ISRG Journal of Economics, Business & Management (ISRGJEBM)

ISRG PUBLISHERS

Abbreviated Key Title: Isrg J Econ Bus Manag

ISSN: 2584-0916 (Online)

Journal homepage: https://isrgpublishers.com/isrgjebm/

Volume – IV Issue -I (January- February) 2026

Frequency: Bimonthly

INTELLIGENT TRANSPORT FOR SMART CITIES

Dr. Elie Mina, DBA[1*], Assist. Prof. Dr. sc. Saša Petar, Ph.D.[2]

[1] Modern University for Business and Science (MUBS)

[2] University North Koprivnica, Croatia

| **Received:** 30.12.2025 | **Accepted:** 04.01.2026 | **Published:** 10.01.2026

***Corresponding author:** Dr. Elie Mina, DBA

Beirut Arab University Beirut, Lebanon

Abstract

A popular research area is internet traffic examination because it has numerous applications, basically for classifying internet traffic. Innovative technologies have been created for anticipating and identifying traffic blockage within the intelligent Internet of vehicles (IOVs). The sending of 5G technology has drawn attention to diverse computer-based scenarios. It is valuable within the setting of Smart Cities, the Internet of Things (IoT), and Edge Computing, among other frameworks. With the high number of connected vehicles, giving network security solutions for the Internet of Vehicles (IoV) isn't a minor prepare due to its decentralized administration structure and heterogeneous characteristics. Machine learning (ML) calculations have the potential to extract designs to cover security requirements better and to detect/classify malevolent behavior in a network. With the exponential development of technologies such as 5G, the Internet of things (IoT), a Cloud of Things (CoT), and dispersed Artificial Intelligence(AI) associated by means of inescapable and always-connected Machine-to-Machine (M2M) communications (5G). Using Intelligent Transportation (IT) like sensors arrangement counting smart domestic sensors, vehicular networking, climate and water sensors, smart parking sensors, surveillance objects, etc. Based on this work the researcher propose an Intrusion Detection System(IDS) for detecting Flooding attacks in vehicular scenarios. This paper proposes an energy-efficient Swarm Intelligence (SI) Internet of Vehicles (IoV)-based technique for opportunistic data collection and traffic engineering for SC management strategies.

Keywords: *IoT, Big Data, Blockchain, AI, IT, 5G, smart cities, IoV.*

DOI: 10.5281/zenodo.18204608

1. INTRODUCTION

The persistent evolution of technology plays a critical part in the advancement of clever frameworks over different spaces of city quality of life of individuals by excelling in numerous key zones: safety, sustainability, and economic development. Transportation is one key figure that essentially influences the socio-economic advancement of smart cities. (Obaidat, et al., 2016). The developing investigation of the 5G network reached in 2020 is already changing numerous viewpoints within the communications scene, the key functional drivers of 5G will unlock a broad range of opportunities, including the optimization of service delivery, decision-making, and end-user experience. (Galal & O'Halloran, 2020)

The efforts of industry and the scholarly community to find solutions to urban traffic issues (such as traffic blockage, cargo burglary, and optimized public transportation, among others) have permitted vehicles to become more than just transportation machines (Magaia et al., 2022). Advanced vehicles are equipped with novel communication gadgets (e.g., wireless antenna and cellular technology) that make it conceivable to communicate with surrounding vehicles, send and get messages, and access remote applications through an internet connection. Regarding cellular innovation, vehicles commonly utilize 4G/LTE (Long Term Evolution) or 5G (fifth-generation mobile network). A few studies have already considered the pending 6G (Zhou et al., 2021) within the vehicular setting. The vehicular network, at first referenced as Vehicular Advertisement hoc Network (VANET), has advanced into the Internet of Vehicles (IoV) (Shen et al., 2020) as a result of its integration with other advances, specifically the Internet of Things (IoT) (Lin et al., 2021). Besides, IoV has distinctive sorts of communication: Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), Vehicle to Sensor (V2S), Vehicle to Roadside Unit (V2R), Vehicle to Pedestrian (V2P), and Vehicle to Everything (V2X) (Silva et al., 2021) They have called consideration to the security necessities, since each communication sort can require diverse layers of security mechanisms.

Intelligent transportation systems (ITS) can offer early direction and legitimate traffic planning to solve this issue. IoVs (Internet of Vehicles) have played a critical part in ITS. An IOV can help gauge street network capacity through signal control, collecting real- time network traffic, viably dispersing traffic information, reducing traffic blockage, and directing traffic members. In expansion to evaluating the traffic capacity and designating street rights based on the IoV, we may too appraise the travel times of each member on the street. An activity estimate in progress can be conducted by gathering and analyzing ITS data to assist avoid traffic blockage. Network action categorization could be a way to recognize between network applications and related traffic most valuable in the current traffic network organization and security systems. IoT traffic, made up of heterogeneous gadgets connected in different ways, presents a challenge to network monitoring and administration frameworks. Then once more, traffic information collection is a progressed methodology that organizes traffic agreeing to different prerequisites and parameters. Application-related classification of network traffic is fundamental for securing networks. The classification can be connected to the diverse information sorts, centering on network traffic such as portable networks, IoT networks, smart cities (Shafiq et al., 2020), and information on traffic.

Although vehicles have less computing assets (e.g., processing power or capacity) than conventional computers, they have caught the consideration of pernicious clients who can adjust the technique of computer-based attacks (e.g., Denial-of-Service (DoS), Sybil, Jamming, Fuzzy, Spoofing, and Eavesdropping) to vehicular systems. In expansion, vehicular systems have the potential to create profitable information from their clients (e.g., tracking vehicles' courses, Global Position System (GPS) facilitates, vehicles' personality, or most visited places) that can also be important for malevolent users. (Ahmed et al., 2021, Lin et al., 2021)

Moreover, as the number of vehicles participating in IoV keeps developing, the expanding network latency and framework throughput will become intense to bargain with (Xie et al., 2020). All vehicles act as hubs in dispersed trust administration frameworks. The appraisals of the trustiness of vehicles are updated, and the information are stored in a distributed way. Blockchain is developing as a potential strategy to handle the trust evaluation for vehicle networks with progressed trust assessment execution, greater capability, and data transparency. Blockchain is inalienably suited for dispersed trust administration in Internet of Vehicles due to its decentralization, invariance, traceability, and namelessness features (Liu et al., 2020).

Wang et al., 2021 outline a few blockchain applications regarding get to control, message approval, trust administration, certificate administration, information administration, monetization of IoV information and security protecting through blockchain within the vehicular environment. Ravi et al. execute the strategy for security whereas fulfilling the client. Aung et al., 2022 conduct a writing considers on the utilize of blockchain to IoV in specific and intelligent transportation frameworks in common.

The future smart cities and smart ports require ICT technologies as a center to be able to handle the inventive smart city challenges. These ICT innovations must join a strong, sustainable, and profoundly leveraged network that gives network, smartness, security, and effective vitality administration. Within the following, the most contributing technologies are discussed. They are IoT, CoT, Big data, Blockchain, 5G, Artificial intelligence (AI), and Intelligent Transportation (IT).

2. Literature review

By 2050, 70 percent of the population will be expected to live in urban areas while only 30 percent will be living in rural areas. (United Nations, 2018). Literature reveals that society is faced with a large number of security issues, justifying the need for Smart Cities to continue thinking about ways to address the problem. The increment within the urban populace increments the require for mobility and the expanding utilization of nourishment and energy. This leads to an increment in living costs, the misfortune of time (e.g. in traffic), and the improvement of poor living habits. The solution to these issues lies within the concept of smart cities and advanced technologies.

2.1.1 Technologies for Smart Cities.

The future smart cities require ICT technologies as a center to be able to handle the inventive smart city challenges. These ICT innovations must join a strong, sustainable, and profoundly leveraged network that gives network, smartness, security, and effective vitality administration. Within the following, the most contributing technologies are discussed. They are IoT and CoT, Big data, Blockchain, Artificial intelligence (AI), Intelligent

DOI: 10.5281/zenodo.18204608

Transportation (IT), 5G technology, Smart City Technologies and Services (SCTS), Cyber Security, IoV and smart sensors deployment.

2.1.2 Internet of Things (IoT) and Cloud of Things (CoT)

Internet of Things (IoT) alludes to the linkage and associations among billions of distinctive objects over the web to create a smart environment. Based on standardized communication conventions, these gadgets share and trade data over heterogeneous stages. Thus, IoT upgrades the interactivity and the effectiveness of basic frameworks such as those utilized in transportation, security, instruction, agriculture, and healthcare. The IoT is considered another huge step within the advancement of the Web. The CoT is imperative within the smart zone and small smart city settings since IoT gadgets deliver a gigantic amount of data that must be stored and prepared. In basic terms, a CoT could be a pool of assets and calculation capabilities open through the Web. For smart cities combining IoT and CoT is significant, so that IoT information can be prepared and stored. Combining the pieces, an advanced ICT-based framework must include technologies such as 5G, IoT, CoT, and AI. Particularly, the AI portion is challenging since it is inserted into the IoT setting, which offers restricted assets. (Gubbi, et al., 2013).

2.1.3 Big data

The utilization of IoT and other future web innovations give a gigantic sum of data (Big Data). This information ought to be appropriately analyzed and overseen to extricate designs, which are useable for applications, services, and integrated ICT approaches like public health, public data frameworks, city administration, energy proficiency, transport, security, and crisis services, squander administration, and water management. Common for these services is that the information requires procurement, capacity, and handling on either a nearby smart city server or on a cloud preparing stage. Handled information can be utilized for creating new services such as smart economy, smart governance, smart environment, and smart portability. (Feng, 2020). Big Data has three characteristics as volume, speed, and diversities. A Big Data activity volume may be Petabytes or Exabytes constituted from billion or trillions of bits of information from millions of individuals or hardware. The volume of M2M traffic approaches 5013 petabytes by 2019 (**Figure 1**).

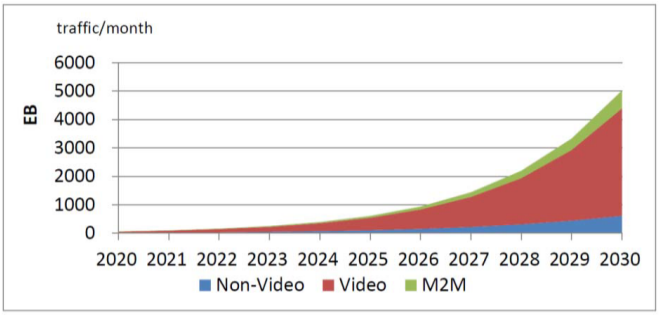


Figure 1:Mobile Estimation. (Report ITU- Report M.2370-0 , July 2015)

2.1.4 Blockchain to secure IoT.

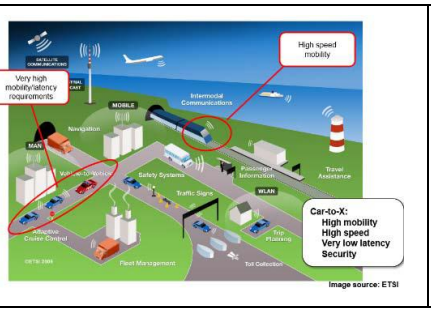
As of late, Blockchain innovation has pulled in the consideration of analysts in totally different zones. Zheng, et al. (2018), have characterized the blockchain as "a grouping of pieces, which holds a total list of exchange records like customary open ledger". Blockchain was presented to back the usage of security techniques, but it has found employments in numerous other areas and zones of application as well. To improve the security of IoT applications, the thought of receiving blockchain with IoT applications was proposed. (Fernández, et al., 2018). For smart cities, blockchain makes a difference to construct a secured environment for their applications by adopting decentralized designs. (Ali, et al., 2018). Blockchain smart contracts are promising and advantageous innovations that can be utilized to manage forms between benefit suppliers and clients. (Portmann, 2018).

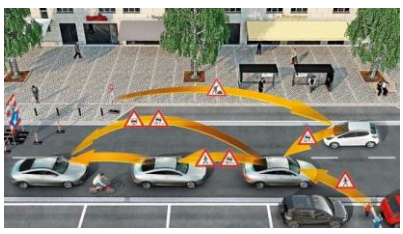
2.1.5 Artificial Intelligence (AI).

Artificial Intelligence (AI) could be a generalized term utilized to portray a framework that shows the properties of human intelligence. An Advanced AI (AAI) framework is required for handling complex IoT designs, by combining AAI frameworks, utilizing 5G to get to the Web, the ICT premise for a smart city is made as an Integrated Smart Home and Smart City (ISHSC) (Panch, et al., 2018). The application zone for AI covers a wide run of applications such as toys, logical investigation instruments, medical determination, and robot control. In expansion, numerous of today's administrations are based on inserted AI, cases are self-navigating, recommender motors, gaming motors, cars gearboxes, discourse acknowledgment, and mechanical robots. Smart situations within the smart zone have to actualize context-aware services that can bargain with everyday exercises, such as preparing, eating, drinking, taking pharmaceuticals and cooking, etc. These frameworks must be able to interface with hundreds or indeed thousands of sensors. (Feng, 2020).

2.1.6 Intelligent Transportation (IT).

Intelligent Transportation (IT) incorporates three sorts: vehicle to individuals, vehicle to vehicle, and vehicle to the framework which are named to V2X. V2X empowers the drivers to be educated of plausible threats and mischances on the street. (**Figure 2**)





DOI: 10.5281/zenodo.18204608

(a) M2M interactions.	(b) Smart vehicle.	(c) V2X.
Figure 2. Intelligent transportation (V2X). (Maeder, A., 2011, Djahel & Hadjadj-Aoul, 2020)		

Figure 2 appears distinctive scenarios of intelligent transportation (IT). (a) portrays that how vehicle speeds and ways are observed. (b) portrays a smart vehicle that's able to transmit/receive video spilling on the display and creates real-time alarms for security and controlling the vehicles. (c) appears that the vehicle may alter the way /speed agreeing to the bumpy street. Signals trade between vehicle and vehicle/station/passengers.

2.1.7 5G Technology.

The 5G organize is the fifth generation of remote broadband systems, advertising speeds, and reliability that outperform its 2G, 3G, and 4G forerunners. 5G is based on the utilization of a building structure joining the customary macro-cellular organize with an overlay of little cell networks. This permits clients to connect to two systems at the same time. The double network permits the macro-cellular arrangement to act as the control plane and the little cells to act as the client plane. The control plane is dependable for signaling between networks and the client plane is allotted for information services (e.g. video spilling or calls). (Osseiran, 2022, Galal & O'Halloran, 2020, Marek, et al., 2019).

2.1.8 Smart City Technologies and Services (SCTS)

Smart Cities utilize Wi-Fi frameworks, to begin with, give free Web get to and or give data to those entering a certain zone. This, in turn, implies information is made concerning portable phones that have entered a specific space. (Galič, 2018) Such information can be utilized in criminal investigations when we are fascinated by the development of a given individual, or when a certain timeline must be built up. It can moreover be utilized to transmit significant data such as Golden cautions or data on lost or needed people. Communication channels, in the event, that is successful, can decrease disappointment with the city or public organization. The choice of the region, time, and frame of innovation can be based on crime measurements, criminology grant as well as a run of other information (mobile phone information, social media examination, etc.) (Meijer & Thaens, 2018).

2.1.9 Cyber security and privacy

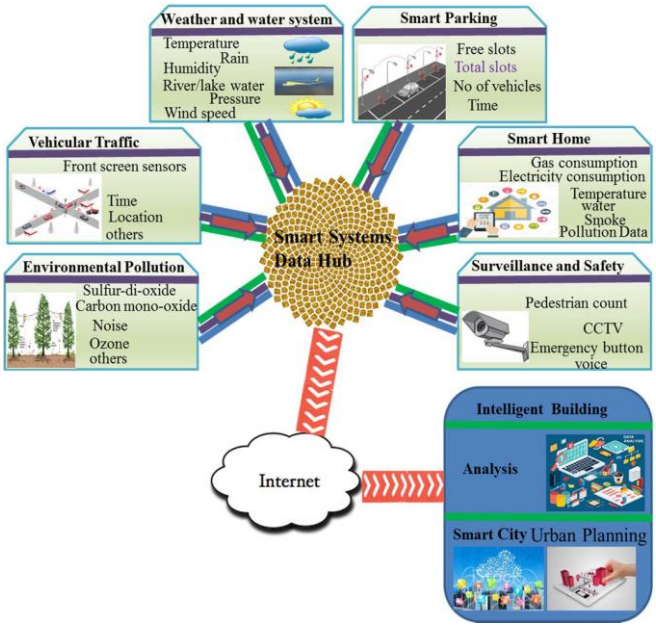
Expanded surveillance and data-driven policing raise concerns almost continuously observed and the potential to hinder political disagreement. Governments and private-sector players presently hold and share touchy individual information, making it basic to set up astute conventions and shields around its dealing with and protection. The IoTs gives a broad surface area for hackers to assault. Cities will have to create cyber security skills and remain side by side with the continually advancing dangerous environment. They will get to get ready for how to reply to breaches-including not as it were specialized remediation but how they will keep up calm and how they will communicate. (McKinsey, 2017)

2.1.10 IoV Based Design for Smart cities

The network between vehicles and the IoT has driven to a modern time of innovative progressions in terms of vehicular systems known as the IoV, which portrays a worldwide convergence of the traditional IoT and the portable internet, whereby vehicles serve as smart moving hubs within the network. The authors of, (Ijemaru et al., 2022, Ang et al., 2018) conceive of the IoV as a technological stage that empowers a network of intelligent between vehicles and other gadgets or objects inside their environment, which may incorporate other vehicles, sensors actuators, people, and street framework. IoV-based innovation gives a gigantic network of intelligent among the different communication models exploiting IoT-based innovations to empower huge data on smart waste containers scattered inside an SC environment and the collection and transmission of such information utilizing vehicular systems. A few application specifics of IoV for SC solutions can be found within the ranges of huge information analytics, infotainment, intelligent transportation frameworks, cloud computing, crash reaction, environmental administration, and traffic administration. (Sadiku et al., 2018, Silva et al., 2017)

2.1.11 Smart Sensors Deployment.

The essential concept of the smart city is to induce the right data at the correct place on the device at the right time to create the city-related choice with ease and to encourage the citizens in speedier and fast ways. To create the IoT-based smart city, we sent a few remote and wired sensors, observation cameras, emergency buttons inroads, and other settled devices. The most challenge is to attain a smart city framework and connect smart system created information at one place. We do this by putting the most data center connecting all smart framework to have them at a central place. (**Figure 3**, shows the Sensors Deployment and smart framework sending in arrange to produce information employing a central hub for building the smart city).



In arrange to urge Real-time city information, we proposed to send numerous sensors at diverse places to realize smart homes, smart parking, weather and water systems, vehicular traffic, environment population and surveillance system. These frameworks are used by the authorities to create clever choices based on the real-time information to set up the smart city. These systems are used with the technological improvement of the living environment in arrange to offer back to occupants and progress their quality of life. (Balasubramanian, & Cellatoglu, 2008)

Smart Cities has been created to make a stronger maintainable and cost productive urban environment. The thought has picked up energy with the realization that megacities will have challenges such as make maintainable and cost effective situations,

DOI: 10.5281/zenodo.18204608

improvement of life quality for the citizens and being able to handle non static concepts over time. Smart parking makes a difference in overseeing the vehicles coming and going out of diverse car parking zones. Weather and water framework gives the climate-related information like temperature, rain, humidity, weight, wind speed, and water levels at waterways, lakes, dams, and other stores. Within the world, most of the surges happen due to rain and so also a few by snow dissolving and dam breakage. The new ruling shape of communication, M2M includes the challenge to form the IoTs context-aware, brilliantly, and able to communicate through IP, and combining them into a distributed framework for future smart homes and smart cities. (Commision of the EC, 2009).

Vehicular traffic data is the foremost critical source of a smart city. Through this sort of information source and with valuable real-time examination the citizen and as well the government can get more benefits. In smart city framework, it getting the activity data by GPRS, vehicular sensors, as well as the sensors set on the front screen of the car. Additionally, in case any accident happens, the front screen will be harmed and the sensor will send the alarm to the police, traffic specialists, and clinic. Besides, a city can never be smart with unfortunate citizens. Hence, whereas planning a smart city, we put a partitioned module to urge natural information which incorporates gasses data such as specific metals, carbon monoxide sulfur dioxide, ozone, and clamor as well. The citizens are alerted when any of the poisonous gas is more within the air.

3. Related work

Related Work Conducting cyber-attacks on vehicular networks can compromise the whole communication structure between vehicles, by hindering vehicles from accepting security messages or by consuming network assets such as bandwidth, thus putting human lives at risk. The need of security instruments for vehicles can cause chaos in a city, where stopping 20% of the vehicles amid heavy traffic would be sufficient for this catastrophe to happen. Diverse studies have been conducted by the scientific community bearing in intellect the seriousness of this risk. The energetic nature of these networks presents characteristics that cannot be overlooked, such as high portability, the number of vehicles in a given zone, and connection time. Attacks on in-vehicle communications, such as espionage, infusion, bus-off, and DoS attacks, point to cause Engine Control Unit (ECU) breakdowns (Hackers, 2023, El-Rewini et al., 2020, Puri et al., 2020, Magaia & Sheng, 2019).

As a result, Kerrache et al. (2018) give a Trust-Aware Communication Architecture for Social IoV (TACASHI). On a consortium blockchain that guarantees certainty in both on-chain information and off-chain information, Chen et al. (2019) recommend a quality-focused sold reward instrument. With an accentuation on the aforementioned variables, such as measurement of weights, measurement of edge, noncompliance detection, etc., Siddiqui et al. (2021) look at state of the art in IoV trust administration by firstly going over the recent appraisals on the security of driving environment and then examining the threats to security and trust within the setting of vehicles, at last categorizing and assess the best methodologies for overseeing the trust for the IoV, proposing a new scientific classification. A few analysts concentrate on utilizing blockchain innovation to address the IoV's information administration issues.

Ravi et al. (2021) execute fitting cryptographic algorithms whereas including rewards to the client. To discover surmised answers, Xu et al. (2022) propose a randomized strategy. The edge server arrangement methodology is studied for IoVs to cover more vehicle hubs. Hildebrand et al. (2022) highlight the foremost recent advancements in Blockchain-enabled IoVs (BIoV), with an accentuation on their applications, such as swarm checking, energy exchanging, urban traffic diminishment, collision and accident anticipation, etc.

Tangade et al. (2019) connected DL in vehicular systems, highlighting the possibility of expanding reliability, diminishing latency, and detecting security issues. The particularities of an inter-vehicle network can directly influence the accuracy of building an ML model. For illustration, each vehicular environment has its possess heterogeneous characteristics (e.g., number of hubs, network topology, and available assets) that can influence how the ML model will respond to the behavior of the whole network Looking for to supply public datasets, Gonçalves et al. (2020, 2021) produced distinctive datasets for IoV, where they performed DoS and Fabrication attacks (i.e., false acceleration, speed, and direction information). Pointing to approve the created information sets, they proposed a hierarchical IDS that uses ML algorithms to identify malicious behaviors within the network.

Within the setting of Smart cities and electric vehicles, Aloqaily et al. (2019) proposed the identification of Probing, User to Root (U2R), Remote to User (R2U), and DoS attacks in Connected Vehicular Network (CVN) utilizing an IDS. The technique utilized comprised of grouping vehicles into clusters (Zhang et al., 2021), for which the algorithm chooses a cluster head (CH) that is mindful for communicating with the Trusted Third Parties (TTP) that are not accessible within the cluster. They utilize Deep Belief Network (DBN) and Decision Tree (DT) algorithms for recognizing and classifying peculiarities. Within the proposed IDS, the researches utilize a hybrid dataset. For the classification of anomalous or ordinary behavior, the network data packets are prepared by the DBN algorithm, which points to decrease unnecessary network data packets.

The related work portrayed over lacks discussion on non-trivial issues in ML, such as information dispersion and how the information are adjusted among classes. These are critical subjects, since ineffectively dispersed and/or unequal datasets can posture genuine difficulties to legitimate model training and resulting execution. Besides, most of the related work moreover appears to totally disregard the convenience of the best and most interpretable ML models, such as decision trees, and how appropriate parameter settings can move forward the quality of the models when respected through distinctive measurements.

4. CONCLUSION.

In conclusion that the first light of the 5G network presents the opportunity for the improvement and execution of technologies that hold the potential to address numerous of the current boundaries to the conveyance of specialist eye care to the worldwide populace. The technologies created may play a key part intending to current challenges, counting holding up times, costs related with care, social suitability, geographic populace, and specialist dispersion. The recommended ISHSC framework is based on a four-layer demonstrate consolidating developing progress in 5G frameworks, Internet of Things, Intelligence Transport and Progressed Artificial Intelligence. These potential

DOI: 10.5281/zenodo.18204608

improvements presuppose arrangements to a push of socio-technological challenges counting different zones such as 5G communication technologies, dispersed AI, IoT-based services, security, belief, and privacy. Arrangements to these will require gigantic investigation efforts utilizing inventive standards, techniques, and strategies. The laid out framework is inherently a user-centric framework that will give a stage for a new eco-system based on modern socio-economic structures.

The smart city includes a major effect on the country's economy. A solid and smart city framework helps in taking fast and clever choices. This paper centers on the execution of the smart city by the utilize of the IoT-based smart framework. Different smart systems are utilized to urge real-time city information to create a decision. The ecosystem is utilized to handle Big Data created by all the smart frameworks conveyed within the city. The Framework is essentially actualized and tried on genuine information.

The researcher proposed a data management paradigm for blockchain-enabled Internet of Vehicles in smart cities. A vehicle–road–cloud architecture is constructed through which data are generated, disseminated, and stored. The choice of the innovative GWD-PBFT-PoT (Grouped, Weighted, and Decayed Practical Byzantine Fault Tolerance and Proof of Trust) consensus algorithm is justified by a comprehensive review of the viability of employing blockchain technology to record IoV data. Comparative experiments with the original PBFT and other derivative algorithms show the system's overall efficiency can be increased while retaining security and availability.

Vehicle registration and subsequent validation. Providing a safer and more reliable process for vehicle registration and subsequent verification of its legal identity will further improve the security of the system. Also Multi-dimension data-based vehicle score. As the traffic information and vehicle-related data in smart cities keep increasing, better models could be trained on those multi-dimension data to evaluate vehicle more precisely. Low-score vehicles are untrustworthy and will leave IoV if their scores are below a certain threshold. High-score vehicles have higher voting rights and thus are more likely to get bookkeeping rights in a blockchain-enabled IoV. Farther more Handling enormous quantitative data. Although GWD-PBFT-PoT outperforms other consensus algorithms like PoW, POS, and PBFT in terms of throughput and consensus latency, it is still unable to handle the massive increase in data volume and high concurrent requests in the fields of technology and Artificial Intelligence

References

1. 'Hackers' Podem Usar Automóveis para Paralisar uma Cidade. Available online: https://www.motor24.pt/noticias/hackerspodem-usar-automoveis-para-paralisar-uma-cidade/666001 (accessed on 20 August 2023).
2. Ahmed, I.; Ahmad, A.; & Jeon, G. (2021). Deep Learning-based Intrusion Detection System for Internet of Vehicles. IEEE Consum. Electron. Mag., 12, 117–123. [CrossRef]
3. Ali, M., Vecchio, M., & Pincheira, K.D. M. (2018). Tutorials, Applications of blockchains in the internet of things: A comprehensive survey, IEEE Commun.Surv. Tutor., 1676-1717, https://ieeexplore.ieee.org/abstract/document/8580364/. (Accessed 25 July 2022)
4. Aloqaily, M.; Otoum, S.; Al Ridhawi, I.; & Jararweh, Y. (2019). An intrusion detection system for connected vehicles in smart cities. AdHoc Networks, 90, 101842. [CrossRef]
5. Ang, L.M.; Seng, K.P.; Ijemaru, G.K.; & Zungeru, A.M. (2018). Deployment of IoV for smart cities: Applications, architecture, and challenges. IEEE, 7, 6473–6492. [CrossRef]
6. Aung, N., Kechadi, T., Dhelim, S., Zhu, T., Berini, A. D. E., & Guerbouz, T. (2022). Blockchain Application on the Internet of Vehicles (IoV). arXiv preprint arXiv:2205.03832.
7. Balasubramanian, K., & Cellatoglu, A. (2008). Improvements in home automation strategies for designing apparatus for efficient smart home, Consumer Electronics, IEEE Transactions on, vol. 54, no. 4, 2008, pp. 1681-1687.
8. Chen, W., Chen, Y., Chen, X., & Zheng, Z. (2019). Toward secure data sharing for the IoV: A quality-driven incentive mechanism with on-chain and off-chain guarantees. IEEE Internet of Things Journal, 7(3), 1625-1640.
9. Commision of the EC. (2009). Internet of Things - An action plan for Europe, EU, Brussels.
10. Djahel, S., & Hadjadj-Aoul, Y. (2020). 5G enabled CAVs for Smart and Sustainable Mobility in Smart Cities, IEEE International Smart Cities Conference (ISC2), Virtual, United States.hal-03140839. https://hal.inria.fr/hal-03140839.
11. El-Rewini, Z.; Sadatsharan, K.; Selvaraj, D.F.; Plathottam, S.J.; & Ranganathan, P. (2020) Cybersecurity challenges in vehicular communications. Veh. Commun., 23, 100214. [CrossRef]
12. Feng, Y. (2020). Research on the Application of Big Data and Artificial Intelligence Technology in Computer Network Technology, International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS), IEEE, Vientiane, Laos. DOI 10.1109/ICITBS49701.2020.00117.
13. Fernández-Caramés, T., & Fraga-Lamas, P. (2018). A review on the use of blockchain for the internet of things, IEEE Access 6, 32979-33001, https://ieeexplore.ieee.org/abstract/document/8370027/. (Accessed 20 July 2022).
14. Galal, H., & O'Halloran, D. (2020). The Impact of 5G: Creating New Value across Industries and Society, World Economic Forum, 91-93, route de la Capite, CH-1223 Cologny/Geneva, Switzerland.
15. Galič, M. (2018). Living laboratories and Big Data in practice: Stratumseind 2.0 - debate on a living lab in the Netherlands, 85-110.
16. Gonçalves, F.; Ribeiro, B.; Gama, O.; Santos, J.; Costa, A.; Dias, B.; Nicolau, M.J.; Macedo, J.; Santos, A. (2020). Synthesizing Datasets with Security Threats for Vehicular Ad-Hoc Networks. In Proceedings of the GLOBECOM 2020-2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11; Volume 2020. [CrossRef]
17. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural elements, and future directions, Future Gener. Comput.

DOI: 10.5281/zenodo.18204608

Syst. 29, 1645-1660, https://doi.org/10.1016/j.future.2013.01.010.
18. Hildebrand, B., Baza, M., Salman, T., Amsaad, F., Razaqu, A., & Alourani, A. (2022). A Comprehensive Review on Blockchains for Internet of Vehicles: Challenges and Directions. arXiv preprint arXiv:2203.10708.
19. Ijemaru, G.K.; Ang, L.M.; &Seng, K.P. (2022). Transformation from IoT to IoV for waste management in smart cities. J. Netw. Comput., 204, 103393. [CrossRef]
20. Kerrache, C. A., Lagraa, N., Hussain, R., Ahmed, S. H., Benslimane, A., Calafate, C. T., & Vegni, A. M. (2018). TACASHI: Trust-aware communication architecture for social internet of vehicles. IEEE Internet of Things Journal, 6(4), 5870-5877.
21. Lin, Z., Lin, M., De Cola, T., Wang, J.B., Zhu, W.P., & Cheng, J. (2021). Supporting IoT with rate-splitting multiple access in satellite and aerial-integrated networks. IEEE Internet Things J., 8, 11123–11134. [CrossRef]
22. Liu, D., Ni, J., Huang, C., Lin, X., & Shen, X. S. (2020). Secure and efficient distributed network provenance for iot: A blockchain-based approach. IEEE Internet of Things Journal, 7(8), 7564-7574.
23. Maeder, A. (2011). How to deal with a thousand nodes: M2M communication over cellular networks," NEC.
24. Magaia, N. & Sheng, Z. (2019). ReFIoV: A novel reputation framework for information-centric vehicular applications. IEEE Trans. Veh. Technol. 2019, 68, 1810–1823. [CrossRef]
25. Magaia, N., Ferreira, P.,Pereira, P.R., Muhammad, K., Del Ser, J., & De Albuquerque, V.H.C. (2022) Group'n Route: An Edge Learning Based Clustering and Efficient Routing Scheme Leveraging Social Strength for the Internet of Vehicles. IEEE Trans. Intell. Transp. Syst. 2022, 23, 19589–19601. [CrossRef]
26. Marek, S. (2019). Marek's Take: making 5G work indoors is a huge task for operators. New York (USA): Fierce Wireless, https://www.fiercewireless.com/wireless/marek-s-take-making-5g-work-indoors-a-huge-task-for-operators. (Accessed 30 July 2022).
27. McKinsey & Company. (2017). Six ways CEOs can promote cybersecurity, mckinsey.com/mgi.
28. Meijer, A., & Thaens, M. (2018). Quantified street: Smart governance of urban safety, Information Polity, 23(1), 29-41.
29. Obaidat, M. S., Nicopolitidis, P., & Morgan Kaufmann Eds. (2016). Smart Cities and Homes: Key Enabling Technologies, https://www.elsevier.com/books/smart-cities-and-homes/obaidat/978-0-12-803454-5. (Accessed 30 July 2022).
30. Osseiran, A. (2022). 5G beyond the hype, Ericsson Business Review, vol. 2. https://www.ericsson.com/en/reports-and-papers/white-papers/5g-wireless-access-an-overview.
31. Panch T., Szolovits, P., & Atun, R. (2018). Artificial intelligence, machine learning, and health systems. J Glob Health.;8:020303, DOI: 10.7189/jogh.08.020303.
32. Portmann, E. (2018). Blockchain: Blueprint for a New Economy, Springer Fachmedien Wiesbaden GmbH, 2018, DOI: 10.1365/s40702-018-00468-4.
33. Puri, V.; Kumar, R.; Van Le, C.; Sharma, R.; & Priyadarshini, I. (2020). A Vital Role of Blockchain Technology Toward Internet of Vehicles. In Handbook of Computer Networks and Cyber Security: Principles and Paradigms; Academic Press: Cambridge, MA, USA, pp. 407–416. [CrossRef]
34. Ravi, N., Verma, S., Jhanjhi, N. Z., & Talib, M. N. (2021). Securing VANET Using Blockchain Technology. In Journal of Physics: Conference Series (Vol. 1979, No. 1, p. 012035). IOP Publishing.
35. Report ITU- Report M.2370-0, July 2015.
36. Sadiku, M.N.; Tembely, M.; & Musa, S.M. (2018). Internet of vehicles: An introduction. Int. J. Adv. Res. Comput. Sci. Softw. Eng., 8, 11. [CrossRef]
37. Shafiq M, Tian Z, Bashir AK, Jolfaei A, & Yu X. (2020). Data mining and machine learning methods for sustainable smart cities traffic classification: a survey. Sustain Cities Soc; 60:102177. https://doi.org/10.1016/j.scs.2020.102177.
38. Shen, X., Fantacci, R., & Chen, S. (2020). Internet of Vehicles. Proc. IEEE, 108, 242–245. [CrossRef]
39. Siddiqui, S. A., Mahmood, A., Sheng, Q. Z., Suzuki, H., & Ni, W. (2021). A survey of trust management in the internet of vehicles. Electronics, 10(18), 2223.
40. Silva, L., Magaia, N., Sousa, B., Kobusin´ska, A., Casimiro, A., Mavromoustakis, C.X., & Mastorakis, G. (2021). De Albuquerque, V.H. Computing Paradigms in Emerging Vehicular Environments: A Review. IEEE/CAA J. Autom. Sin., 8, 491–511. [CrossRef]
41. Silva, R.; Bonnin, J.M.; & Ernst, T. (2017). An ITS-based Architecture for Opportunistic Networking. In Proceedings of the VEHICULAR: The Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications, Nice, France, 23–27.
42. Tangade, S.; Manvi, S.S.; & Hassan, S. (2019). A deep learning based driver classification and trust computation in VANETs. In Proceedings of the 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), Honolulu, HI, USA, 22–25. [CrossRef]
43. United Nations, 68% of the world population is projected to live in urban areas by 2050, (2018), https://www.un.or/developent/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html. (Accessed 25 July 2022).
44. Wang, C., Cheng, X., Li, J., He, Y., & Xiao, K. (2021). A survey: applications of blockchain in the internet of vehicles. EURASIP Journal on wireless communications and networking, 2021(1), 1-16.
45. Xie, S., Zheng, Z., Chen, W., Wu, J., Dai, H. N., & Imran, M. (2020). Blockchain for cloud exchange: A survey. Computers & Electrical Engineering, 81, 106526
46. Xu, L., Ge, M., & Wu, W. (2022). Edge server deployment scheme of blockchain in IoVs. IEEE Transactions on Reliability, 71(1), 500-509.
47. Zhang, D.; Gong, C.; Zhang, T.; Zhang, J.; & Piao, M. (2021). A new algorithm of clustering AODV based on

DOI: 10.5281/zenodo.18204608

edge computing strategy in IOV. Wirel. Netw., 27, 2891–2908. [CrossRef]

48. Zhou, X., Liang, W., She, J., Yan, Z., & Wang, K. (2021). Two-Layer Federated Learning with Heterogeneous Model Aggregation for 6G Supported Internet of Vehicles. IEEE Trans. Veh. Technol., 70, 5308–5317. [CrossRef]

DOI: 10.5281/zenodo.18204608