelligence have a vital role. Subsequently, we can infer that handling confidentiality and security is a key challenge in the edge network, which comprises the diverse range of edge nodes performing edge computing on data roaming among all possible edges.

Furthermore, while considering 5G and beyond V2X communication applications, the major privacy and security exposures are caused by authentication protocols, isolation configurations, network protocols, and switching mechanisms. Consequently, the characteristics of decentralization, trace-ability, and nontempering, we have opted for blockchain and hashing mechanisms improved with blind signature to address security and privacy issues of the overall network. Also, it is assumed that melding blockchain with 5G and beyond applications provides more reliable, secure, and efficient collaboration for the vehicular network [20].

Concurrently, with the rise in wireless traffic and networks, mobile utilities supported by wireless standards are also soaring heterogeneously. Therefore, efficient usage of limited resources like bandwidth, processing power, and spectrum is also necessary. Thus, to curb this issue for edge computing, efficient transmission, and achieving minimum latency from vehicle to server, [21] proposed the idea of introducing cache at mobile edge network for each mobile base station.

In this proposed work, we put forward the idea of a 5G and beyond V2X communication through improved block-streaming service enabled through trusted authentication for 5G and beyond vehicular networks. Due to the decentralization and hashing characteristics, we entailed blockchain as an intermediary agent between an edge node and vehicle for authentication. Due to the feature of strong deterrence against any attack, we exploited hashing mechanism for recording node's interaction into the chain. Moreover, we utilized an improvised message-digest (MD-5) encryption algorithm with digital signatures from a blockchain network to devise an effective verification scheme at the node level. Such that on receiving a microservice, any vehicle will first validate its security and legality following a fact that hashed information is traceable and immutable to avoid data tampering during the interaction.

Other than that, to ensure the individual's identity, privacy, and full-duplex verification during the interaction between edges and connected vehicles, we entailed blind signatures of each vehicle as a primary key to devise a security mechanism for vehicle forming V2X communication network and requesting services from edge nodes in incognito mode. Moreover, we also allocated cache for each edge node depending upon the request initiated by a vehicle, and to enhance cache hit rate by each vehicle over the edge server, we also formulated a service awareness mechanism.

1.1. Research Contributions. Our main contributions are defined as follows:

(1) Initially, for streaming data in the 5G and beyond V2X communication network to support mobile edge computing, we projected the idea of blockchain to act as an intermediate trusted body for authenticating communication between vehicle node and service provider and to eliminate chances of data tampering. Consequently, for reliable and verified communication and microservice handling between both ends, every communication is recorded and authenticated by blockchain

(2) Second, for minimizing latency and maximizing the throughput of the system, we designed a separate cache mechanism at each node dedicated for computation, whereas the size of the cache depends upon requests generated by individuals vehicles

(3) Our third contribution is realizing secure, reliable, and full-duplex verification between every 5G-enabled vehicle member and edge node by exploiting identity-dependent blind signature scheme such that each vehicle requests desired service from the edge server in hidden mode

(4) At last, we analyzed our method by taking security and performance as key performance indicators (KPI) by evaluating the efficiency and other constraints from other available literature and comparing the achieved results with previous state-of-art works

2. Related Works

In the related work section, we inculcate the prerequisites required to understand our proposed work.

2.1. Block Streaming as Service Loading Model for 5G-Beyond V2X Communication. The basic idea behind the implementation of block streaming as a service (BSaaS) provider is to decorrelate storage from operations and software from nodes. Also, the incurred computations are fetched and stored to "unconsciously, usercontrollable" private services aided by cached operation supported by streaming [22]. Which further allows decimated applications to triangulate from cloud to edge, vehicular equipment, and vice versa [23]. In general, due to the restrictions in equipment's resources, the vehicle nodes do not support storage capability for whole or multiple applications.

However, one possible solution is decimating applications for the number of available blocks such that on need each vehicle node can request a flexible number of application chunks to facilitate number of vehicles. Furthermore, on the server side, there are some microservices along with applications that are in the execution phase, thus, there is no need to waste network bandwidth for maintenance purposes. Subsequently, on requesting a new application or service from the vehicle node, the edge server will complete block streaming and application segmentation execution from server proxy block-streaming execution platform (BSEP) by transmitting service code and relevant data [24].

Figure 1 illustrates the communication model of BSaaS. In case, when edge node seeks service from the cloud via the network, it means the request generated for service is from a nonedge node. Consequently, the vehicle node is facilitated by connected service. Afterward, the cache of an edge is flushed to facilitate services queued in the 5G network [25].

Lemma 1. *Let us define loading delay by L_D for BSaaS in the following expression incurred at both parts of download and execution.*

$$L_D = \frac{B_x}{CSI(t)} + \frac{I_{NS}(x)}{N_I}. \tag{1}$$

Lemma 2. *For energy compaction in BSaaS, we represent it as by ε for operating on block stream loading process.*

$$\varepsilon = \frac{B_x}{CSI(t)} * \varepsilon_l + \frac{I_{NS}(x)}{N_I} * \varepsilon_e. \tag{2}$$

In the above two expressions, we symbolized the number of chunks by x, represented channel state information for each slot "t" is given by CSI (t). We assumed two energy compaction variables one for download ε_l and other for execution ε_e. Furthermore, we represent the number of instructions executed by IoT machine in one second as N_I. Subsequently, we defined the size of xth block by B_x and $I_{\mathrm{NS}}(x)$ for instructions entailed in each block. Whereas time required to process x blocks is computed by $I_{\mathrm{NS}}(x)$/NI [26].

2.2. Blockchain Choice Parameters. Blockchain was previously introduced to record documents and linking them. However, [27] was the first to include blockchain for recording transactions through hashing mechanism. Intuitively, it is clear from the name that it is a chain of data inside blocks connected in chronological order such that each next block is pointing to the hash of previous block. Furthermore, within the network whenever any node solves the puzzle, it publicly announces the solution such that everyone within the network updates themselves. Hashing mechanism in blockchain is due to the SHA-256 algorithm which is nonreversible which makes it nontampering and vigilant to any adversary attack. Furthermore, [27] describes that short agreements in blockchain can autonomously process conditions defined in the program.

SHA256 is generally employed in the hash function, therefore, hashing in blockchain is the only mean of ensuring security, authentication and joins the chain of block such that each next block has hash of previous block. A hash function takes an input of any length and generates a hash of fixed length for example if the input text is a string of ten characters or a book having the size of 100 MB both have hash of similar length. Second, this generated hash is irreversible but whenever the system processes the same input, a similar hash will be generated but from the output, no one can guess what was at the input. In general, SHA256 is used for forming blocks and RIPEMD160 and others for assigning addresses. Hence, both functions of SHA256 algorithms in blockchain hashes input messages of variable length and generates output string of fixed size, i.e., 256-bit binary string for storage. We can realize SHA256 as blockhash function which takes input the hash of previous block for example Blockhash = SHA256 (block.header). Similarly, each successor block header has a pointer pointing to the hash of previous block. Consequently, any alteration in the current block or in previous block will cause the update in hash.

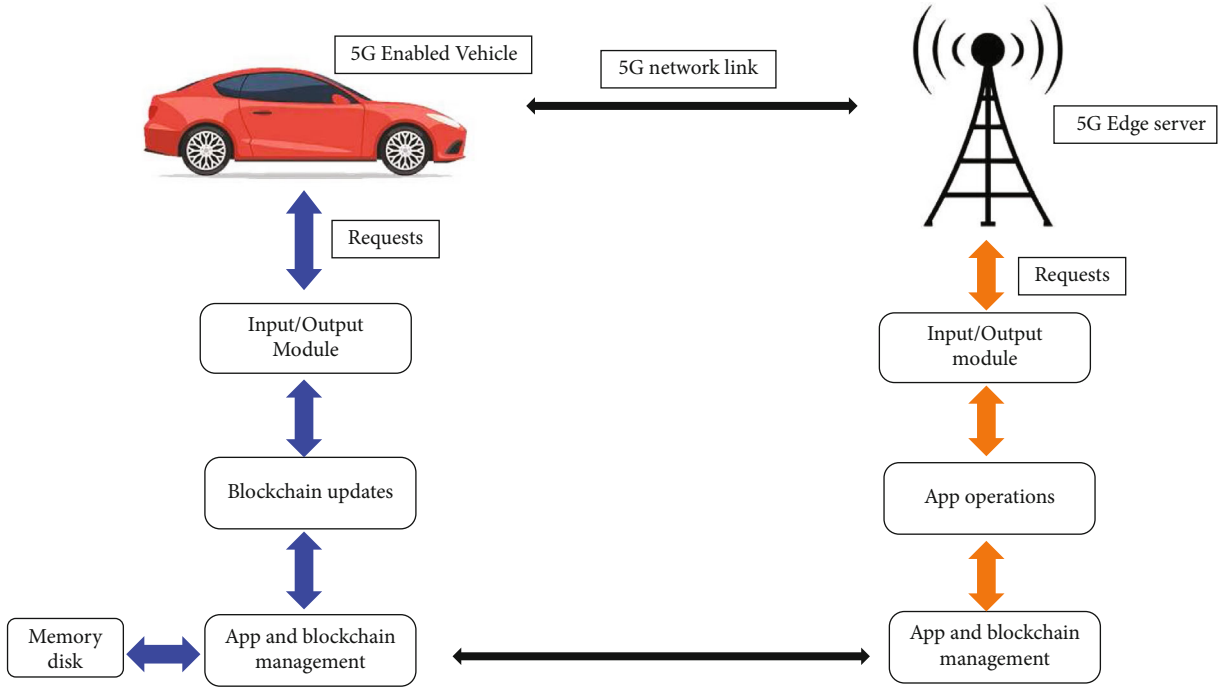

Figure 1: Blockchain communication model for BSaaS.

Mathematically, we can write it as

$$\begin{aligned}&\text{SHA256(Pre\_BLOCKHASH + BLOCK.BODY + Other)}\\&\quad = \text{SHA256(block.header)}\\&\quad = \text{BLOCKHASH.}\end{aligned} \tag{3}$$

As we mentioned earlier, major application of blockchain was in recording ledger, such that Hyperledger Fabric [28, 29]. However, FISCO BCOS has a project utilizing blockchain in financial applications. Furthermore, Ethereum utilizing blockchain has many complexities, which were mitigated by FISCO BCOS while retaining the main function of blockchain. But FISCO BCOS's main intention was to explore financial applications only which are a very limited scope of application. Unlike, Hyperledger Fabric which is different from public blockchain-like bitcoin (BTC) and Ethereum (ETH). That is the reason before joining the network, each public node is verified and validated, which consequently bypass the processing and energy overhead brought by proof of work (PoW) which is one of the main requirement for an energy-efficient and high-performance proposal. Meanwhile, Hyperledger Fabric opts a function-wise approach that separates every module from others like a consensus, block submission, authentication, and endorsement module.

Furthermore, the authentication function has a cryptographic mixed algorithm (X.509 merged with Asymmetric encryption), which is a zero-knowledge proof function. Therefore, users do not need to show their identities or any personal information to proceed further [30]. Hence, in our proposal, we selected a ledger structure designed by fabric for efficient computation and processing required for saving microservice and service cooperative model to accredited blockchain in the form of hashed data which can be used further in trace-ability [31].

As hyper ledger is asymmetric in design and to realize nonrefutation, its digital signatures are very important. Another definition of asymmetric cryptography is public key cryptography that specifically uses public and private key pairs. In the process of encryption and decryption, similar keys are not required but the private key is generally used for decryption. But we also know that public keys are a subset of private keys. Hence, public keys are generated from the respective private key. However, its vice versa is not possible. Further, it is clear that public keys having elliptic curve response and RSA both are from the same family of asymmetric cryptography. But when comparing from other aspects, elliptic curve encryption outperforms in security performance to RSA method with low complex computation, high throughput, storage resource efficiency, and low bandwidth [32]. Hence, the mechanism to encrypt the information is given in Table 1.

2.3. Previous State-of-Art Works. Merging edge computing along with blockchain to form a new application has become an emerging domain of research. With emerging number of connected vehicle traffic and numerous applications over the vehicular network, their security is one of the key requirements. Therefore, blockchain being a key contender with vigilant security powered by hashing mechanism can provide more improved security along with data integrity for the proposed system. Similarly, edge computing renders benefits for scalable storage and processing. There are some

Table 1: Mechanism of encryption and authenticating signatures.

Encrypt the information	Authenticating signature
Step 1: opt an elliptic curve expressed by $\delta(c, d)$ with a base point defined by B. Step 2: define two keys one as private key expressed as Key_{Pr} such that $\text{Key}_{\text{Pr}} < n$, where n we define here for order of B, Key_{Pb}, for the public key. Subsequently, a public key can be calculated by $\text{Key}_{\text{Pb}} = \text{Key}_{\text{Pr}} P$. Step 3: further we selected an arbitrary integer number denoted by μ such that $\mu(\mu < n)$ is generated at the calculation $\rho = \mu B$. Step 4: for calculating hash $H = \text{SHA 256 (content}, e, f)$, such that e and f are the xy plane values of point ρ. $S_{ign} \equiv \rho - H + \text{KeyPr}(\lvert n \rvert)$ Step 5: We define signature as (μ, S_{ign}). With condition, if one random number μ and S_{ign} have zero value, then, go to step 3.	However, the process of authenticating signature is given below: step1: when information content is received along with signature (μ, S_{ign}), the forward calculations are $Sp + \text{SHA256(content)}\varpi = (e1, f1)\mu_1 \equiv e1/\lvert\varpi\rvert$ Further, step 2 will validate the expression, such that $\mu_1 \equiv \mu/\lvert\varpi\rvert$ Step 3: in this step, it is verified whether the identity in equation (6) is satisfied, if yes, then the signatures are valid otherwise a signature is invalid.

other works proposed in the domain of integrating blockchain wand edge computing targeting authentication and security exploiting the nonrefutation property of blockchain [33–36], some enhanced smart are [37, 38], and user protection is in [39].

Merging blockchain with edge computing to achieve tight security and verification, many researchers have proposed implementation methods, solutions, efficient architectures, and challenges. At last, the most optimal and practical solution to secure user security by joining edge computing and blockchain was proposed by [40]. Another solution proposed in [33] formed BNCS, i.e., blockchain-based nonrepudiation network computing service scheme, a secured platform dependent on the chain connected by industrial IoT and IOV through homomorphic encryption algorithm for riven services and generated hash in blockchain and [34] further extended this work by improving latency and security. Furthermore, [36] proposed an integrity check mechanism for vehicular network data in the blockchain, which mainly aims to facilitate the limited number of public chain nodes by opting random nodes. Work proposed in [35] formulated a token mechanism, which acts as a bridge especially for 5G-connected V2X networks and blockchain to validate privacy in internet of vehicles (IOV).

Smart contracts are also utilized extensively in similar applications, such that if written on blockchain can render an effective combination of conventional service level agreement (SLA) with the public blockchain [37]. The article proposed in [38] exploited distributed properties of blockchain edge computing in formulating penalty and recompense methods to encourage participants in using smart contracts to ensure implementation of predefined policies for the realization of a system where a trustee is only a blockchain.

With the advent of smart cities and ITS, 5G enables V2X network to face numerous challenges especially to secure communication, vehicle privacy, verification, etc. Therefore, the trend in this era is moving to combine blockchain with the 5G-V2X [32]. Thus, to ensure vehicle private data, [33] proposed a model considering privacy and security in smart grid application, to distinguish any glitch in overall acquired data and to guarantee its full-duplex communication's security utilizing blockchain and mutable autoencoders for securing glitches in acquired data.

All the above proposals are combining blockchain with ITS applications, IoVs, 5G-V2X, and smart grid factories. However, our network has the characteristic of mobility which is very critical for addressing its security and network-related concerns. [41] has proposed a novel solution targeting the security of vehicular network by using blockchain.

[42] continued similar bitcoin type approach, in which blockchain acts as an intermediary agent and also there is a reward for participants so that each node remains honest node to discourage any attack generated by the dishonest node. On the other side, consensus rules (contains incentives for participant node depending upon smart contract) for BFT participants are defined to develop multistep smart contracts to ensure security and privacy in vehicular network-based edge computing model

2.4. Blind Signature Process. In this subsection, we inculcate prerequisites relevant to blind signatures required in blockchain process.

Lemma 3. *Relational mapping.*

There is a relational mapping among both variables such that ℓ be a safety variable and p be a number represents ℓ bit prime. Furthermore, we define two cyclic groups $CG1$ and $CG2$, such that $CG1$ is an additive group comprised of p prime generated by P, Q which belongs to $CG1$ group.

However, $CG2$ is a multiplicative group having similar order p, such that linear mapping of both variable groups can be written as $\gamma : CG1 * CG2$, holding property of bilinearity such that any element c, d from set $Zp.$, there exists equality $\gamma(cP, dQ) = \gamma(P, Q)^{cd}$ with generative unity holding given by $\gamma(P, Q)\, 6 \neq 1$. Afterward, there are algorithms defined for computing gamma function $\gamma(P, Q)$.

Lemma 4. *CDH (computational Diffie-Hellman).*

We know that cyclic group $CG1$ is additive having p th order formed by beta β and arbitrary number c, d which are elements of $Zp.$, given that $c\beta$ and $d\beta$ are elements of additive group $CG1$. However, solving cdg is a challenging task.

Lemma 5. *Blind signature.*

Blind signature defined in [34, 43] comprises of a signer S_{ign}, a vehicle denoted by Ω and group of time variant polynomial algorithms (K_G, S, V).

(1) We represented the key generation algorithm by KG such that safety parameter for input is defined by $1^{`}$, for output, we use Out. The key generation algorithm generates pair of keys having one public and another private key $(\text{Key}_{\text{Pb}}, \text{Key}_{\text{Pr}})$

(2) For signature, a S sign variable is used to represent probabilistic time-variant polynomial in the defined protocol. Overall, the function requires system variables as input along with the public key Key_{Pb} such that, user Ω converts message msg into a blind message $msg*$ and then transmit it to the S_{ign}. Where S_{ign} is privately signed by private key Key_{Pr}. Afterward, the output is generated in a condition if protocol quits in the stipulated time, the algorithm will sign the output with S to generate signature $\tau(msg)$, in other cases process will be failed

(3) Third, the input parameter is verify given by, another time-variant polynomial based algorithm, having four inputs Out, Key_{pb}, msg,$\tau(msg)$, authenticates whether $\tau(msg)$ is the actual signature of msg message, if yes, then Boolean T is generated else F is the output

Let us assume signed message as a sequence of bits in string format of length n_{msg}, such that hash function is noncollision when $\text{HSH} : \{0,1\}* \longrightarrow \{0,1\}nmsg$. Hence, the algorithm can be realized in three subalgorithms.

2.4.1. System Parameter Generation. We initially assumed two cyclic groups $CG1$ and $CG2$ as an additive and multiplicative with order p and g be the generator variable of $CG1$ with the bilinear mapping γ: $CG1 * CG2 \longrightarrow CG2$. Also, for all $a \in Z.p$, there are n_{msg} +2 possible numbers $(\beta 2, t^{'}, t^{1}, .. \cdots, t_{n_{msg}})$ from given cyclic group $CG1$. Suppose that public key $\text{Key}_{\text{pb}} = \beta 1 = \beta c$ and private keys $\text{Key}_{\text{Pr}} = c$ and system function having output parameters $\text{Out} = (CG1, CG2, \gamma, \text{Key}_{\text{pr}}, \beta_2, t^{'}, t_1, .. \cdots, t_{nmsg})$ includes a secret c.

2.4.2. Signature. To formulate a signature, public safety parameter 1^{ℓ} along with output out needs to be entered. Furthermore, S_{ign} function provides its private key c, whereas, for signing Ω user transmits message msg secretly.

(1) *Blindness.* To achieve blindness in the message, Ω user enters respective ψ values for message msg signing, such that $\psi = t^{'} \prod_{i \in N_I} ti, N_i \subset \{1, .. \cdots n_{msg}\}$ having index i and $msg[i] = 1$, where i is the pointer indexing to the message bit string. Each user Ω selects $\ell \in_{N_I} \mathcal{Z}^{'}{}_{P}$,, computes ψ, $= \psi * \beta$, and transmits for the signatory purpose to S_{ign}

(2) *Blind Signatures.* On receiving ψ, at signor S_{ign}, the signor will generate a signature $\tau^{'} = (\tau_1^{'}, \tau_2^{'}) = (\beta^{c_2} \psi^{'l}, \beta^{l})$ of message ψ and forward it to Ω

(3) *Unblindness.* On receiving blind signature $T^{'}$, user Ω unfolds covered blindness by _

(4) *Verify.* At last in verification stage, source message string msg with length n_{msg} is entered. Afterward, the public key Key_{Pb} is verified along with the signature $\tau = (\beta_c^2 \psi^{l}, \beta^{l})$ of msg such that equality in expression (4) must hold

$$\gamma(\tau_1, \beta) = \beta(\beta_1, \beta_2)\gamma(\psi, \tau_2). \tag{4}$$

On satisfying the above equation the output will be 1; otherwise, the output will be zero.

3. Problem Modeling

Mobile edge computing is an example of decentralization, which distributes the load of processing and storage to resources available on wireless communication nodes like roadside base station (RBS). But the other fact is the availability of storage and processing resources on each 5G-enabled vehicle is restricted. A simple solution is to just execute a relevant piece of a function instead of loading the whole application can aid in maintaining the quality of service (QoS) with efficient energy consumption. While considering multiple vehicles for edge computing, the number of vehicles interactions also increases within the vehicular network, which is directly proportional to the probability of threat of data leakage. Therefore, handling vehicle's information security and privacy is a key challenge in this case. Hence, in this proposal, we design a blockchain-based trusted verification and streaming service awareness for 5G and beyond vehicle-to-everything (V2X) communication. The overall proposed network model in Figure 2 has triple-layer architecture defined as central cloud layer, edge layer, and on-road layer.

Second, the central cloud layer comprises of numerous servers on the cloud having high throughput for computing complex applications with huge storage because the server is accountable for complex computation along with bulk storage applications.

The intermediary layer is called as edge layer and contains several numbers of distributed edge cloud servers (i.e., roadside base station–RSB) interconnected with each other over the secure network. They are usually distributed among roadside base stations, road infrastructure including vehicles such as buses, cars, on the road having low computing, and storage resource, hence, they utilize services from distributed servers of these edge cloud servers to transmit service request in a block over. Other than organizing

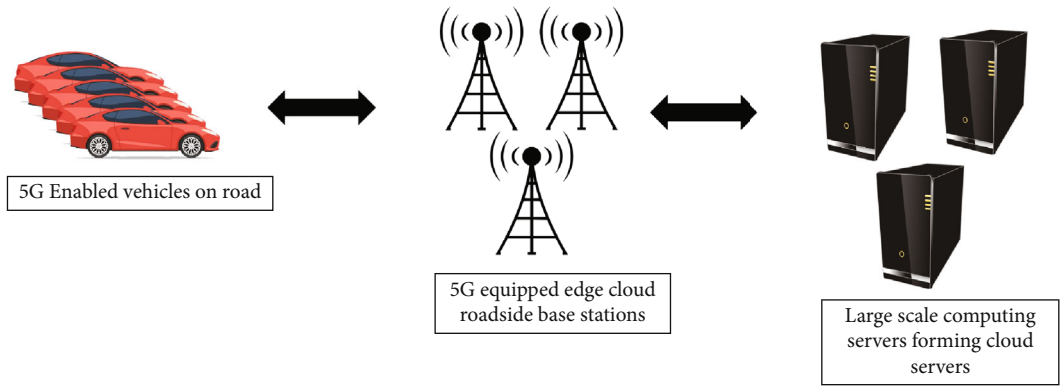

Figure 2: System model.

resources for computing and storage purposes for vehicular devices, the servers on the edge layers form blockchain connectivity due to the availability of traceability. TO maintain security and data integrity blockchain's traceability provides a way back to find save data, transmitted information, and along other running applications on the internet.

3.1. Adversary Model. The vehicle nodes are nowadays supporting many applications like video, navigating maps, and games. More precisely, maps used for navigation composed of hundreds of images connected with each other, and games nowadays require heavy processing power for execution. Therefore, to support execution of such application edge devices now are equipped with sufficient processing and memory to support vehicle agent for block stream placed at installed operating system along with dynamic and stream processing. Thus, edge devices rely on edge servers to process the application for computing and storing data using a wireless communication network. Communication security is a key factor required in wireless transmission. Hence, the main threats in this domain are counterfeit attacks or man in the middle may act as an adversary while communicating. In the overall network model, edge nodes are on main threat because after attacking, an adversary may transmit false information to the connected vehicles while communicating services to the vehicular node over the network. Second, the threat can be of targeting services information for tampering such that attacker may try to forge vehicle device and ask for true information/service from edge users (or ask for irrelevant) information.

In the proposed network, we suppose that within our communication, the edge node is honest and does not participate in any malicious attack and act true node and will not transmit any false cloud service. Consequently, the client will accept all offered services assuming correctness. Hence, both the parties will only share and store true information to the blockchain-based network.

3.2. System Model. As shown in Figure 2, the key elements for the proposed work are three main parts. The first part is service-based computing block, which aims to load dynamic applications from edge server storage into the connected vehicle through block streaming using 5G communication link. Second, to compensate intermediary agents, we introduce blockchain to authenticate each interaction between the edge server and vehicle nodes in the form of transactions. Furthermore, depending upon vehicle accessibility and need, the edge cache method is responsible for picking cache nodes according to edge node properties. Afterward, following the uniqueness and popularity of available services and resources, the cache replacement task is accomplished.

In our proposed method, for safe and efficient verification and execution of subservices among 5G-enabled vehicle node and edge server, we introduced nonrefutation and ineditable features inherited from blockchain to support block streaming for service computing in the existence of intermediary authentication and also, assign each vehicle nodes to time stamp evidence of communication between both ends. In the meantime, it is required to store spectral information of vehicle requesting service without sharing its privacy, so that by analyzing stored spectral information offered services and their combination feedback the efficiency of subservice can be enhanced. Furthermore, similar to the mechanism of blind signature, blinding vehicle node identity method is presented following improved bilinear mapping method by sharing given output parameters with the vehicle and server embedded with the blind variable of a received message, $\mathrm{Out} = (CG1, CG2, \gamma, \mathrm{Key}_{\mathrm{Pr}}, \beta_2, t, t1, \ldots t_{n_{msg}})$, in such a way the edge server will remain unknown of requesting vehicle node and will only have message requesting for service.

In our proposed method, we constructed our model on Hyperledger Fabric chain, where Hyperledger Fabric inside blockchain belongs to open source community of Linux foundation, considered as one of high-performance design used to define consensus rule driven by preopted nodes. Furthermore, Hyperledger Fabric contains some encryption algorithms known as identity mixer, which facilitates in hiding user identity and data privacy over the blockchain. This is same method adopted by [34].

The key steps for system model execution are as follows:

(i) *Initialization*. On getting start kick, the blockchain is initiated over the network based on X.509 certificate protocol. Afterward, several keys are generated by the ECDSA scheme and PKI method (public key infrastructure) to assign a digital certificate to each

node. Initially, a registration application is required from each IoV node and edge server on joining blockchain over the network for the first time so that for authorization, they can get their token generated at the time of user registration certification. Subsequently, a certificate is issued using account title and secret pin by authority for generation of token from each certificate. Finally, the generated token is then transmitted to account for adding and querying the identification certificate of each event in the form of blockchain. Other than certificates, the MSP interface is used to configure each vehicle for ensuring the security and privacy of each vehicle node because to achieve tight verification with user privacy protection for incognito mode interaction and decorrelation, the MSP interface provides several encryption protocols known for identity mixer. Hence, the certificate issuer shows that characteristics of vehicle nodes group are also produced in the form of digital certificates, such that a zero-knowledge-based certificate is generated by credentials, which optionally presents features chosen by vehicle node. Therefore, due to anonymity, no vehicle information will be shared with others [29]

(ii) *Services*. We know that each service is split into microservices. Hence, a service provider has all microservices stored in its storage and their execution flow order depends upon call graph defined in the blockchain ledger. As storage consumption of blockchain data is very little, therefore, in our scheme, we will store encrypted microservice on the blockchain is the form of hashed data such that the information to be stored is in the defined sequence (address of service handler, hash value of service function, and time stamp along with the QoS at the receiver). Likewise, finite state machines, we define here a service call graph (SRG) as an acyclic graph. On storing service relationships, the SRG can also be saved through the adjacency matrix of relationship and reach-ability of service relationship

In general, whenever a transaction occurs blockchain records it on nodes in the form of hash data. The general syntax of transactions over blockchain has a header and a message body. The header of a message includes information associated with the channel and code of calling chain, caller identification certificate along the appended arbitrary number (use to authenticate message). Furthermore, the node that solves the puzzle then simulates the transaction and verifies the correctness of format, like if submitted then validate the signature and checks whether the provider has granted write consent for the current channel or not. On authentication, a set is created for read/write operations. Moreover, read/write set is digitally signed to output response for calling application. On the server side, application loads SDK to produce transaction and announce it for sorting purpose, so that sorting node processes sorting operation on all the transactions and produces subsequent blocks accordingly. After sorting, ranking nodes produce blocks, which are then forwarded to master node accounting nodes available on the channel for several operation purposes. At last, the accounting and master node will initially validate the information contained on the block and then record the information on the respective ledger.

(i) *Requests*. This relates to the process to load and verify the service request. To maintain the security of each vehicle, each node initiates a query prior to the requesting service from the provider. In return, blockchain replies with the address of service provider along with the hash and time stamp and QoS information at the receiver. Furthermore, for hiding identity, each vehicle implements blind signatures to work as incognito in requesting service. Initially, the proposed system is kicked by key generation mechanism by providing safety parameter along with the output having system parameters Out = $(CG1, Cg2, \gamma, \text{Key}_{\text{Pb}}, \beta_2, t', t_1, \cdots..t_{nmsg})$, where Key_G generates pair having public and private key. After receiving message *msg*, vehicle node applies the blind function on the message *msg* requesting for microservice to acquire ψ for sending it to the edge server. We assume that on the edge server ψ is received, afterward, edge server will generate the signature τ' for the *msg* and forward it to vehicle. Whenever vehicle node receives τ', it applies deblind operation and authenticates the signature. On successful signature verification, Boolean true will be returned, and vehicle sends ψ and *msg* anonymously to the edge server as in algorithm 2. Afterward, on accepting service requests from vehicle node, another request is generated to blockchain from edge server for judicious verification of the invited microservice from the client. Whereas, on blockchain side, the network passes through the service call supported by the search algorithm on the graph (from the entrance to exit, searching an optimally reachable path inside the acyclic graph) to return the requesting caller with the optimal result of service. After verification of whether the request is reasonable or not, if not, then the requested service will be denied by initiating a smart contract. In the other case, if the request is cogent, then microservice will be granted firmly to the requesting vehicle

(ii) *Verification*. After verification of request and service, the microservice receives at the vehicle end. In the subsequent step, to generate a hash of microservice, a fast hashing function is applied to compare existing hash value from blockchain with the newly generated hash value. If both new and saved hash are equal, it means service granted by an authenticated edge server and throughout the process microservices remains free of attack, nontampered, and nonreplaced. However, if both hash values are not equal, the user will deny accepting microservices and initiate the smart contract

3.3. Caching Replacement. To enhance the hit rate on the cache of vehicular node by the cloud edge server for

handling service request, we devised a mechanism for edge cache replacement followed by requests from nodes and service awareness. Thus, in edge computing scheme, a model is uploaded by streaming data blocks such that the available edge server provides storage and resources for operating system (OS) execution to facilitate individual data and software at the application layer. In the defined network model, edge terminal provides a limited resource for storing the most frequent data required by edge nodes in mobile network and have precompiled services in memory to facilitate services to the requesting edge nodes with high throughput and minimum latency. Hence, increasing cache hit rate at each mobile edge node has pros in achieving a high-performance model.

In the initial step, to define cache node based on characteristics of communication, processing, and caching. However, based on vehicle mobility and movement, edge nodes and user nodes are at some distance, which is used to formulate a communication model depending upon received power.

$$P_W = \frac{C}{D_{ist}\left(\Omega_i, E_j\right)^2}. \tag{5}$$

We represent received power between distant nodes by P_W, where C is a constant factor, to minimize power, we divide the constant by normalizing distance D_{ist} between user Ωi and Ej edge node.

Every vehicular node's efficiency and performance depend upon available physical resources to facilitate requests in terms of compilation, resource allocation, and processing. Hence, more physical resources are directly proportional to the throughput achieved in handling user requests in fullduplex mode. Usually, the processing capacity of the node is represented by the term calculation degree Cd as a count number of operating nodes inside the network [37]. Hence, to define the processing power of a single edge node, we say $Cd = 1$, whereas, for defining power of multiple nodes, we formulate $Cd = n +$, in incremental way. More precisely, we say that Cd represents counting digit of operating nodes in computing data over the network.

For cache replacement, cache size is determined by subtracting occupied cache size from the total cache size. Therefore, cache size has a direct relation with the cache hit rate. Furthermore, vacant cache memory pertains to the capability of a node to perform cache operation irrespective of cache replacement. Therefore, among available nodes, request handling operation is forwarded to nodes having large vacant cache size, and we define cache vacant rate by C_{idle} to represent cache size of the node, which is calculated by the following expression.

$$C_{\text{idle}}\left(E_j\right) = \frac{C_{\text{vac}}\left(E_j\right)}{C_{\text{total}}\left(E_j\right)}. \tag{6}$$

Here in expression (6), we represented the vacant cache size of node by $C_{\text{vac}}(E_j)$ and denoted full cache capacity of node by $C_{\text{total}}(E_j)$. Hence, after analysis of the aforementioned abilities of edge node, we can rank each node through expression (7), where the ranking factor is RAN

$$\text{RAN}\left(E_j\right) = \frac{C_d * C_{\text{idle}}\left(E_j\right)}{P_w}. \tag{7}$$

We know that edge nodes have restrictions in resources for storing and processing. Hence, to load entire data requested by the client in cache is both resource and time-consuming task. For this challenge, we only choose the information which needs replacement on a frequent request basis (i.e., freshness and popularity) to facilitate streaming in 5G-V2X communication.

Performance of vehicle cache over edge network depends upon two attributes freshness and popularity. Therefore, to increase the performance of cache system, the cache node must have to validate resource freshness. Every time when the service request is hit by a cellular vehicle, an update event occurred such that an edge node will accept the updated version of the information. Mathematically, at edge node, we represent resource freshness by

$$\Omega(l) = T - r_r(T). \tag{8}$$

In expression (8), we denoted time by T at which edge node acknowledges information update event, whereas to represent timestamp for resource request generated by the user, we used variable $r_r(T)$. By intuition, we can say that $\Omega(l)$ has an inverse relation with the resource serving "l" popularity and is directly proportional to the delay occurred in receiving updated user information at edge node.

Depending upon the popularity of requested service resources, edge node can enhance hit rate of clients requesting services. Therefore, let us suppose on edge node E_j, l be the number of times service resource requested by the client previously, then:

$$A_j(l) = M_r(l) \sum_{i=1}^{n} M_{u_i}. \tag{9}$$

In expression (9), denominator represents previously accumulated number of requested resource l at edge E_j. Hence, in light of all the above discussion, we say $M_{trc}(l)$ be variable for cache metric. Whereas η be a controlling factor to curb magnitude of service resource in terms of freshness along with the popularity.

$$M_{trc}(l) = n\frac{1}{\Omega(l)}(1-n)A_j(l). \tag{10}$$

In the subsequent step, cache content having smaller metric value $M_{trc}(l)$ is available for cache and replacement purposes.

4. Performance Analysis

We have used Hyperledger Fabric 1.4.4 alliance chain-based blockchain implemented on open-source Ubuntu operating system using the specifications as shown in Table 2.

Moreover, in Table 3, a detail comparison for performance evaluation between 4G and 5G technologies is presented, and the performance of the proposed work has been done with the previous state of artwork [33, 34] in terms of:

(1) The efficiency with respect to average time vs. data

(2) Size

(3) The compiling time vs. hit rate (%). Note that the term hit rate is used to describe the success rate of an effort. In this proposed work, the successful effort is achieving optimum data rate with respect to number of vehicles

(4) Total startup delay vs. data size

(5) For mobility analysis switching time vs. vehicle speed

The main reason to analyze the proposed work on these four features is that whenever a security and trust algorithm is devised and incorporated in wireless communication applications like 5G-V2X, the over latency is increased, which is not required for mission-critical application of V2X communication. Therefore, an effective proposed work should have better performance with respect to these above-mentioned four features to attain lower latency at higher data rates. Lastly, we have also performed the security analysis of the proposed work such that its effectiveness in terms of providing security is also established.

4.1. Average Time vs. Data Size. One of the important factors in wireless communication is the average time taken by the algorithm to process data. As data size increases average time increases. For an application like 5G-V2X which requires minimum latency with a high data rate, the average time must not increase with the increase in data size. Figure 3 shows average time vs. data size, which clearly shows that the proposed work has achieved the minimum increase in average time as data size is increased; whereas previous works, i.e., [33, 34] have failed to do so. This is a clear indication that the proposed work comprehensively outperforms these previous research works. Thus, the proposed method is more suitable for 5G-V2X scenarios providing effective security while not compromising on average time.

4.2. Compiling Time vs. Hit Rate (%). The next important feature for an effective vehicular network is compiling time vs. hit rate (%). From Figure 4, we can deduce that as hit rate of the system is increased the compiling time decreases. Clearly, from Figure 4, we can see that the proposed work requires minimum compiling time to achieve a higher hit rate when compared with previous research works [33, 34].

4.3. Startup Delay vs. Data Size. Another important factor that needs to be considered is startup delay vs. data size. Figure 5 shows startup delay vs. data size. From this Figure 5, we can see that the proposed work comprehensively outperforms the previous works [33, 34]. The overall startup delay is minimum achieved by the proposed method, and as data size is increased, there is only a slight increase in startup delay, whereas [33] experienced an enormous increase in startup delay as data size is increased. [34] also shows a considerable increase in startup time when data size is increased.

4.4. Switching Time vs. Vehicle Mobility. As 5G-V2X network consists of various 5G-enabled vehicles traveling at various mobilities, i.e., speed. Switching time also depends upon the speed of the vehicle. An effective work would have minimum variation between switching time and vehicle speed. From Figure 6, it can be seen that the proposed work has almost the same switching time at various vehicle speeds, whereas [33] has shown a large increase in switching time when vehicle mobility is increased. Similarly, for [34], there is a significant change in switching time as vehicle mobility is increased. Overall, the proposed work has shown better performance than previous works.

4.5. Security Analysis of Proposed Work. This section theoretically explains the security analysis of the proposed model. As the key characteristic of blockchain is to remain immutable once written, hence, the data once stored in the chain cannot be altered; therefore, embedded smart contract is an essential object as intermediary trustee agent. Consequently, hash value at blockchain saved by the service provider is secure and immutable to facilitate edge vehicle with secure and verified information.

Data security in terms of tampering can be secured by blockchain. However, to ensure user privacy, we exploited several protocols for encryption known as identity mixer. Generally, these protocols follow the zero-retention concept, such that each vehicular node needs to authenticate itself over the blockchain without sharing any identity-based private information. More precisely, IoV node validates itself on blockchain by expressing reasonable identity but not the actual during authentication procedure [43]. Consequently, the connected IoV nodes can communicate over the blockchain network without fear of information leak.

While considering our model, we entailed a secure hash algorithm (SHA256) [44] to implement encryption. The second main characteristic of blockchain is irreversibility, i.e., one can go from input to output and obtain the same result every time but performing an inverse function on output cannot take us to the input. Hence, one-way attribute of blockchain can further infer below two functions:

(1) *Easy Computation.* Say that there exists a deterministic polynomial time-variant system represented by δ. Such that on every input x, the respective output of system δ is $y(x)$. By mathematical relation, we can write $\delta(x) = y(x)$

Table 2: System specifications.

	Cloud blockchain	Cloud edge server	Vehicle
CPU	3 GHz	1.8 GHz	64 MHz
RAM	16 GB	4 GB	64 KB
Storage	512 GB	32 GB	512 KB
Network	10 GB	1 GB	1 GB

Table 3: A comparison between 4G and 5G technologies.

	4G	5G
Data rate	300 Mbps	10 Gbps
Users per m^3	5	50–100
Mobility support	250–350 km/h	500 km/h
Latency	50 ms	1 ms
Inherit support for V2X	No	Yes

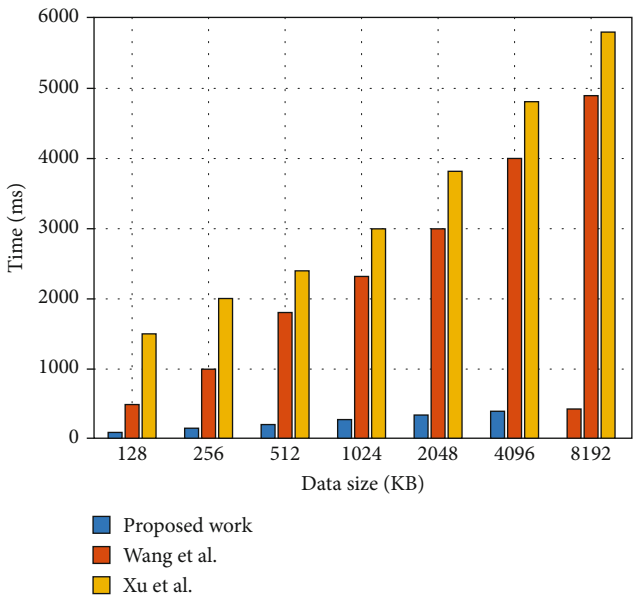

Figure 3: Average time vs. data size.

(2) *Difficult in Inverse Implementation*. Probabilistically, for each time-variant polynomial model, we denote,. subsequently, each nonnegative function $P(.)$, and for entire n, we describe a mathematical expression:

$$\Pr\left[\delta'(y(\Omega_n), 1^n) \in \delta^{-1}(\delta(\Omega_n))\right] < \frac{1}{P(n)}. \quad (11)$$

In general, the computed hash is collision-free. Hash collision occurs when two distinct input yields same hash output from the same hash function. Usually, hash collision is due to the reason of infinite possibilities of the input string and limited range of processed hash outputs. Therefore, by opting SHA256, we have 256-bit binary number at the output, and theoretically, we have 2^{256} possibilities at the output. Again theoretically, the estimated probability of hash collision is almost 0.9 given that provided inputs are 2^{130} in numbers. In this scenario, the probability of hash collision is ignorable. This characteristic is a strong contender in ensuring blockchain's data integrity because while communicating, saving, and retrieving operations, data is tampering proof and in another case, if someone is able to tamper successfully, it will be detected on time to handle security breach.

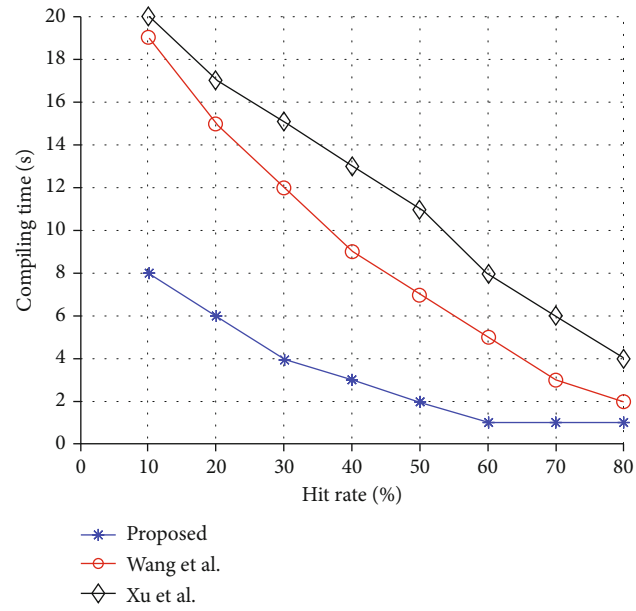

Figure 4: Compiling time vs. hit rate.

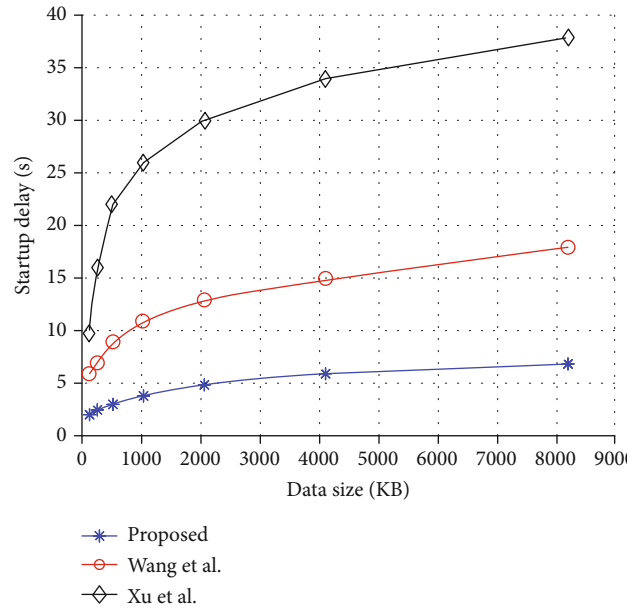

Figure 5: Start-up delay vs. data size.

4.5.1. Theory. Due to the WTRA algorithm, vehicle identity remains anonymous to the edge server whenever a request is generated. Hence, public and private key generation to achieve blindness has a strong effect in ensuring user privacy.

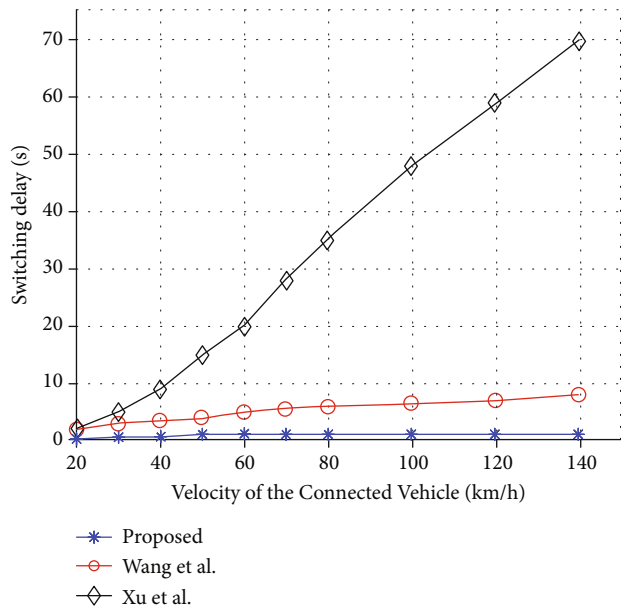

FIGURE 6: Switching time vs. vehicle mobility (speed).

4.5.2. Proof. To prove our message blindness concept, we assume IoV node process $\psi' = \psi.\beta^l$ (safety parameter l is selected secretly). Furthermore, edge server cannot calculate ψ from. Whereas ψ is similar to the message *msg*. We can imply that edge server is blind to the identity and service request of the user simultaneously. Moreover, the correctness of blind signature is verified by the below expressions:

$$\gamma\left(\tau'^1, \beta\right) = \gamma\left(\beta^{c_2}\psi'^{\ell}, \beta\right) = \gamma(\beta^{c_2}, \beta)\gamma\left(\psi'^{;}, \beta\right) = \gamma(\beta_2, \beta^c)\gamma\left(\psi', \beta^l\right) = \gamma(\beta_1, \beta_2)\gamma\left(\tau'^2, \psi'\right). \tag{12}$$

5. Conclusions

This paper proposes a novel work pertains to trust service awareness along with reliable authentication in big data driven 5th generation and beyond vehicle-to-everything (V2X) communication. The proposed work presents a way to upload microservice along with relationship graph to Hyperledger Fabric-based blockchain by introducing the blockchain as an intermediary trustee agent to witness each interaction between roadside base station as edge node and vehicle on the road in the form of hash. Furthermore, we integrated improved blind signature based on individual's identity to formulate a security mechanism for vehicle equipment, so that it can communicate anonymously in requesting services from roadside edge node, this is the way we ensured verified communication between two ends by hiding actual identity. The proposed work also put forward the development of a roadside edge cache scheme to increase the efficiency of resource and vehicle's cache hit rate basis on vehicle requests along with service awareness to place precompiled services at each vehicle node for prompt caching. In the end, we compared our work with the previous existing works. The simulation result shows that our proposal elicits considerable efficiency and security for future applications in 5G and beyond vehicle-to-everything (V2X) communication.

Data Availability

The data that support the research findings are available on request. The data are not publicly available due to privacy of research participants.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] W. U. Khan, X. Li, A. Ihsan, M. A. Khan, V. G. Menon, and M. Ahmed, "NOMA-enabled optimization framework for next-generation small-cell iov networks under imperfect sic decoding," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–10, 2021.

[2] M. Asif, W. Zhou, M. Ajmal, N. A. Khan, Z. U. A. Akhtar, and N. A. Khan, "A construction of high performance quasicyclic LDPC codes: a combinatoric design approach," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 7468792, 10 pages, 2019.

[3] W. U. Khan, T. N. Nguyen, F. Jameel et al., "Learning-based resource allocation for backscatter-aided vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–15, 2021.

[4] M. Asif, W. Zhou, Q. Yu, X. Li, and N. A. Khan, "A deterministic construction for jointly designed quasicyclic LDPC coded-relay cooperation," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 5249373, 12 pages, 2019.

[5] W. U. Khan, M. A. Javed, T. N. Nguyen, S. Khan, and B. M. Elhalawany, "Energy-efficient resource allocation for 6g backscatter-enabled NOMA IoV networks," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–11, 2021.

[6] M. Asif, W. Zhou, Q. Yu, S. Adnan, M. S. Ali, and M. S. Iqbal, "Jointly designed quasi-cyclic ldpc-coded cooperation with diversity combining at receiver," *International Journal of Distributed Sensor Networks*, vol. 16, no. 7, 2020.

[7] M. Asif, W. U. Khan, H. Afzal et al., "Reduced-complexity LDPC decoding for next-generation IoT networks," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 2029560, 10 pages, 2021.

[8] W. U. Khan, F. Jameel, N. Kumar, R. Jantti, and M. Guizani, "Backscatter-enabled efficient v2x communication with non-orthogonal multiple access," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1724–1735, 2021.

[9] K. Yue, Y. Zhang, Y. Chen et al., "A survey of decentralizing applications via blockchain: the 5g and beyond perspective," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2191–2217, 2021.

[10] C. Bachechi, L. Po, and F. Rollo, "Big data analytics and visualization in traffic monitoring," *Big Data Research*, vol. 27, p. 100292, 2022.

[11] S. Malathy, P. Jayarajan, H. Ojukwu et al., "A review on energy management issues for future 5g and beyond network," *Wireless Networks*, vol. 27, no. 4, pp. 2691–2718, 2021.

[12] E. Ahvar, S. Ahvar, and S. M. Raza, "Next generation of sdn in cloud-fog for 5g and beyond-enabled applications: opportunities and challenges," *Network*, vol. 1, no. 1, pp. 28–49, 2021.

[13] V. Konecny, C. Barnett, and M. Poliak, "Sensing and computing technologies, intelligent vehicular networks, and big data-driven algorithmic decision-making in smart sustainable urbanism," *Contemporary Readings in Law and Social Justice*, vol. 13, no. 1, pp. 30–39, 2021.

[14] N. Anwar, D. R. Adhy, B. Tjahjono, R. Hermawan, N. Widiyasono, and M. A. Hadi, "Reliability analysis of communication network service quality for internet of vehicles (iov)," *International Journal of Science, Technology & Management*, vol. 2, no. 5, pp. 1588–1599, 2021.

[15] I. Rasheed, "Enhanced privacy preserving and truth discovery method for 5G and beyond vehicle crowd sensing systems," *Vehicular Communications*, vol. 32, p. 100395, 2021.

[16] X. Meng, S. Roberts, Y. Cui et al., "Required navigation performance for connected and autonomous vehicles: where are we now and where are we going?," *Transportation Planning and Technology*, vol. 41, no. 1, pp. 104–118, 2018.

[17] Y. Zhang, X. Lan, J. Ren, and L. Cai, "Efficient computing resource sharing for mobile edge-cloud computing networks," *IEEE/ACM Transactions on Networking*, vol. 28, no. 3, pp. 1227–1240, 2020.

[18] Y. Zhang, K. Guo, J. Ren, Y. Zhou, J. Wang, and J. Chen, "ransparent computing: a promising network computing paradigm," *Computing in Science & Engineering*, vol. 19, no. 1, pp. 7–20, 2017.

[19] T. Nguyen, N. Tran, L. Loven, J. Partala, M.-T. Kechadi, and S. Pirttikangas, "Privacy-aware blockchain innovation for 6g: challenges and opportunities," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*, pp. 1–5, IEEE, 2020.

[20] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future intelligent and secure vehicular network toward 6g: machine-learning approaches," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 292–307, 2020.

[21] D. Lu, R. Han, Y. Shen et al., "Xtseh: a trusted platform module sharing scheme towards smart IoTehealth devices," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 370–383, 2021.

[22] J. Ren, D. Zhang, S. He, Y. Zhang, and T. Li, "A survey on endedge-cloud orchestrated network computing paradigms: transparent computing, mobile edge computing, fog computing, and cloudlet," *ACM Computing Surveys (CSUR)*, vol. 52, no. 6, pp. 1–36, 2019.

[23] J. Ren, Y. Guo, D. Zhang, Q. Liu, and Y. Zhang, "Distributed and efficient object detection in edge computing: challenges and solutions," *IEEE Network*, vol. 32, no. 6, pp. 137–143, 2018.

[24] X. Peng, J. Ren, L. She, D. Zhang, J. Li, and Y. Zhang, "BOAT: a block-streaming app execution scheme for lightweight iot devices," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1816–1829, 2018.

[25] D. Zhang, R. Shen, J. Ren, and Y. Zhang, "Delay-optimal proactive service framework for block-stream as a service," *IEEE Wireless Communications Letters*, vol. 7, no. 4, pp. 598–601, 2018.

[26] F. Lyu, J. Ren, N. Cheng et al., "Lead: large-scale edge cache deployment based on spatio-temporal wifi traffic statistics," *IEEE Transactions on Mobile Computing*, vol. 20, no. 8, 2021.

[27] W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li, and R. Chen, "NutBaaS: a blockchain-as-a-service platform," *Ieee Access*, vol. 7, pp. 134422–134433, 2019.

[28] V. Aleksieva, H. Valchanov, and A. Huliyan, "Implementation of smart contracts based on hyperledger fabric blockchain for the purpose of insurance services," in *2020 International Conference on Biomedical Innovations and Applications (BIA)*, pp. 113–116, IEEE, 2020.

[29] C. Gorenflo, S. Lee, L. Golab, and S. Keshav, "Fastfabric: scaling hyperledger fabric to 20 000 transactions per second," *International Journal of Network Management*, vol. 30, no. 5, p. e2099, 2020.

[30] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the IoT and industrial IoT: a review," *Internet of Things*, vol. 10, p. 100081, 2020.

[31] W. Wang, J. Song, G. Xu, Y. Li, H. Wang, and C. Su, "Contractward: automated vulnerability detection models for ethereum smart contracts," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1133–1144, 2020.

[32] I. Rasheed, L. Zhang, and F. Hu, "A privacy preserving scheme for vehicle-to-everything communications using 5G mobile edge computing," *Computer Networks*, vol. 176, p. 107283, 2020.

[33] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, and Y. Zhang, "A blockchain-based nonrepudiation network computing service scheme for industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3632–3641, 2019.

[34] Y. Wang, Y. Tian, X. Hei, L. Zhu, and W. Ji, "A novel IoV block-streaming service awareness and trusted verification scheme in 6g," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 5197–5210, 2021.

[35] D. Mazzei, G. Baldi, G. Fantoni et al., "A blockchain tokenizer for industrial IoT trustless applications," *Future Generation Computer Systems*, vol. 105, pp. 432–445, 2020.

[36] Y.-J. Chen, L.-C. Wang, and S. Wang, "Stochastic blockchain for iot data integrity," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 373–384, 2020.

[37] A. Alzubaidi, E. Solaiman, P. Patel, and K. Mitra, "Blockchain-based sla management in the context of IoT," *IT Professional*, vol. 21, no. 4, pp. 33–40, 2019.

[38] X. Xu, X. Zhang, H. Gao, Y. Xue, L. Qi, and W. Dou, "Become: blockchain-enabled computation offloading for IoT in mobile edge computing," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4187–4195, 2019.

[39] M. Keshk, B. Turnbull, N. Moustafa, D. Vatsalan, and K.-K. R. Choo, "A privacy-preserving-framework-based blockchain and deep learning for protecting smart power networks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5110–5118, 2019.

[40] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: a survey, some research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1508–1532, 2019.

[41] S. Wang, D. Ye, X. Huang, R. Yu, Y. Wang, and Y. Zhang, "Consortium blockchain for secure resource sharing in vehicular edge computing: a contract-based approach," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, 2021.

[42] C. Chen, J. Wu, H. Lin, W. Chen, and Z. Zheng, "A secure and efficient blockchain-based data trading approach for internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 9110–9121, 2019.