



Fusing Type -2 Neutrosophic in Decision-Making Methodology for Appreciation Blockchain Capabilities in Securing Environment of Vehicles Fog: Practice Realistic Scenarios

Alaa Salem ¹, and Mona Mohamed ^{2*}

¹ Faculty of Computers and Informatics, Zagazig University, Zagazig 44519, Egypt; as.ata23@fci.zu.edu.eg.

<https://orcid.org/0009-0009-9628-862X>;

²Higher Technological Institute, 10th of Ramadan City 44629, Egypt; mona.fouad@hti.edu.eg, <https://orcid.org/0000-0002-8212-1572>

Abstract

Right now, Contemporary technologies have become imperative in many domains to achieve societal safety. As is practiced in transportation systems through merging information and communication technologies (ICTs) in transportation to be an intelligent sector. As well Internet of Vehicles (IoVs) for facilitating communication between vehicles for safe driving. Similarly, fog computing in Vehicular Ad Hoc Networking (VANET) contributes significantly to addressing timing and latency issues by enabling cloud services for nearby vehicles. Nonetheless, there are hazards of cyber-attacks on vehicles in VFN, which makes it uneasy to disclose personal information to unidentified fog devices. Consequently, an online criminal might target vehicles with counterfeit attacks. Herein, blockchain technology (BCT) is another technology of ICTs and is provided in this study as a handler for the problem of cyber-attacks. Due to BCT's characteristics of permanent, or immutable, peer-to-peer, decentralized, and distributed ledger technology. Thereby, this study contributes to constructing an appraiser model for appraising BCT as the secured methodology in VFN. Multi-criteria decision-making (MCDM) techniques such as entropy and weighted sum method (WSM) have been harnessed in the appraising process motivated by the uncertainty theory of Type-2 neutrosophic sets (T2NSs). The appraiser model's findings indicated that BCT 5(A5) was the optimal candidate based on its ranking. In contrast, BCT 4 (A4) is the worst one.

Keywords: Vehicular Ad-hoc Networks (VANET); Internet of Vehicles (IoVs); Vehicular fog network (VFN); Blockchain Technology (BCT); Multi-Criteria Decision Making; Type-2 Neutrosophic

1. Introduction

There are more accidents and problems with traffic congestion these days due to the massive growth in the number of vehicles on the road. This highlights the necessity for significant planning to guarantee traffic efficiency and road safety. Various technologies have been implemented to promote safer and more efficient driving on roads. One such technology is the Vehicular Ad-hoc Network (VANET), which allows vehicles to exchange information about their location, speed, and other road-related parameters. This increases the vehicles' awareness of the conditions of the surrounding roads and facilitates the making of more informed and timely decisions [1]. Up until recently, VANET's primary goal was to gather and share

data with other drivers to improve comfort and safety for drivers in a moving vehicle environment [2]. But VANET is quickly evolving into a transportation network where intelligent cars with integrated sensors, adapters, and control units may effectively communicate with nearby cars in addition to monitoring their environment [3]. The main issues with connected Vehicles in VANET are privacy and security. Vehicle data security can be easily breached by anyone with a connection to a vehicle, such as an owner, mechanic, or member of the governmental staff. Data validation, access control, device and network security, and driver and vehicle privacy are among the potential security risks that attackers may exploit [4]. As such, creating privacy and security solutions for connected Vehicles in VANET is a more difficult task. But as today's technologies—such as cloud computing platforms, wireless technologies, sensor devices, and smart cars—develop more quickly, the demand for stronger vehicular networks has grown. Thus, the Internet of Vehicles (IoVs) emerged, able to take advantage of and integrate all these cutting-edge technologies to offer drivers and passengers of automobiles more rewarding real-time services [1]. IoVs are a next-generation wireless roadside system that is rapidly expanding [1]. A variety of vehicle interactions are now possible thanks to recent developments in sensor and communication technologies such as vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-roadside units, vehicle-to-mobile-infrastructure, vehicle-to-sensors, and vehicle-to-personal devices [5]. IoVs idea seeks to establish a networked infrastructure for the exchange of resources and information among smart vehicles, hence enabling the advancement of the Intelligent Transportation System (ITS). IoV will enable continuous connectivity between vehicles, roadside infrastructure, and pedestrians, and will increase the number of intelligent and linked automobiles in IT [6]. IoV is developing more quickly because of ongoing advancements in intelligent vehicle technology. Data exchange and interaction in the IoV is currently a popular area of study. Road data, car-generated data, data supplied by other nodes, etc. are all included in the vehicle interaction data [7]. By supplying connected Vehicles with services like storage, infrastructure, and increased processing capacity, cloud computing enables them to be charged by their needs [5]. Numerous dangers, including identity theft, denial of service, access control, data breaches, and data loss, affect cloud computing. By employing devices that can provide cloud computing's characteristics to the necessary vehicle, fog computing extends the functionality of cloud computing to the network's edge [6]. Consequently, vehicular fog network (VFN) refers to the network that has been integrated with IoVs and fog devices. The fact that VFN stores all its data on a single, centralized cloud server creates serious security risks since if one of the entities is compromised, the entire system is at risk. The disadvantage of one entity being hacked is eliminated by Blockchain (BC) technology, which is dispersed and decentralized. To write and validate transactional data and transport all verified transactions in a block, it works with numerous connected vehicles [7].

2. Comprehensive Review of Earlier Insights

In recent years, numerous technical methods have been presented by numerous researchers to improve IoT performance. Because of its distinct qualities, IoVs is one of the main subjects of literature studies among them [8]. Vehicles in IoV process a lot of data. Additionally, they use a mesh network to directly perform V2V connection and ensure reliable data flow. The data could be about simple text messages, multimedia, or proximity to a location. Ensuring network security becomes imperative to uphold user trust [9]. According to Song et al.[10], a group of vehicles with similar average speeds and directions of travel can be formed based on navigation, and intergroup communication will keep the positions of the

individual vehicles and those of other vehicles hidden. However, because of the vehicle's speed and the unpredictability of the surrounding environment, there is still a serious problem with communication between geographically independent groups of vehicles. This problem manifests itself in the form of difficult information exchange and the need to repeat the intermediate authentication process whenever a vehicle rejoins another group of vehicles [8]. To address the security concerns around the Internet of Vehicles, a novel form of BC framework has been investigated to facilitate the safe transfer of information [11]. The reliability of a node and a message were recorded in a ledger on a local public BC that the researchers built for this purpose. Authors in [12] have identified problems with passing alert messages without disclosing the sender's identity as well as a lack of imagination in cars to do so. Their proposal was for an effective incentive announcement network built on BC technology that protects anonymity, enables vehicles to operate in the network anonymously, and provides incentives for their efforts. The researchers in [13] used consortium BC and smart contract technologies in order to enable the safe exchange and storage of data within in-vehicle edge networks. These technologies work to prevent information from being shared illegally. The researchers also developed a reputation-based data-sharing strategy to guarantee that the vehicles continuously provided high-quality data. The authors in [14] built software-defined fault tolerance and quality-of-service-aware IoT-based vehicular networks using edge computing made possible by BC. This resulted in a reduction in overall communication time, message failure fault tolerance, and safe service delivery for VANET. The ability for vehicles to exchange messages is what VANET is there for. The difficulty here is that such messages must be stored and forwarded by a reliable party. An additional obstacle is that the vehicle can refuse to take part in the creation and dissemination of announcement messages unless doing so benefits it. Authors have proposed a BC-enabled safe data-sharing system for the Internet of Vehicles (IoVs) that uses a parent and auxiliary BC to store the messages by various organizations from various places in order to address this issue and provide secure communication [15]. In order to address timeliness and latency difficulties, vehicular fog networking integrates fog computing and vehicular ad hoc networking to offer cloud services to neighboring automobiles [16]. Security and privacy concerns plague vehicular fog computing [17]. Another issue is that, even though the cloud and fog service providers are reliable organizations, automobiles in VFN frequently feel uneasy disclosing private information to unidentified fog devices [18]. The internet connection of vehicles in VFN is another major factor contributing to cyberattacks. BC, a distributed, decentralized, immutable, consensus-based network, may be a useful way to address VFN's issues with cyberattacks, latency, and timeliness [19]. Despite all its benefits, BC technology is still in its infancy and many firms still have reservations. According to a PWC (PricewaterhouseCoopers) poll, the main obstacles to BC adoption include regulatory ambiguity (48%), a lack of confidence (45%), and the question of whether the BC network can be connected (44%) [20]. Therefore, are all BC services appropriate for every firm at this point? Perhaps not the answer. Each type of BCT—private, public, and community—has pros and cons of its own. Therefore, by considering both economics and other pertinent criteria, enterprises should use a scientific decision-making tool to determine which BC service provider is more appropriate [21].

2.1 Blockchain (BCT)

BC is a viable method to address challenges. BC consists of a group of interconnected blocks that are connected by certain cryptographic procedures to form a chain. The blocks store information such as

records, queries, and transactions. The digital ledger, which is updated by every network member, records every new block that is created and added to the chain. For this reason, another name for BC technology is distributed ledger technology (DLT) [22]. A BC can be classified as either public (completely dispersed and permissionless), private (permissioned, belonging to a particular organization), or consortium (federated, resembling a private BC) [23].

- **Public BC:** This BC is entirely decentralized, distributed, and permissionless, allowing any connected autonomous vehicles (CAVs) to connect to the network and view its contents. Take cryptocurrency networks like Ethereum and Bitcoin, for instance. It costs a lot of computer power to publish a new block. A processing charge is required to store a transaction on the BC.
- **Private BC:** This is a single organization-created, fully permissioned BC. The authority organization is aware of every member of the organization and does not impose any fees for transaction processing.
- **Consortium BC:** This kind of BC is comparable to a private BC, but it spans several organizations (several authorities) as opposed to just one.

BC technology eliminates the need for a central authority by enabling everyone to create and approve transactions in a peer-to-peer network, greatly lowering the time and money associated with the middleman [1].

2.2 Vehicular Fog Networking (VFN)

Cisco was coining the phrase "fog computing." The fog offers decentralized distributed computing capabilities at the edge of the network, in contrast to the cloud, which is a centralized server. Fog provides a more effective way around the restrictions of cloud computing by utilizing this feature [24]. Any device that can share resources on rent and is referred to as a fog device can provide fog functionality. Applications that need a quick reaction and are time-sensitive are the greatest candidates for fog computing [25]. One of the major uses of fog computing is the Internet IoVs; this integration is called a Vehicular Fog Network (VFN)[15]. Because vehicles do not need to send data to the cloud, a VFN has the advantages of low latency, reduced network bandwidth requirements, security, and increased reliability. Any dynamic node, such as a vehicle, or any static node, such as a router, switch, base station, or RSU, could function as a fog device in a VFN. A fog device can be hired out to the necessary cars for computation and storage because it has an underutilized infrastructure. In addition, data segregation, forwarding, and real-time decision-making for vehicular communication are all impacted by fog [26]. Even while the fog sends all the data it needs for analysis later, it communicates only the data that is needed.

The BC idea is used with VFN to increase security by storing reward point values and vehicle reliability in a traffic scenario. Furthermore, the combination of fog computing with the BC idea may be able to address the main security issues in an IoVs environments [5].

2.3 BCT in Vehicular Fog Network

Vehicular fog computing, a novel vehicular network architecture, is introduced with the BC security framework. BC security transactions are accelerated by vehicle network design and fog computing, which together offer cloud computing capabilities at the network's edge. VFN is the name of this system. Applying the BC concept to VFN increases its security by storing reward point values and vehicle trustworthiness in a traffic scenario. Additionally, fog computing and the BC idea have the potential to address the main

security issues in an IoVs environments [25]. In complex road traffic scenarios where vehicles lack confidence, BCT is well suited for decentralized application environments with distributed consensus features. Data is secure against easy manipulation by adversaries because of BC technology. Multiple service providers may be able to collaboratively manage the user's account information with the help of this encryption feature [8]. To accomplish the full identity authentication process across several servers, a user simply needs to keep track of their account details on the ledger, potentially increasing efficiency. Nevertheless, in contrast to other Internet of Things, IoVs based on BC technology allows for energy consumption to be met directly by the vehicle, avoiding the drawback of high energy consumption of the BC network [8].

BC technology is also having a significant impact on businesses that we never would have predicted would become unstable. It makes sense to research this kind of topic since the service provider selection problem in a BC system might undergo significant changes in the future. Furthermore, an enterprise's performance and success are directly correlated with the choice of suitable BC service providers. Enterprises seeking growth and development will collaborate with capable firms to create BC technology, viewing these firms as their own BC service providers [21].

3 Methodology: Appraising of Blockchain

In this study, the advantage of Entropy technique to determine the weights of criteria in MCDM problems is combined with WSM to evaluate and rank a set of BCT as security methodology. these techniques under the authority of T2NSs.

Phase 1: Problem Formulation

Step 1.1: Set of BCTs is determined as alternatives that contribute to the appraiser model. will where the alternatives are represented as BCTs = {BCT1, BCT 2, . . . , BCT m}.The determined alternatives are appraised based on a set of criteria as $C = \{C1, C2, . . . , Cn\}$ which is mentioned in Table 1 .

Step 1.2: the panel of DMs is formed for appraising the alternatives of BCTs.

Table1: Determined criteria based on blockchain technology [1]

Criteria	Description
Decentralization: C1	BC technology demonstrates a decentralized nature in which data records are held and managed by all participating entities, in contrast to centralized storage platforms where both data storage and maintenance are handled by a trusted single node. This helps VFN settings by avoiding the single point of failure problem, reducing maintenance costs related to centralized server configurations, and reducing resource constraints.
Immutability: C2	The BC is nearly impossible to tamper with or alter since the creation and validation of new blocks of transactions must be approved by all or most of the peers using various consensus procedures before being added to the BC.
Security and privacy: C3	The adoption of digital signatures and cryptographic hash functions in BC technology can guarantee the security of transaction data as well as the privacy of users taking part on the Internet of Vehicles.
Transparency: C4	All participants have access to all timestamped BC transactions since they each maintain a copy of the public ledger. As a result, peers can transparently manage, search for, and validate transactions at any moment without the need for a

	middleman. By handling their transactions, peers are relieved, and the intermediary party's time and financial expenses are also reduced because of its self-auditability and transparency.
Automation: C5	Smart contracts, which are software programs that can be launched automatically by a triggering event or upon fulfilling a predetermined set of rules, are made possible by BC technology. This BC's automation feature can allow many VFN applications operate more efficiently and provide a range of services on their own without requiring a trusted third party.
Traceability: C6	Every transaction record, along with a timestamp indicating when it occurred and was added to the public ledger, is stored in the BC. The fact that the recordings are timestamped makes it easier to identify the events in a chronological order, improving traceability and supporting VFN non-repudiation requirement.

Phase2: Generating criteria weights

Step 2.1: Construct neutrosophic decision matrices. DMs utilized the linguistic terms presented in Table2 to assess the opinions of DMs about each criterion [27]

Step 2.2: Use the de-neutrosophic Eq. (1) for transforming neutrosophic decision matrices to the crisp matrices [27].

$$S(U_1^{\sim}) = \frac{1}{12} + (8 + (T_{T_{U_1}}(z) + 2(T_{I_{U_1}}(z)) + T_{F_{U_1}}(z)) - (I_{T_{U_1}}(z) + 2(I_{I_{U_1}}(z)) + I_{F_{U_1}}(z)) - (F_{T_{U_1}}(z) + 2(F_{I_{U_1}}(z)) + F_{F_{U_1}}(z))) \tag{1}$$

Table2: Linguistic Scale

Linguistic Terms	T2N scale for < (T _T , T _I , T _F), (I _T , I _I , I _F), (F _T , F _I , F _F) >
Very Bad (VB)	<<(0.20, 0.20, 0.10),(0.65, 0.80, 0.85),(0.45, 0.80, 0.70)>>
Bad (B)	<<(0.35, 0.35, 0.10),(0.50, 0.75, 0.80),(0.50, 0.75, 0.65)>>
Medium Bad (MB)	<<(0.50, 0.30, 0.50),(0.50, 0.35, 0.45),(0.45, 0.30, 0.60)>>
Medium (M)	<<(0.40, 0.45, 0.50),(0.40, 0.45, 0.50),(0.35, 0.40, 0.45)>>
Medium Good (mg)	<<(0.60, 0.45, 0.50),(0.20, 0.15, 0.25),(0.10, 0.25, 0.15)>>
Good (G)	<<(0.70, 0.75, 0.80),(0.15, 0.20, 0.25),(0.10, 0.15, 0.20)>>
Very Good (VG)	<<(0.95, 0.90, 0.95),(0.10, 0.10, 0.05),(0.05, 0.05, 0.05)>>

Step 2.3. Eq. (2) is employed in crisp matrices to aggregate it into a single decision matrix.

$$x_{t_{ij}} = \frac{\sum_{j=1}^N s(U_i^{\sim})}{N} \tag{2}$$

Where: $S(U_i^{\sim})$ refers to value of criterion in matrix, N refers to number of decision makers

Step 2.4: Normalizing the aggregated decision matrix r_{ij} based on Eq.(3)

$$r_{ij} = \frac{x_{ij}}{\sum_{i=1}^n x_{ij}} \tag{3}$$

Where: $\sum_{i=1}^n x_{ij}$ represents sum of each criterion in aggregated matrix per column.

Step 2.5: Compute Entropy e_i for normalized matrix by Eq.(4)

$$e_j = (-h) \sum_{i=1}^n r_{ij} \ln(r_{ij}) \tag{4}$$

where $(h) = \frac{1}{\ln(n)}$; n refers to number of alternatives

Step 2.6: Calculation of variation coefficient

$$d_j = |1 - e_j| \tag{5}$$

Step 2.7: Calculation of weights

$$w_j = \frac{d_i}{\sum_{i=1}^n d_j} \tag{6}$$

Phase 3: Recommending the most secure BCT amongst BCTs

Step 3.1: Eq.s(3,8) are employed for normalizing the aggregated matrix from previous phase 2.

$$N = \frac{1}{x_{ij}} \tag{7}$$

$$Nor_{Aggj} = \frac{N}{\text{sum}(N)} \text{ , For Non - Beneficial criteria} \tag{8}$$

Step 3.2: weighted decision matrix is generated based on Eq.(9)

$$\delta_{ij} = w_j * Nor_{Aggj} \tag{9}$$

Step 3.3: Obtaining global score based on Eq.(10).

$$V(\delta_{ij}) = \sum_{j=1}^n \delta_{ij} \tag{10}$$

Where $V(\delta_{ij})$ is global score values.

4 Implementation of Appraiser Model in Realism:Case Study

To ensure the accuracy of the constructed appraiser model, we applied it to a smart city aiming for sustainable development. We are volunteering five BCTs to be candidates in this study which appraising based on six criteria have been determined in Table 1.

4.1 Weighting criteria based on entropy- T2NSs.

- Five Neutrosophic decision matrices are constructed and converted to crisp values using score function of Eq.(1).
- The de-neutrosophic matrices are combined based on Eq.(2) into a single matrix called an aggregated matrix as listed in Table 3.
- The aggregated matrix normalized according to Eq.(3) and generate normalized matrix as listed in Table 4.
- The normalized matrix is harnessed in Eq.(4) for computing entropy as in Table 5.
- Finally, Eq.(6) is applied for generating criteria weights which resulted in Table 6. Fig 1 showcases the weights of criteria where C1 has the highest value otherwise C6 has the lowest value .

Table 3: Aggregated decision matrix

	C1	C2	C3	C4	C5	C6
BCT1	0.7092	0.5617	0.5017	0.5617	0.5300	0.4725

BCT 2	0.4492	0.6008	0.6350	0.5600	0.5525	0.5067
BCT 3	0.5342	0.5175	0.6725	0.6025	0.6792	0.5967
BCT 4	0.5058	0.7208	0.5317	0.4358	0.4725	0.5400
BCT 5	0.5567	0.4617	0.5067	0.7092	0.7008	0.6183
sum	2.7550	2.8625	2.8475	2.8692	2.9350	2.7342

Table 4: Normalizing the aggregated decision matrix

	C1	C2	C3	C4	C5	C6
BCT1	0.2574	0.1962	0.1762	0.1958	0.1806	0.1728
BCT 2	0.1630	0.2099	0.2230	0.1952	0.1882	0.1853
BCT 3	0.1939	0.1808	0.2362	0.2100	0.2314	0.2182
BCT 4	0.1836	0.2518	0.1867	0.1519	0.1610	0.1975
BCT 5	0.2021	0.1613	0.1779	0.2472	0.2388	0.2262

Table 5: Compute Entropy e_j for normalize

	C1	C2	C3	C4	C5	C6
BCT1	-0.3493	-0.3195	-0.3059	-0.3193	-0.3091	-0.3034
BCT 2	-0.2957	-0.3277	-0.3346	-0.3189	-0.3144	-0.3124
BCT 3	-0.3181	-0.3092	-0.3408	-0.3277	-0.3387	-0.3322
BCT 4	-0.3112	-0.3473	-0.3133	-0.2863	-0.2940	-0.3203
BCT 5	-0.3231	-0.2943	-0.3072	-0.3455	-0.3420	-0.3362

Table 6: Compute Weight Vector

	C1	C2	C3	C4	C5	C6
$\sum_{i=1}^n r_{ij} \ln r_{ij}$	-1.5974	-1.5980	-1.6019	-1.5976	-1.5981	-1.6045
e_j	0.9925	0.9929	0.9953	0.9926	0.9930	0.9969
d_j	0.0075	0.0071	0.0047	0.0074	0.0070	0.0031
W_i	0.2030	0.1938	0.1280	0.2003	0.1911	0.0838

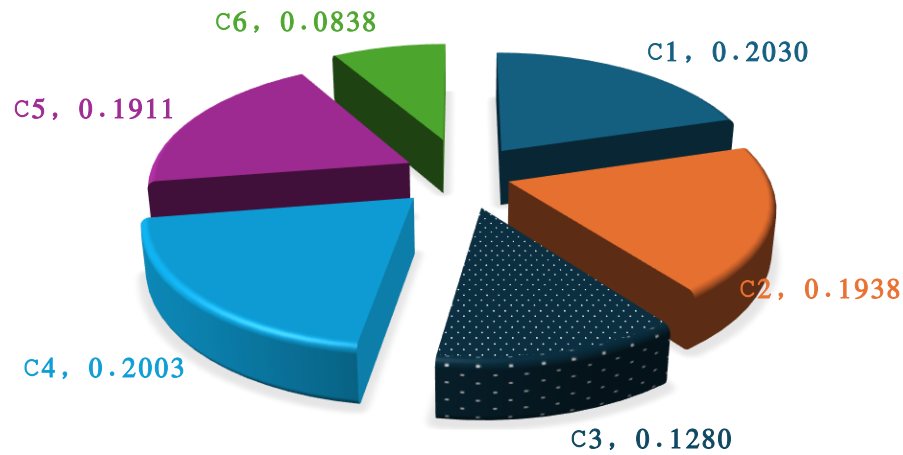


Fig 1. Final weights of criteria

4.2 Obtaining optimal secure BCT using WSM and T2NSs

- In our case, all criteria are beneficial. hence, we utilized the normalized matrix from entropy based on T2NSs for generating a weighted decision matrix by utilizing Eq(9) as in Table 7.
- Finally, the candidates of BCTs are ranked based on values of global score. The findings of BCTs ranking are represented in Fig where BCT3 is the optimal alternative whilst BCT4 is the worst alternative.

Table 7: Weighted decision matrix

	C1	C2	C3	C4	C5	C6
BCT1	0.0523	0.0380	0.0225	0.0392	0.0345	0.0145
BCT 2	0.0331	0.0407	0.0285	0.0391	0.0360	0.0155
BCT 3	0.0394	0.0350	0.0302	0.0421	0.0442	0.0183
BCT 4	0.0373	0.0488	0.0239	0.0304	0.0308	0.0166
BCT 5	0.0410	0.0312	0.0228	0.0495	0.0456	0.0190

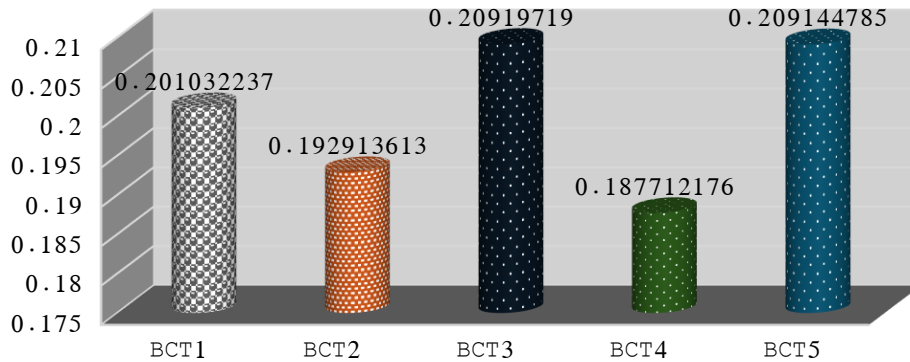


Fig 2. Final rank for alternative based on WSM-T2NSs

5 Comparative Analysis

We applied another method besides implementing our appraiser model in the real case study; we performed various scenarios for changing the criteria's weights by implementing sensitivity analysis. The objective of the sensitivity analysis process is to verify the stability of model's decision by determining how decisions are affected based on changes in the values of criteria weights.

Fig 3 illustrates the seven cases for changing the values of criteria weights besides criteria weights obtained from entropy based on T2NSs. The findings of the changed values of criteria weights are formed in Fig 4. According to this Fig the decision of the worst BCT for all cases is like the appraiser model's decision where BCT 4 is the worst. Nevertheless, the difference in the optimal BCT where the constructed appraiser model and six cases agree that BCT3 is the optimal followed by BCT5. Otherwise, case five where BCT5 is the optimal followed by BCT3.

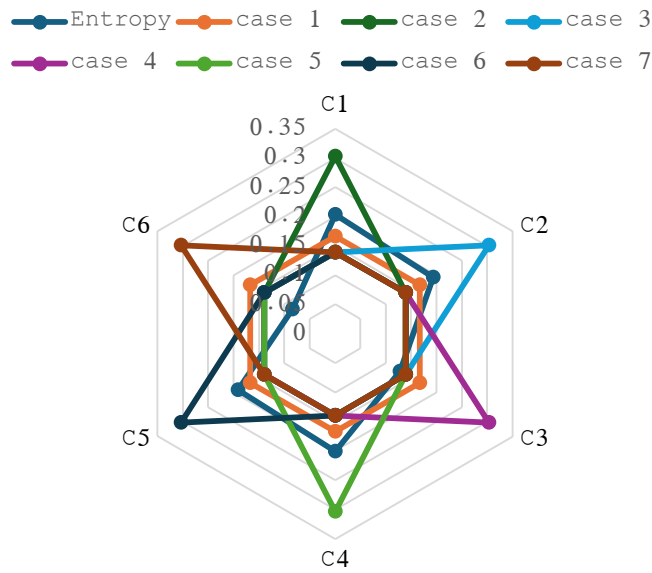


Fig 3. Changing values of criteria weights

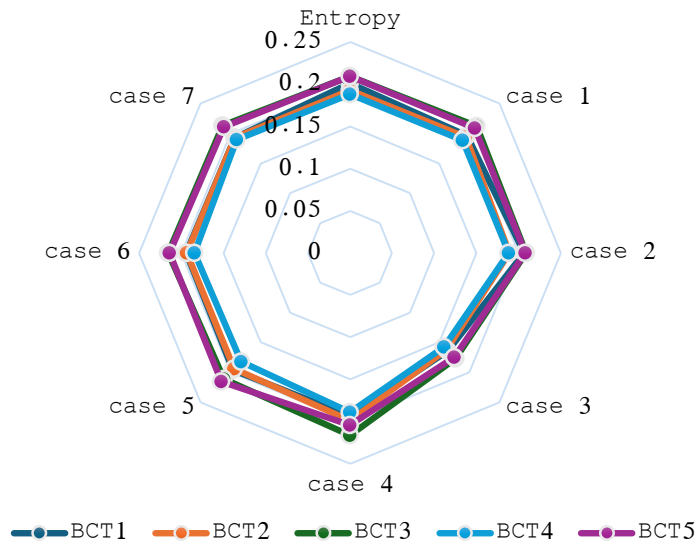


Fig 4. The decision of ranking BCTs based on various cases

6 Conclusions

This survey for prior studies demonstrated the security for both the earlier Vehicular Ad Hoc Networking (VANET) and other technologies as IoVs in intelligent transportation systems is a critical issue. Hence, Vehicular Fog Network (VFN) is constructed through integrating fog computing and VANET to provide cloud services to nearby vehicles to deal with timeliness and latency issues. There was also a focus on the capabilities of the recently developed BC technology in VFN. Making use of BCT to enable secure and efficient data trading for IoVs is becoming increasingly useful. BC technology is also having a significant

impact on businesses that we never would have predicted would become unstable. It makes sense to research this kind of topic since the service provider selection problem in a BC system might undergo significant changes in the future. Furthermore, an enterprise's performance and success are directly correlated with the choice of suitable BC service providers. Enterprises seeking growth and development will collaborate with capable firms to create BC technology, viewing these firms as their own BC service providers. The problem of selecting optimal BC is represented in selection according to set of attributes. MCDM techniques are employed in BCs selection to analyze attributes and recommend the optimal BCs among set of Decision makers. Herein, the entropy technique implemented in BCTs selection to obtain attributes' weights through the preferences of experts who related to our scope. The rating is performed by applying T2NSs. The results of the implementation of entropy indicated that Decentralization (C1) is optimal attribute otherwise Traceability (C6) is the least based on the final values of its weights. After that WSM leverages the generated weights of attributes to rank BCTs candidates and recommend the best and worst BCT. In our study, there is an agreement on recommending BCT3 as the optimal candidate based on its ranking. In contrast BCT4 is the worst one. But in case five BCT5 is recommended as optimal securing methodology in VFN.

References:

- [1] S. Abbas, M. A. Talib, A. Ahmed, F. Khan, S. Ahmad, and D. H. Kim, "BC-based authentication in internet of vehicles: A survey," *Sensors*, vol. 21, no. 23, 2021. doi: 10.3390/s21237927.
- [2] F. Ahmad, A. Adnane, C. A. Kerrache, V. N. L. Franqueira, and F. Kurugollu, "Trust Management in Vehicular Ad-Hoc Networks and Internet-of-Vehicles," 2019. doi: 10.4018/978-1-5225-9019-4.ch004.
- [3] G. Rathee, F. Ahmad, F. Kurugollu, M. A. Azad, R. Iqbal, and M. Imran, "CRT-BIoV: A Cognitive Radio Technique for BC-Enabled Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, 2021, doi: 10.1109/TITS.2020.3004718.
- [4] S. Woo, H. J. Jo, and D. H. Lee, "A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, 2015, doi: 10.1109/TITS.2014.2351612.
- [5] P. Gaba, R. S. Raw, O. Kaiwartya, and M. Aljaidi, "B-SAFE: BC-Enabled Security Architecture for Connected Vehicle Fog Environment †," *Sensors*, vol. 24, no. 5, 2024, doi: 10.3390/s24051515.
- [6] S. Tu, H. Yu, A. Badshah, M. Waqas, Z. Halim, and I. Ahmad, "Secure Internet of Vehicles (IoV) with Decentralized Consensus BC Mechanism," *IEEE Trans. Veh. Technol.*, vol. 72, no. 9, 2023, doi: 10.1109/TVT.2023.3268135.
- [7] L. Xu, M. Ge, and W. Wu, "Edge Server Deployment Scheme of BC in IoVs," *IEEE Trans. Reliab.*, vol. 71, no. 1, 2022, doi: 10.1109/TR.2022.3142776.
- [8] X. Wang, P. Zeng, N. Patterson, F. Jiang, and R. Doss, "An improved authentication scheme for internet of vehicles based on BC technology," *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2909004.
- [9] M. Kamal, G. Srivastava, and M. Tariq, "BC-Based Lightweight and Secured V2V Communication in the Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, 2021, doi: 10.1109/TITS.2020.3002462.
- [10] J. H. Song, V. W. S. Wong, and V. C. M. Leung, "Wireless location privacy protection in vehicular Ad-Hoc networks," *Mob. Networks Appl.*, vol. 15, no. 1, 2010, doi: 10.1007/s11036-009-0167-4.
- [11] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new type of BC for secure message exchange in VANET," *Digit. Commun. Networks*, vol. 6, no. 2, 2020, doi: 10.1016/j.dcan.2019.04.003.
- [12] L. Li *et al.*, "CreditCoin: A Privacy-Preserving BC-Based Incentive Announcement Network for Communications of Smart Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, 2018, doi: 10.1109/TITS.2017.2777990.
- [13] J. Kang *et al.*, "BC for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, 2019, doi: 10.1109/JIOT.2018.2875542.

- [14] A. Ahmed, S. Abdullah, S. Iftikhar, I. Ahmad, S. Ajmal, and Q. Hussain, "A Novel BC Based Secured and QoS Aware IoT Vehicular Network in Edge Cloud Computing," *IEEE Access*, vol. 10, 2022, doi: 10.1109/ACCESS.2022.3192111.
- [15] L. Zhang *et al.*, "BC based secure data sharing system for Internet of vehicles: A position paper," *Veh. Commun.*, vol. 16, 2019, doi: 10.1016/j.vehcom.2019.03.003.
- [16] M. Sookhak *et al.*, "Fog Vehicular Computing: Augmentation of Fog Computing Using Vehicular Cloud Computing," *IEEE Veh. Technol. Mag.*, vol. 12, no. 3, 2017, doi: 10.1109/MVT.2017.2667499.
- [17] C. Huang, R. Lu, and K. K. R. Choo, "Vehicular Fog Computing: Architecture, Use Case, and Security and Forensic Challenges," *IEEE Commun. Mag.*, vol. 55, no. 11, 2017, doi: 10.1109/MCOM.2017.1700322.
- [18] J. Ni, A. Zhang, X. Lin, and X. S. Shen, "Security, Privacy, and Fairness in Fog-Based Vehicular Crowdsensing," *IEEE Commun. Mag.*, vol. 55, no. 6, 2017, doi: 10.1109/MCOM.2017.1600679.
- [19] N. A. Ali, A. E. M. Taha, and E. Barka, "Integrating BC and IoT/ITS for Safer Roads," *IEEE Netw.*, vol. 34, no. 1, 2020, doi: 10.1109/MNET.001.1900146.
- [20] PwC, "Global BC Survey 2018 - PwC," *Glob. BC Surv. 2018*, 2018.
- [21] S. Liu, Y. Hu, X. Zhang, Y. Li, and L. Liu, "BC Service Provider Selection Based on an Integrated BWM-Entropy-TOPSIS Method under an Intuitionistic Fuzzy Environment," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.2999367.
- [22] M. B. Mollah *et al.*, "BC for the Internet of Vehicles towards Intelligent Transportation Systems: A Survey," *IEEE Internet of Things Journal*, vol. 8, no. 6, 2021. doi: 10.1109/JIOT.2020.3028368.
- [23] R. Gupta, A. Kumari, and S. Tanwar, "A taxonomy of BC envisioned edge-as-a-connected autonomous vehicles," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 6, 2021, doi: 10.1002/ett.4009.
- [24] S. A. Siddiqui and A. Mahmood, "Towards fog-based next generation internet of vehicles architecture," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2018. doi: 10.1145/3267195.3267200.
- [25] P. Gaba and R. S. Raw, "BIVFN: BC-Enabled Intelligent Vehicular Fog Networks," in *Smart Innovation, Systems and Technologies*, 2023. doi: 10.1007/978-981-19-4162-7_3.
- [26] P. Gaba and R. S. Raw, "Vehicular cloud and fog computing architecture, applications, services, and challenges," in *IoT and Cloud Computing Advancements in Vehicular Ad-Hoc Networks*, 2020. doi: 10.4018/978-1-7998-2570-8.ch014.
- [27] M. Abdel-Basset, M. Saleh, A. Gamal, and F. Smarandache, "An approach of TOPSIS technique for developing supplier selection with group decision making under type-2 neutrosophic number," *Appl. Soft Comput. J.*, vol. 77, 2019, doi: 10.1016/j.asoc.2019.01.035.

Received: Mar 9, 2024. Accepted: May 29, 2024