Traffic-Aware Content Caching For Vehicular Social Networks Using Deep Reinforcement Learning

G Nisha[1], .A Ashmol[2]
[1, 2] Dept of CSE
[1, 2] Arunachala College of Engineering for Women

Abstract- *Vehicular social networking is an emerging application of the Internet of Vehicles (IoV) which aims to achieve seamless integration of vehicular networks and social networks. However, the unique characteristics of vehicular networks, such as high mobility and frequent communication interruptions, make content delivery to end-users under strict delay constraints extremely challenging. In this paper, we propose a social-aware vehicular edge computing architecture that solves the content delivery problem by using some vehicles in the network as edge servers that can store and stream popular content to close-by end-users. The proposed architecture includes three main components: 1) the proposed social-aware graph pruning search algorithm computes and assigns the vehicles to the shortest path with the most relevant vehicular content providers. 2) the proposed traffic-aware content recommendation scheme recommends relevant content according to its social context. This scheme uses graph embeddings in which the vehicles are represented by a set of low-dimension vectors (vehicle2vec) to store information about previously consumed content. Finally, we propose a deep reinforcement learning (DRL) method to optimise the content provider vehicle distribution across the network. The results obtained from a real-world traffic simulation show the effectiveness and robustness of the proposed system when compared to the state-of-the-art baselines.*

Keywords- Internet of vehicles, Deep reinforcement learning, Mobility

I. INTRODUCTION

Vehicle ad hoc networks (VANET) are often referred to as networks on wheels, which are used to provide connectivity between vehicle nodes. It is an outgrowth of mobile networks. Vehicular nodes are self-organized and connect with each other in a less environmentally sound infrastructure. The IEEE Committee has established the IEEE 802.11p standard for VANETs, recognizing that the ad hoc vehicle network is essential for the provision of safety-associated applications in the Intelligent Transportation System. For short-range transmission, the US Federal Communication Commission (FFC) has allotted 75 MHz of bandwidth at 5.9 GHz between vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). The main objective of VANETs is to create an intelligent framework for transport. In building V2V and V2I communications, Dedicated Short Range Communication (DSRC) may play an important role. DSRC has a range of around one thousand meters. Inter-networking via VANETs has received huge attention over the past few years. Realizing its increasing importance, academia, major automotive manufacturers, and government agencies are making efforts to develop VANETs.

VANET has mobile nodes, sensor vehicles, static networks, fixed roadside access points (RSAP), and wireless links such as V2V, V2I, and point-to-a-vehicle access (I2V). Depending on the coverage requirements, this wireless communication device consists of a combination of GPS and a cellular communication system using either one- or multi-hop mode. One of this technology's main services is to support drivers with protection so that road injuries can be reduced. Providing protection for onboard passengers is the main service offered by this form of network. A VANET's key requirements are high processing power, large storage space, adequate energy, and node movement estimation. This technology facilitates a variety of applications that affect daily human life, such as infotainment, traffic management services, and security.

The emergence of the Internet of Vehicles (IoV) as a new networking paradigm that interconnects vehicles with the ubiquitous Internet of Things (IoT) network and the increasing adoption of the 5G network in many countries, the vision of the intelligent transportation system (ITS) is closer to realisation than ever. The IoV network is expected to enhance many applications and offers a wide range of services, ranging from essential emergency services to entertainment service applications. There are currently more than 1.4 billion vehicles worldwide, and it is expected to reach three billion in 2037, which will worsen the existing traffic congestion problem. As more and more people spend hours in traffic congestion, they turn to social media and other entertainment services to spend the waiting time. The IoV can offer an alternative to connect the users with the Internet and seamlessly interconnect their existing social networks to a vehicular social networking

model that brings social content near to passengers and reduce the expensive access to the 4G/5G networks.

One of the most challenging problems in a vehicular social networking model is the difficulty of seamlessly accessing social network content without interruptions and delivery delays. In vehicular networks, the content can be delivered through Vehicle to Infrastructure (V2I) communication with the Roadside Units (RSU) connected to the Internet or through cellular base stations using 4G or 5G networks. The former is reasonably cheap and convenient communication but suffers from difficult access and sparse RSUs. Vehicles must rely on Vehicle-to-Vehicle (V2V) communications to overcome sparse RSUs. The latter has the advantage of wide coverage and instant access, but it has expensive communications. The intuitive approach is to store the content of social networks on a cloud server, and the vehicles can access it through V2I communications or by downloading it using 4G or 5G cellular networks. Nonetheless, V2I communications are not appropriate for live streaming due to the high speed of vehicles and the frequent disconnections between vehicles and RSUs. On the other hand, the vehicle-to-base station communications are more stable compared to V2I communications but not suitable for downloading large files due to the high costs of those network usage.

II. LITERATURE SURVEY

Improving road safety is one of the primary goals of smart transportation systems. Vehicle accident alert systems broadcast collisions to automobiles in an ad hoc vehicle network. Emergency vehicles must respond promptly in order to offer emergency services and must have clear clearance on roadways. A little lag in the transit period of an emergency vehicle might result in the loss of important lives. The system requires faster broadcast of safety and emergency notifications in order to minimize additional effect. Regarding priority to cars and messages, our suggested strategy of fair scheduling of priority messages or vehicles aids in the speedier distribution of emergency messages by broadcasting with a reduced number of backoff timeslots and giving fair channel access to priority messages, indicating improved reliability.

The Vehicular Social Network (VSN) is an emerging mobile communication system combining a VANET with a social network. It provides a new means of sharing, disseminating, and delivering data for passengers, drivers, and vehicles. However, a VSN may expose users' private information, such as identities, location information, and trajectories, and tampering with shared data may lead to security and safety problems in vehicle systems. Considering the security and privacy preservation of shared data, hence using a lightweight decentralized multiauthority access control scheme based on Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and blockchain, by which a decentralized multi-authorization node supports vehicle users by performing lightweight calculations with the assistance of the Vehicle Cloud Service Provider (VCSP). To use blockchain to record storage and access transactions, achieving self-verification by users and tamper-resistance of ciphertexts. An improved smart contract reduces the workload of verification by users and achieves privacy preservation by hiding the policy. It supports user revocation and outsourced decryption, enabling more flexibility and better performance. A security and performance analysis shows the scheme has clear advantages over existing schemes.

Vehicular social network is emerging as a new promising concept, combining two types of network paradigms, namely, vehicular networks and social networks. In order to manage efficiently the security and the control of the network, this paper proposes a new framework based on the emerging concepts of Software-Defined Vehicular Network (SDVN) and blockchain. Using the SDVN makes the network more programmable, virtualized, and partitionable. Hence introduce the blockchain paradigm that will enable the certification of transactions and ensure data anonymity in a fully distributed manner. To this end, three levels of controllers are needed: a Principal Controller (PC), Roadside Units (Rsus), and a local controller. In order to dynamically select miners, a Distributed Miners Connected Dominating Set Algorithm (DM-CDS) has been proposed. The DM-CDS is a single-phase distributed algorithm that supports a dynamic topology based on a trust model and some other network parameters, such as the connectivity degree, the average link quality indicator, and the rank. The performance of the proposed DM-CDS is evaluated throughout multiple scenarios using different parameters, such as trust metric, node density, node mobility, and radio range.

With the rapid development of Internet of Vehicles (IoV), vehicle-based Spatial Crowdsourcing (SC) applications have been proposed and widely applied to various fields. However, location privacy leakage is a serious issue in spatial crowdsourcing because workers who participate in a crowdsourcing task are required to upload their driving locations. In this paper, They propose a decentralized location privacy-preserving SC for IoV, which allows vehicle users to securely participate in SC with ensuring the task's location policy privacy and providing multi-level privacy preservation for workers' locations. Specifically, To introduce blockchain technology into SC, which can eliminate the control of vehicle user data by SC-server. To combine the additively

homomorphic encryption and circle-based location verification to ensure the confidentiality of task's location policy. To achieve multi-level privacy preservation for workers' driving locations, Hence to reveal a grid where workers are located in. The size of the grid represents the level of privacy preservation. To leverage the order-preserving encryption and non-interactive zero-knowledge proof to prevent workers from illegally obtaining rewards by forging their driving locations. The security analysis results show that our framework can satisfy the above requirements. In addition, the experiment results demonstrate that framework is efficient and feasible in practice. Realizing access control to sensitive data offloaded to a Cloud is challenging in the Internet of Things, where various devices with low computational power and different security levels are interconnected. Despite various solutions, the National Institute of Standards and Technology (NIST)'s Attribute-Based Access Control (ABAC) model is one of the preferred techniques in the literature. In this model, users who satisfy access policies using both static and dynamic attributes are allowed to access the data. However, NIST's ABAC model does not support encryption and therefore does not satisfy data confidentially. Attribute-Based Encryption (ABE) is a known cryptographic primitives that enables fine-grained access control over encrypted data. However, currently the existing ABE schemes do not meet NIST's ABAC requirements or are not computationally efficient enough for IoT applications. In this paper, To propose a Multi-Level Security ABAC (MLS-ABAC) scheme that satisfies the requirements of NIST's ABAC model. Our construction is efficient and relies on a decryption outsourceable Ciphertext-Policy ABE scheme. Additionally, based on realistic application scenarios, only the authorized data users can decrypt the ciphertext, and check the integrity of the retrieved message. Furthermore, we present both conceptual and formal models for proposed MLS-ABAC architecture along with performance metrics.

The Vehicular Social Networks(VSNs) supports diverse kinds of services such as traffic management, road safety, and sharing data (videos, audios, roads photos, air quality, and so on). However, its complex, large-scale and dynamic network structure poses new security challenges. Among these challenges, secure data transmission has turned to be a spotlight. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) may be adopted to realize one-to-many data sharing in VSNs. In traditional CP-ABE schemes, access policy is stored and granted by the could, which lacks credibility due to centralization. In this article, To propose a secure and verifiable one-to-many data sharing scheme to solve the above problem. To use blockchain to record the access policy, realizing user self-certification and cloud non-repudiation. Considering the computing capabilities of the vehicular user, we propose an effective scheme for certificating. Meanwhile, considering the sensitive information included in the access policy, Hence to propose a policy hiding scheme. This scheme also supports data revocation when a vehicular user no longer wants to share the data in VSNs. Finally, security analysis and simulation show our scheme is both secure and efficient.

One of the challenges in Attribute-Based Access Control (ABAC) implementation is acquiring sufficient metadata against entities and attributes. Intelligent mining and extracting ABAC policies and attributes make ABAC implementation more feasible and cost-effective. This research paper focuses on attribute extraction from an existing enterprise relational database management system – RDBMS. The proposed approach tends to first classify entities according to some aspects of RDBMS systems. By reverse engineering, some metadata elements and ranking values are calculated for each part. Then entities and attributes are assigned a final rank that helps to decide what attribute subset is a candidate to be an optimal input for ABAC implementation. The proposed approach has been tested and implemented against an existing enterprise RDBMS, and the results are then evaluated. The approach enables the choice to trade-off between accuracy and overhead. The results score an accuracy of up to 80% with no overhead or 88% of accuracy with 65% overhead.

Reducing energy consumption in cloud data centers is one of The cryptosystem-based data privacy preserving methods employ high computing power of cloud servers, where the main feature is to allow resource sharing and provide multi-user independent services. Therefore, to achieve the rapid allocation and release of resource sharing in cloud computing, decentralized cryptographic protocols need to be proposed for multi-user consensus systems. In this work, First present a multi-secret sharing scheme with multi-level access structure, where the secret reconstruction algorithm satisfies the additive homomorphism. The secret sharing scheme needs no trusted third parties and any user can play the role of dealer. In the designing, multiple target secrets are independently shared, where each subset of users forms a sub-access structure and shares one target secret only with a short secret share. This scheme is efficient and unconditionally secure And our e-voting scheme does not need any high-complexity computational cost operation such as module exponential operation, etc. Finally, the common feature of Blockchain and Ad Hoc networks is decentralized. Thus the main idea of this protocol without a trusted third party can be used to achieve a secure consensus among multiple nodes in Blockchain and Ad Hoc network, meanwhile, the consensus results can be verified.

III. PROPOSED SYSTEM

The two common ways of delivering content in vehicular networks are V2I connection or cellular base stations using a 4G/5G interface. The former is cheap and has a simple communication model, but it is not easy to directly access the content. The vehicles rely on V2V communications to reach the sparse RSUs. The latter has the advantage of better coverage and instance access, but at the expense of expensive communications. To deal with these issues, VeSoNet implements a hybrid data distribution approach, where only popular data content is replicated and stored in vehicles to avoid excessive simultaneous downloads from 4G or 5G networks. In this regard, we distinguish three types of vehicular nodes: 1) Consumers form most vehicles in the network and represent the system end-users. 2) Provides store social content. The objective is to maximize the delivery to consumers as they travel through the city. 3) Meta-data vehicles, situated in busy locations of a city, provide information about content locations and perform various tasks, such as shortest social path calculation, content similarity, etc.

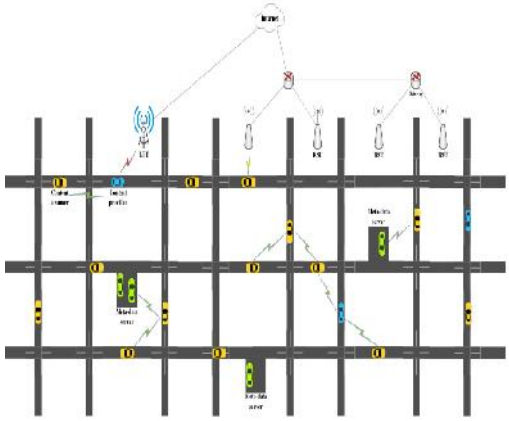


Fig 1 Proposed System Architecture

Consumer, provider, and meta-data server vehicles are represented in yellow, blue, and green, respectively. Meta-data servers are in busy locations, such as parking lots, where they are always present and not moving frequently, which ensures the quality of content lookup service. Meta-data servers maintain a table that contains a list of available contents in the network and a list of providers. The providers send frequent location and expected path updates to meta-data servers. The VeSoNet system follows Information-Centric Networking (ICN) model. When a consumer requests a given content, it creates a packet regarding the desired information that contains the content identifier and traffic information of the requesting vehicle, such as the expected travel path. The message is sent to all neighbouring nodes and forwarded to other nodes until it reaches the provider. When an intermediate node receives that packet and does not store the requested content, it forwards it to the nearest meta-data servers. If the providers do not have the requested content, RSU downloads it from an external network and forwards it to the requester. The providers back it up for future use.

The proposed framework leverages traffic information and dynamic changes in vehicles' travelling paths to bring the consumers close to providers, enhancing the content delivery experience. As a provider takes the same path as consumers, the delivery delay is significantly reduced. A consumer is travelling from the source location (S) to the destination location (D). Although path P1 is the shortest path, the system recommends P2 since it contains more providers and does not exceed the rerouting threshold as P3 does.

Let Psh = {Is → Ix1 , . . . , Ixn → Id } be the shortest path based only on traffic information, without considering the availability of the providers. Is and Id are the starting intersection (source intersection) and destination intersection, respectively. The objective is to find an alternative social-aware shortest path Pso that maximizes the number of providers for a vehicle during its trip, subject to the difference between shortest travel time τ (Psh) and social path τ (Pso) is less than a threshold ε. A naive approach is to find the shortest paths between Is and Id , then consider the social path that maximizes the number of providers and satisfies the threshold ε. However, this approach is computationally expensive.

IV. MODULES DESCRIPTION

Consumers Path Planning

Path planning is like the brain of a self-driving car. It's how the vehicle makes decisions about how to move through the world. In our model of the self-driving car software stack, it comes after perception and localization.

Traffic-Aware Content Recommendation

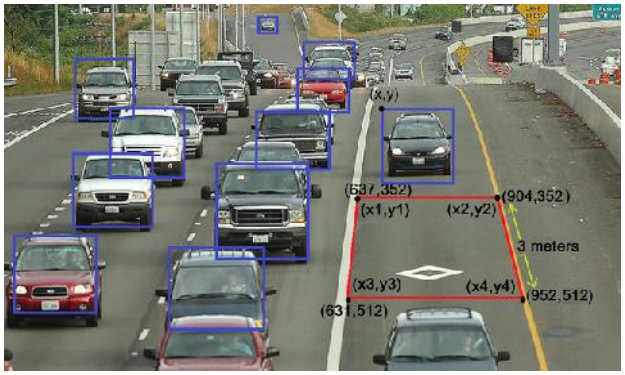
A graph embedding-based content recommendation approach called Vehicle2vec, where the vehicles are represented by a set of low dimensional vectors of the previously consumed content. Vehicle2vec starts by learning the feature representations of each content available in the system. The content network is represented as a graph data structure, where the nodes represent the data content, and the edges represent the content similarity between these nodes. Vehicle2vec learns the content node low dimensional vector that preserves the neighbourhood of nodes in the original graph. To build such content node embeddings, vehicle2vec

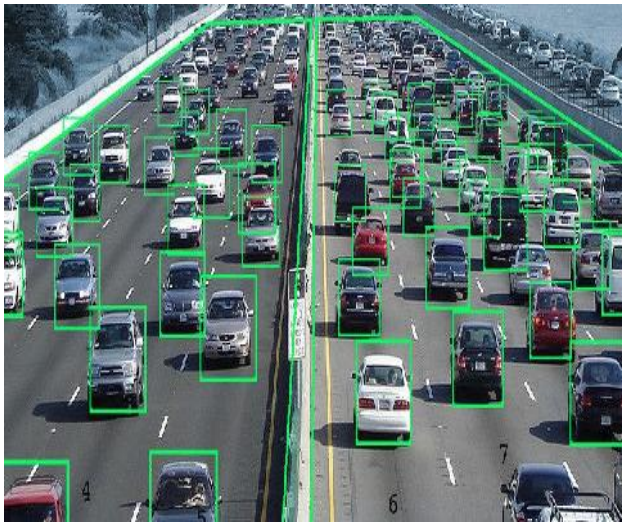
uses stochastic gradient descent (SGD) to optimize the objective function, hence learning the low dimensional representation.

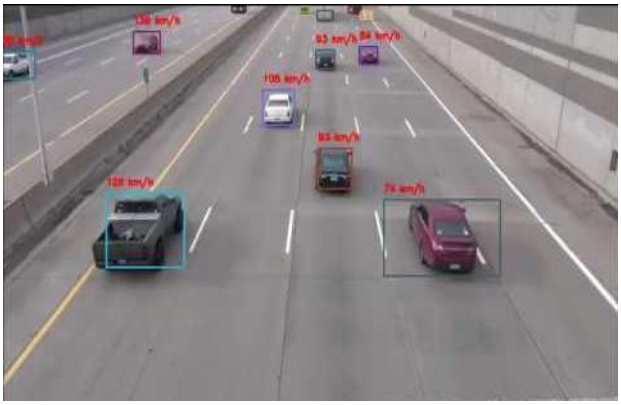
Content Provider Distribution

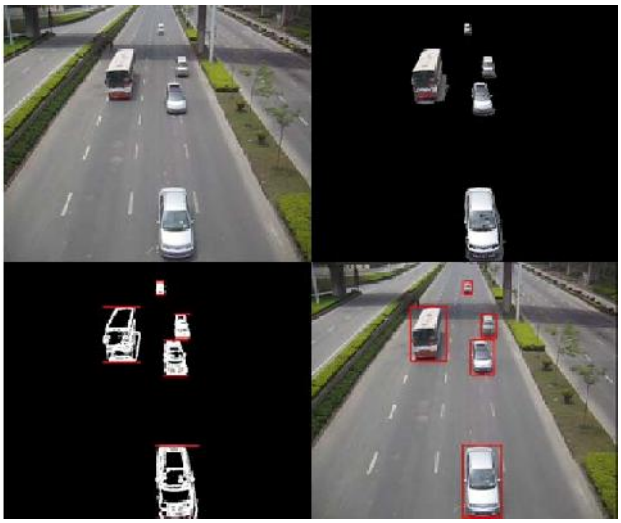
Finding optimal routing from content providers to consumers is known as the vehicle routing problem (VRP). VRP is NP-hard. Various meta-heuristic algorithms have been proposed to find sub-optimal solutions, such as the firefly algorithm , genetic algorithm or hybrid meta-heuristic algorithms. In addition, these meta-heuristic algorithms assume stable traffic conditions. Unlike traditional VRP, in the problem at hand, the traffic flow is constantly changing over time. In other words, one needs to find near-optimal solutions to a VRP with dynamic traffic conditions. Given a content provider vehicle vx travelling from starting position PoSs to PoSD taking the path px , the objective is to optimize the revenue generated from the advertisements delivered to consumers. An intuitive approach would be to choose a road that maximizes the number of consumer vehicles, but when the same road contains many provider.

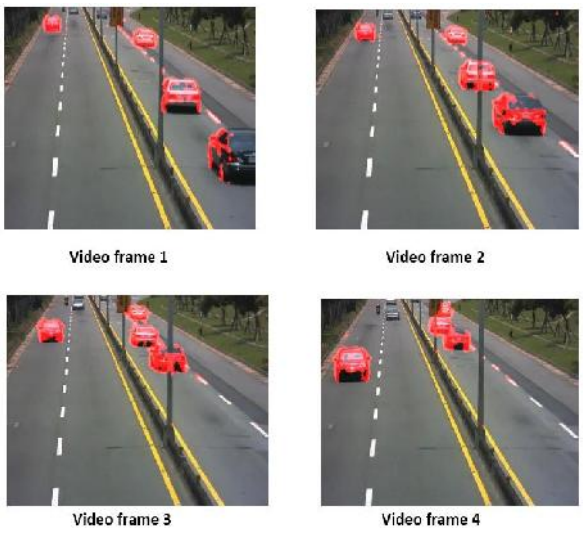
V. SCREEN SHOTS











VI. CONCLUSION

In this phase, presented a traffic-aware vehicular content caching architecture that optimizes content

dissemination among vehicles using a social-aware graph pruning technique. This technique computes and assigns the shortest paths with the most relevant providers to the corresponding consumers. To recommend relevant content according to their social context, we proposed a traffic-aware content recommendation approach based on graph embeddings. An efficient formal model, where vehicles are represented by a set of low dimensional vectors (vehicle2vec) of their previously consumed content. Experimental results show that the proposed architecture reduces content delivery delay and delivery ratio by more than 20% compared to the state-of-the-art baselines, at a slightly higher computational cost and average travel time.

All the communications between content consumers and content providers are encrypted, however, it is still possible to perform statistical attacks to infer the content consumers future paths, the privacy of the content consumers can be preserved by adding a pseudonyms identification scheme. The vehicular edge computing architecture can be further extended by adding computational task offloading, where all the computational tasks are performed in the vehicles. The social path selection process could be further extended to include driver preferences for individual road selection. used CNN as a training model for DRL. VeSoNet can be further developed by optimizing the training model.

REFERENCES

[1] Padiya, Ms Puja, and Mr Amarsinh Vidhate. "Fair Scheduling of Priority Message or Vehicle (FSPMV) in Vehicular Ad-hoc Network."

[2] Zhang, Leyou, Ye Zhang, Qing Wu, Yi Mu, and Fatemeh Rezaeibagha. "A Secure and Efficient Decentralized Access Control Scheme Based on Blockchain for Vehicular Social Networks." IEEE Internet of Things Journal (2022).

[3] Yahiatene, Youcef; Rachedi, Abderrezak; Riahla, Mohamed Amine; Menacer, Djamel Eddine; Nait-Abdesselam, Farid (2019). A blockchain-based framework to secure vehicular social networks. Transactions on Emerging Telecommunications Technologies, (), e3650–. doi:10.1002/ett.3650 .

[4] Zhang, Junwei; Yang, Fan; Ma, Zhuo; Wang, Zhuzhu; Liu, Ximeng; Ma, Jianfeng (2020). A Decentralized Location Privacy-Preserving Spatial Crowdsourcing for Internet of Vehicles. IEEE Transactions on Intelligent Transportation Systems, (), 1–15. doi:10.1109/TITS.2020.3010288 .

[5] A. F. M. Suaib Akhter;Mohiuddin Ahmed;A. F. M. Shahen Shah;Adnan Anwar;Ahmet Zengin; (2021). A Secured Privacy-Preserving Multi-Level Blockchain Framework for Cluster Based VANET . Sustainability, (), –. doi:10.3390/su13010400.

[6] Fan, Kai, Qiang Pan, Kuan Zhang, Yuhan Bai, Shili Sun, Hui Li, and Yintang Yang. "A secure and verifiable data sharing scheme based on blockchain in vehicular social networks." IEEE Transactions on Vehicular Technology 69, no. 6 (2020): 5826-5835.

[7] Cash, Michael, and Mostafa Bassiouni. "Two-tier permission-ed and permission-less blockchain for secure data sharing." In 2018 IEEE International Conference on Smart Cloud (SmartCloud), pp. 138-144. IEEE, 2018.

[8] Suat-Rojas, Nestor, Camilo Gutierrez-Osorio, and Cesar Pedraza. "Extraction and Analysis of Social Networks Data to Detect Traffic Accidents." Information 13, no. 1 (2022): 26.

[9] Wang, Xianmin; Huang, Zhengan; Wang, Licheng; Xiang, Yang (2019). Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing. Journal of Parallel and Distributed Computing, (), S074373151930262X–. doi:10.1016/j.jpdc.2019.04.003.

[10] Mehdi, Hamid, Zahra Pooranian, and Paola G. Vinueza Naranjo. "Cloud traffic prediction based on fuzzy ARIMA model with low dependence on historical data." Transactions on Emerging Telecommunications Technologies 33, no. 3 (2022): e3731.

[11] Kirar, Anshu, Arun Kumar Yadav, and Supriya Maheswari. "An efficient architecture and algorithm to prevent data leakage in Cloud Computing using multi-tier security approach." IEEE, 2016.

[12] Akhter, AFM Suaib, Mohiuddin Ahmed, AFM Shahen Shah, Adnan Anwar, and Ahmet Zengin. "A secured privacy-preserving multi-level blockchain framework for cluster based VANET." Sustainability 13, no. 1 (2021): 400.

[13] Hegde, Nayana, and Sunilkumar S. Manvi. "Mfzkap: Multi factor zero knowledge proof authentication for secure service in vehicular cloud computing." pp. 1-6. IEEE, 2019.

[14] Yu, Xiang, Zhangxiang Shu, Qiang Li, and Jun Huang. "BC-BLPM: a multi-level security access control model based on blockchain technology." China Communications 18, no. 2 (2021): 110-135.

[15] Aghili, Seyed Farhad, Mahdi Sedaghat, Dave Singelée, and Maanak Gupta. "MLS-ABAC: efficient multi-level security attribute-based access control scheme." Future Generation Computer Systems 131 (2022): 75-90.