

# Blockchain-based and Fuzzy Logic-enabled False Data Discovery for the Intelligent Autonomous Vehicular System

ZIAUR RAHMAN\*, XUN YI, and IBRAHIM KHALIL, RMIT University, Australia  
ADNAN ANWAR and SHANTANU PAL, Deakin University, Australia

Since the beginning of this decade, several incidents report that false data injection attacks targeting intelligent connected vehicles cause huge industrial damage and loss of lives. Data Theft, Flooding, Fuzzing, Hijacking, Malware Spoofing and Advanced Persistent Threats have been immensely growing attack that leads to end-user conflict by abolishing trust on autonomous vehicle. Looking after those sensitive data that contributes to measure the localisation factors of the vehicle, conventional centralised techniques can be misused to update the legitimate vehicular status maliciously. As investigated, the existing centralized false data detection approach based on state and likelihood estimation has a reprehensible trade-off in terms of accuracy, trust, cost, and efficiency. Blockchain with Fuzzy-logic Intelligence has shown its potential to solve localisation issues, trust and false data detection challenges encountered by today's autonomous vehicular system. The proposed Blockchain-based fuzzy solution demonstrates a novel false data detection and reputation preservation technique. The illustrated proposed model filters false and anomalous data based on the vehicles' rules and behaviours. Besides improving the detection accuracy and eliminating the single point of failure, the contributions include appropriating fuzzy AI functions within the Road-side Unit node before authorizing status data by a Blockchain network. Finally, thorough experimental evaluation validates the effectiveness of the proposed model.

CCS Concepts: • **Computer systems organization** → **Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

Additional Key Words and Phrases: Blockchain, False Data, Fuzzy Logic, Intelligent Vehicle, Autonomous

## ACM Reference Format:

Ziaur Rahman, Xun Yi, Ibrahim Khalil, Adnan Anwar, and Shantanu Pal. 2018. Blockchain-based and Fuzzy Logic-enabled False Data Discovery for the Intelligent Autonomous Vehicular System. *ACM Trans. Graph.* 37, 4, Article 111 (August 2018), 11 pages. <https://doi.org/XXXXXXX.XXXXXXX>

## 1 INTRODUCTION

The world has experienced an appealing technological rise of intelligence-connected vehicular cyber-physical systems (CPS). According to the Internet Crime Complaint Center (IC3) of the United States(US) Federal Bureau of Investigation (FBI), 95% of the recorded breaches

\*Corresponding Author

Authors' addresses: Ziaur Rahman, [zia@iut-dhaka.edu](mailto:zia@iut-dhaka.edu); Xun Yi, [xun.yi@rmit.edu.au](mailto:xun.yi@rmit.edu.au); Ibrahim Khalil, [ibrahim.khalil@rmit.edu.au](mailto:ibrahim.khalil@rmit.edu.au), RMIT University, 414-418 Swinston St., Melbourne, VIC, Australia, 3000; Adnan Anwar, [adnan.anwar@deakin.edu.au](mailto:adnan.anwar@deakin.edu.au); Shantanu Pal, [shantanu.pal@deakin.edu.au](mailto:shantanu.pal@deakin.edu.au), Deakin University, 221 Burwood Hwy, Melbourne, VIC, Australia, 3000.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](mailto:permissions@acm.org).

© 2018 Association for Computing Machinery.

0730-0301/2018/8-ART111 \$15.00

<https://doi.org/XXXXXXX.XXXXXXX>

targeted critical infrastructure, such as sensor-enabled CPS. In July 2020, the Texas state power grid system was hacked, and the attacker tried to spoof the system's monitoring tools to inject false data to bully the whole system. This was not the first time; a similar attack occurred in December 2015, when an attack on Ukraine's power grid caused a massive blackout. These recent incidents reveal that the CPSs, including intelligence vehicles, are extremely vulnerable to False Data Injection (FDI). Blockchain has immense potential to secure the Vehicular CPS to protect it from injecting inaccurate data from neighbouring vehicles. Fuzzy logic and rule-based techniques can potentially discover data anomalies based on system behaviours. Instead of centralised monitoring, distributed and transparent control by the vehicle owners and roads and highways authorities, automatic false data detection can be advantageous if reliable techniques are involved.

An FDI attack is an unprecedented attack that often raises conflict against the reliable operation of the Vehicular CPS. Adding false data or misguiding an autonomous vehicle measurement may occur for different reasons. Any unauthorised intermediaries or even trusted neighbouring vehicles, intentionally or mistakenly, can inject malicious data. If the system control is maintained based on the trust employed through a TTP (i.e., service provider), the potential threat rises exponentially [Wollschlaeger et al. 2017]. Accordingly, preserving incorrect or vehicular measurement data can be utterly misleading. Conventionally, the data-associated with the IAVS is maintained by a cloud from the provider side. Autonomous Vehicular stakeholders can see their contributions but barely have any control authority. At this point, if any vehicle is compromised with misleading data, the sole responsibility is on those entitled to control the system. In addition to data forgery, negligible and erroneous data may appear due to technical errors that deserve proper preservation for extensive record keeping and monitoring. In the IAVS, this status history often constructs a reputation that is necessarily important for further decision-making, cost measuring and further localisation and measurement. Figure 1 shows the conventional network infrastructure of vehicular Cyber-physical systems.

## 1.1 Challenges and Perspectives

As the existing detection approaches demand proper revision to ensure transparency and accuracy, the research community has expressed deep concern for convincing solutions. However, blockchain has proven its ability to preserve transparent data transmission and sharing generated from a distributed network with the desired anonymity and immutability. They work through adaptable consensus and smart contract mechanisms [Gramoli 2020]. A false data attack is a kind of attack targeting the autonomous vehicle that causes different disruptions including localisation and further estimation issues. In false data attacks, misleading information is

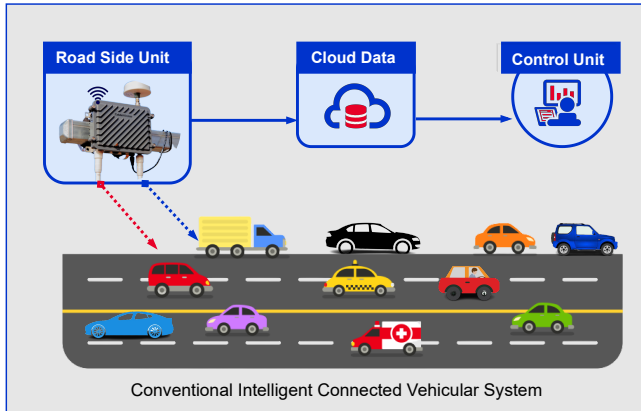


Fig. 1. Conventional Vehicular Data Communication Flow. The vehicles communicate with the nearby Roadside unit for an update. RUSU is connected with a Cloud-driven data centre controlled by the Roads-highway authority.

allegedly appended to one of the major operational modules [Wang et al. 2019b]. Therefore, detecting infected data and assessing how much data of IAVS is compromised should be done confidentially and securely.

Due to its immutable, efficient, reliable and enormously accessible behaviours, blockchain can be an exciting solution to this FDI and transparency problem [Li et al. 2019]. This article proposed a false data discovery and preservation technique. Besides, a reputation-building process is proposedly integrated. To secure status data while travelling from sensors to the blockchain ledger, the design incorporated a customised digital signature mechanism, fuzzy rule-based detection accuracy that works by following an infected data detection algorithm [Mendel and Wu 2017] [Wang 2017]. Further, another functional algorithm was designed to communicate with the blockchain ledger. The fuzzy-based detection methods show convincing accuracy, and the blockchain-aligned reputation preservation process brings a transparent and secure outlook for IAVS management [Li et al. 2017].

## 1.2 Contributions and Organizations

This work was motivated to address and demonstrate a blockchain and AI-enabled false data-detection and reputation preservation for the sensor-enabled, intelligent Cyber-physical system especially targeting IAVS. The specific contributions of this work are as follows.

- The proposed Fuzzy logic-enabled false data-discovery technique can filter data anomalies based on the behaviour rules. As described in the respective sections, the fuzzy-based model has higher effectiveness in terms of cost and security.
- The proposed model incorporates a novel reputation preservation mechanism based on infected vehicles that potentially generate false or misleading data. The reputation status of the measurement units helps other autonomous vehicles to be aware of the devices and protect the system from being misled.

Terms	Elaboration & Description
ADAS	Advanced Driver Assistance Systems
AI	Artificial Intelligence
BC	Blockchain
BFT	Byzantine Fault Tolerance
BTC	Bitcoin
CC	Chaincode
CFT	Crash Fault Tolerance
CPS	Cyber-physical System
ETH	Ethereum
FDD	False Data Detection
FL	Fuzzy Logic
HLF	Hyperledger Fabric
IAVS	Intelligence Autonomous Vehicular Systems
LiDAR	Light Detection and Ranging
MF	Membership Functions
MSP	Membership Service Provider
ML	Machine Learning
P2P	Peer to Peer Network
RADAR	Radio Detection And Ranging
RSU	Road Side Unit
SC	Smart Contract
SPOF	Single-point of Failure

Table 1. Technical Terminology along with its notation entries and abbreviation in alphabetic order

- Blockchain-based transaction verification ensures collaboratively built trust and security rather than relying on a single party. It eliminates PKI-driven cloud and centralised systems to protect the IAVS.

## 2 BACKGROUND AND RELATED WORKS

In this section relevant background knowledge on Blockchain technology, Fuzzy AI technique, autonomous vehicular technology and Related works are presented. Table 1 depicts the technical terms, notations and respective abbreviations frequently used throughout the paper.

### 2.1 Blockchain Technology for the Vehicular CPS

The emerging blockchain technology has immense potential to secure and enhance autonomous driving operations and management. Because of its self-governing smart contract protocols and consensus-driven block verification, its integration into the IAVS increases data and communication integrity and security [Taleb et al. 2017]. As shown in Figure 2, blockchain is an expanding and unchangeable list of records consisting of connected blocks using a secure and immutable hash algorithm. The network works on the distributed P2P network constituted by IAVS components, such as moving vehicular sensors, LiDAR sensors etc. Unlike centralised cloud-driven services, blockchain ensures multiparty authorisation, which essentially eliminates SPOF [Tschorsch and Scheuermann 2016].

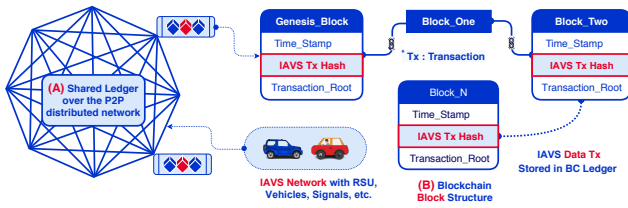


Fig. 2. Sample Blockchain Structure Consisting of IAVS Transactions ( $Tx$ ). A) Peer-to-peer (P2P) network of vehicular CPS where blockchain peers communicate and B) Blockchain block structure

Before storing a IAVS transaction in an associated ledger, it must be consented to by the contributory peers through a special process called the consensus mechanism. Earlier generation blockchain, such as Bitcoin and Ethereum, incorporated the PoW type of consensus, which is often criticised because of its significantly slower transaction processing rate. Based on the joining rights, blockchain can be either public or consortium, where only authorised users are allowed to join and contribute. Apart from PoW, CBC like Corda, HLF and Ripple incorporate fault tolerance consensus techniques (e.g., BFT and crash fault tolerance [CFT]). Crash fault tolerance excludes longer ID and transaction verification and, thus, has higher throughput and negligible DL [Li et al. 2019]. For example, for Bitcoin and Ethereum, the transaction processing rate (known throughput, transactions per second) ranges from 4 to 15 transactions per second, whereas HLF can process 3,000–20,000 transactions per second. By excluding computation-intensive validation, it eliminates conventional rewards or incentives, which makes CBC a great alternative for real-time and critical infrastructure, such as smart grids and IAVS [Ju et al. 2020; Rahman et al. 2021; Truong et al. 2020].

## 2.2 FL for False Data Discovery

Fuzzy logic is a form of AI reasoning that makes decisions in the same way as humans. Its computer-digestible logic block takes precise input and produces a definite output equivalent to real-world reasoning. IAVS follow particular rules and behaviour that can be logically translated into an input membership function (MF) of AI FL [Mendel and Wu 2017]. Thus, several MFs build intelligence together for a decision required for a particular IAVS. Unlike Boolean logic or probability theory, its decision-making process relies on the degrees of truth factor between *true* and *false*. Although FL is based on the levels of probabilities of input variables towards the purposeful output, it is a subset of AI that can be trained using software, hardware or both. The fundamental FL architecture contains at least four components, including rule specification and MFs. Where an MF for a fuzzy set  $f$  on the universe of discourse  $y$  is defined as  $\mu_f : y \rightarrow [0, 1]$ . The advantages of FL system are as follows [Wang 2017].

- Mathematical concepts for FL reasoning are simple to implement and can be modified easily by revising the integrated rules.

- Fuzzy logic systems can work dynamically with imprecise, anomalous input data. As a result, reasoning and decision-making can be made with fewer power constraints, reducing system deployment costs.

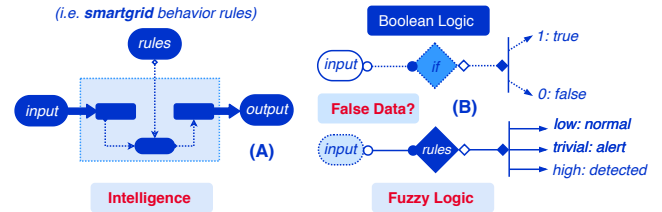


Fig. 3. Fuzzy logic (FL) components and salient characteristics that makes it distinct from its counterpart name boolean logic.

Figure 3 shows the basic components of FL and how it varies from Boolean logic. The rule can relate to any conditions or behaviours. For example, False data injection attack on a neighboring vehicle is discovered when the Error ( $E$ ) is larger than a threshold ( $E_{threshold}$ ) and the Weight ( $W$ ) for that source is lower than a threshold ( $W_{threshold}$ ). The edge node trained with these autonomous vehicular behaviours can detect data status and identify the source device if such conditions (as determined by MF) are not met. The considered IAVS rules will be explained in the forthcoming Section.

## 2.3 Related Works

False Data detection in the cyber-physical system has attracted research community for a couple of years and a good number of works highlighted the importance of the stealthy FDI attacks [Dey et al. 2015; Zhao et al. 2021]. [Li and Song 2015; Petit and Shladover 2014] proposed a secure model for data attack detection. The work above seems to have better performance as claimed through their simulation-based evaluation. In [Biron et al. 2018] [Ju et al. 2020; Sun et al. 2020] the authors proposed a monitoring system to determine the real-time occurrence of a disturbance in the voltage before suggesting a remedy in response. A group of researchers has recently made a private blockchain-based approach for local power consumption and generation without any trusted intermediaries. Another distributed ledger-driven effort based on smart-contract was explained by the authors to enhance the security and resilience of the energy CPS [Mengelkamp et al. 2018]. Apart from a distributed ledger, work done on distributing the host-based approach to detect FDI attacks by proposing novel False Data Detection (FDD) method, state estimation and performance reputation update with maximum likelihood algorithm [Zhao et al. 2021]. In their work, the authors have considered distributed host-based effort instead of the distributed ledger, and the rules assumed to evaluate seem to not exceed four host monitors. We have extracted sample from three different rules mostly on the autonomous vehicles's weight measurement, particle filtering, data fusion behaviours throughout our initial investigations, but even this number not seems to be portraying an entirely complex scenario of the IAVS. In our approach, we

also have considered distributed network and instead of centralized monitoring. Distributed ledger both private and public blockchain have been incorporated. Another work done based on weak data attack arising due to stealthy and corrupted measurement seems to be done the experiments and demonstrated theoretical analysis before claiming their approach has less relative error [Jo et al. 2015]. A lightweight privacy-preserving technique for distributed RSU has also claimed the authentication speed [Dinh et al. 2018].

### 3 DESIGN CONCEPTS AND SYSTEM MODEL

The proposed design concepts include three different components. Firstly, a fuzzy-based false detection technique in the Roadside Unit (RSU) end filters data before sending it to the blockchain network. Secondly, the blockchain authenticates data and the generating source devices through a certificateless and collaborative signing process [Aitzhan and Svetinovic 2018a; Kumar et al. 2020]. Finally, only the verified data are stored in the storage node. The proposed framework was designed considering these salient features and incorporated a permissioned blockchain and DHT mechanism for demonstration and evaluation [Truong et al. 2020; Wang et al. 2019a]. However, it conceptually supports the public type of blockchain and storage service. Figure 4 shows the high-level view of the proposed detection and reputation preservation approach. The communication flow of the proposed system can be divided into three parts: discussed as follows.

#### 3.1 Vehicle to RSU Communication

Autonomous vehicular CPS employs Sensor Fusion such as Radars and LiDARs. Fusion sensors are connected to the global remote terminal unit via the V2R (Vehicle-to-RSU) network. Other IoT sensors are able to send data to the destination through the constituted edge devices, irrespective of whether sources are wired or wireless [Aitzhan and Svetinovic 2018b; Erwin Adi and Zeadalli 2020]. Portion A of Figure 4 shows the V2r communication where the proposed fuzzy rules work to detect data anomalies [Mendel and Wu 2017].

#### 3.2 Blockchain Ensures Secure Data Transport

Instead of cloud-driven systems, the edge data are authenticated via a blockchain network to reduce the chance of SPOF and centralised trust. The proposed solution incorporates a certificateless multisignature-based device and data authentication over the P2P network [Aitzhan and Svetinovic 2018a; Li et al. 2019]. The network can be either public or restricted; however, considering the high data processing time and DL, the proposed model constitutes CBC. It establishes secure communication with the IAVS RSU and MEMS and validates the transported data. Portion B of Figure 4 depicts the secure data transport using blockchain.

#### 3.3 Reputation Preservation and Storing

The reputation preservation algorithm works within the detection model to update the reputation of autonomous vehicles. Once the particular vehicle seem to be generating false data, it will update its individual status. The reputation and the data transaction are recorded in the blockchain ledger, and data are stored in off-chain

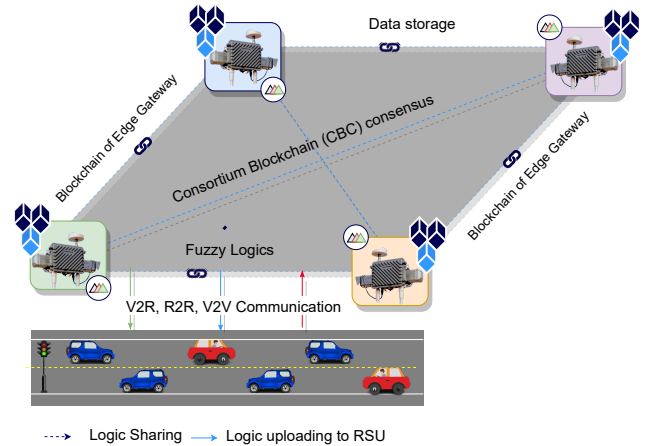


Fig. 4. High-level Representation of the Proposed Blockchain and Fuzzy Logic-aligned False Data–Detection and Reputation Preservation for the Intelligent Autonomous Vehicular System (IAVS). A) Source Vehicles send data through the edge gateway, B) the client vehicles submit the data transaction to the blockchain network (i.e., key generation and distribution [KGD] consortium) and C) upon successful verification, the data transaction and the detection status and reputation are recorded in the ledger, and data are stored in distributed hash table storage (e.g., interplanetary file system [IPFS] and Kademlia).

storage. The proposed framework considered the salient features and incorporated DHTs, such as IPFS and Kademlia [Huang et al. 2020]. Reputation preservation happens in the earlier portion; Portions A and C of Figure 4 portrays the storage mechanism. However, storing data directly in the blockchain network, even in an encrypted form, threatens consumer or stakeholder privacy and does not comply with privacy standards [Rahman et al. 2021, 2022].

#### 3.4 Threat Model

The proposed model was designed based on the considered threat model. The decentralised blockchain ensures that an attacker cannot corrupt the consortium network. Any unauthorised peer or adversary cannot modify the blockchain ledgers, which implies that the resource is compromised. The threat model prevents impersonation by an unauthorised party or an adversary, as the associated multisignature cannot be tempered or forged. Therefore, security threats can be generalised into two broad categories. Firstly, an internal party or peer disguised in a Byzantine way has probably been granted access to IAVS data [Zamani et al. 2018]. Secondly, an honest or trusted vehicle but its security credentials, such as private or decryption keys, are disclosed to an external adversary. Thus, the external party with the stolen access can bully the network. Blockchain smart contracts contain a token validation technique, which is refreshingly expired after a particular time or transaction, that protects the network from being compromised with the latest type of threat. However, the blockchain ledger will record the reputation of the malicious peers and block them temporarily or permanently. The BFT or CFT technique ensures the system runs smoothly, even after some peers

Table 2. Overview of recent research on IDSs for IoT applications

Referral Work	Crypto	Efficiency	Limitations	Application	Blockchain
[Zhao et al. 2021]	√	Low	IAMS Incompatible	Security	×
[Dey et al. 2015]	√	Medium	Cost-intensive	Small-scale IoT	√
[Petit and Shladover 2014]	√	Low	Coalition attacks	Security	×
[Li and Song 2015]	√	Low	Chosen-text attack	Security	×
[Li and Song 2015]	×	High	Cost-intensive	IoT	×
[Aazam et al. 2018]	×	Low	Com.-Intensive	Medical IoT	×
[Truong et al. 2020]	×	Medium	High overhead	Vehicular Sensor	×
[Anwar et al. 2017]	√	Medium	Not efficient	VANET	√
[Li and Wang 2015]	√	High	Cost-intensive	Critical system	√
[Liang et al. 2016]	√	Very High	Com.-intensive	Industrial IoT	√

have been suspended. Besides the security threats, the model considers the privacy of the IAVS and their data. The encryption and partial secret (PS) of the multisignature ensure pseudo-anonymity, whereas CBC only allows authorised peers, meeting the privacy challenges of the Autonomous Vehicular CPS [Gramoli 2020].

### 3.5 Trust Assumption

The proposed model assumes that RSU constituting the blockchain network are honest or semi-honest. The model obviates the membership service provider (MSP) who has equivalent CA to PKI [Nix 2016]. As investigated throughout the centralised cloud-driven approaches, it increases the chance of being compromised and SPOF. Besides, the elliptic curve–cryptographic primitives and hash function are assumed to be particularly secure. This means that attackers cannot extract keys using reverse exponentiation, break the hash algorithms or temper the multi-signature. In addition, the model considers that the data transfer occurs over an insecure network or internet. The next section discusses the proposed mechanism for false data detection and preservation [Yang and Tan 2011].

## 4 FALSE DATA DISCOVERY AND REPUTATION UPDATE

As assumed that the IAVS usually operates on a normal stable status where the associated state parameters and variables differ in an interchangeably balanced manner. For example, the IAVS follows specific behaviours. Thus, any variable state changes due to a system fault cause corresponding state changes and produce anomalous data. However, data anomaly can be identified if variables change on one bus without affecting the parallel variables.

In this paper, IAVS communicates with the RSU servers and publishes information about itself and its neighbours with a unique vehicle identity (ID). After the RSU server gathers the information from all the IAVS in a platoon, neighbouring vehicles information can be associated using the vehicle ID, and neighbouring unconnected vehicles information from multiple IAVS on-board sensors (i.e., Lidar or Radar) is assumed to be fused using a multi-source data association method so that each unconnected vehicle is also assigned with a specific vehicle ID. Therefore, by leveraging vehicle IDs, data

Table 3. Typical behaviour of IAVS rule examples

Sl	Behaviour Rules	Variable Description
1	$\Delta I_k > I_{Threshold}$	Malicious data injected by a vehicle
2	$P_E = P_F + P_M$	$P_E$ from probability of ( $P_M$ ) & ( $P_F$ )
3	$E_t > E_{Threshold}$	Error larger than threshold
4	$W_t < W_{Threshold}$	Weight lesser than threshold

for neighboring vehicles can be identified, and only neighbouring IAVS information will be used in the proposed solution.

IAVS Error Variation				
Weight Variation	DETECT	Trivial	Fair	Vital
	Minor	NO	NO	YES
	Average	NO	NO	YES
	Major	YES	YES	YES

Fig. 5. Behavioural rule extraction and its corresponding fuzzy representation. A) Rule matrix for different status B) Rule specifications

### 4.1 Rule Specifications

When a IAVS is under usual operation, all of its state variables follow particular constraints and hold desired properties.

The following Table 3 shows similar rules considered. These are some fundamental rule specifications to detect false data due to anomalous PMU activities.

The fuzzy rule specifications as explained in the next subsection considers following basic rules. Behavioural rules can be similarly specified for all other rules listed in the above Table.

- a false data injection attack on a neighbouring vehicle is identified when the error ( $E_t$ ) at time  $t$  is larger than a threshold  $E_{threshold}$



- Weight at time  $t$  for that source is lower than a threshold ( $W_{Threshold}$ )
- $P_E = P_F + P_M$  means that Error obtained from probability of misdetection ( $P_M$ ) & the probability density function ( $P_F$ )

The following Figure 5 shows the rule-matrix that works to filter the data quality. First, it needs to classify the behaviour in different states [Li and Wang 2015]. For example, as per Rule 4 of Table 3, the variation of Error should not be always greater than a measured threshold. The threshold can be calculated following up the dynamic nature of the IAVS and previous records. However, as settled that the Weight variation at a time  $t$  should be always less than the threshold. Considering the severity of the difference, it Fuzzy system classify, it as *minor*, *average* or *major*. Similarly, for Error, it can be *trivial*, *fair* or *vital*. Based on the rule matrix as demonstrated by Figure 5, the corresponding fuzzy rules are listed above. For example, if Error deviation is *trivial* and Weight is *minor* then the fuzzy system will not mark it as *NO* and will send it to the blockchain peers for further processing. In different cases, it will either *YES* data as anomalous or send it with a *warning* flag [Mengelkamp et al. 2018; Mylrea and Gouriseti 2017].

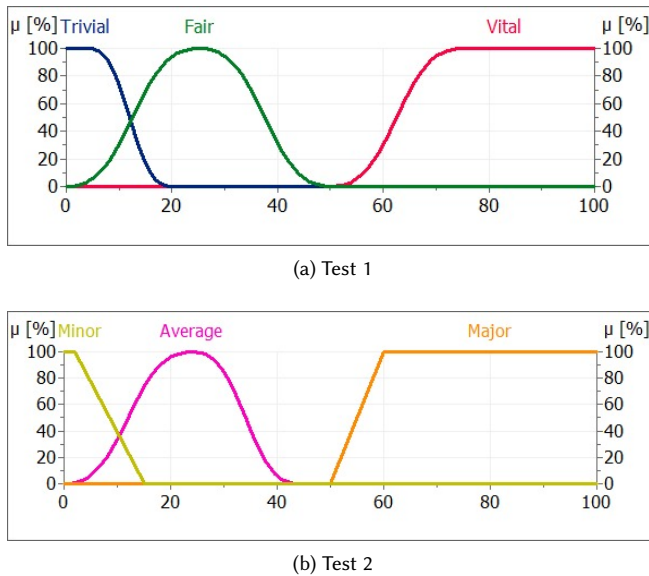


Fig. 6. Input MF definitions based on IAVS behavior rules

#### 4.2 Defining Fuzzy Membership Function (MF)

The graphical representation of fuzzy membership function (MF) shows how each point in the input space is mapped to the corresponding system status. FL modelling includes at least four components including rule specification and membership MFs. Where an MF for a fuzzy set  $f$  on the universe of discourse  $y$  is defined as  $\mu_f : y \rightarrow [0, 1]$ . It quantifies the severity of MF element both in  $x$  and  $y$  axis where  $x$ -axis shows the universe of discourse and  $y$ -axis represents the degree such as *trivial*, *minor*, *fair* etc. within

the variation range. As investigated, the accuracy varies as per type MF functions [Mendel and Wu 2017]. For example, if Error is implemented with a *triangular* function, the detection varies from the *trapezoidal* MF. Targeting the maximum throughput, the proposed evaluation runs with the *gaussian* and its variant *SP-line* MF. In a normalized *SP-line* MF  $\mu_i^m$  of order  $m$  (degree  $(m-1)$ ) for the fuzzy subset  $[a, b]$  over  $R$  (Real number range) the variation  $\Delta : a = k_0 < k_1 < \dots < k_{n+1} = b$  as  $\mu : [a, b] \rightarrow [0, 1]$ . Here  $m_i$  is the multiplicity of the knot  $k_i$ .

Figure 6 depicts the respective membership of functions of based on the degree of variation of both Error and Weight angel as mentioned earlier. During the range selection of the demonstration, we changed ranges to a different level. For example, the following Figure 6 shows that if the variation exceeds about 50% then severity is classified as *vital* for Error and *major* for Weight deviation. However, based on the previous record of RSU the ranges could be varied to improve the system performance [Wang 2017].

Following a similar process, the output membership functions have been selected. The *gaussian* and *SP-line* seem to bring higher accuracy in comparison to *trapezoidal* and *triangular* MF. The threshold basically depends on the previous record of the Vehicular CPS, however, it has been finalized one-fourth (25%) of the system's overall deviation. That means it verdicts the *detected* if the average variation of Weight exceeds the Threshold. Sample false data detection after debugging the MF and its configured behaviour rules is discussed here. Here  $A$  and  $B$  are the input MF configuration based on  $E_t$  as explained earlier [Wang 2017].  $C$  depicts the corresponding output. For example, for a particular case,  $W_t$  becomes varies within the Threshold then it detects the severity of the False Data is about 85%. In such a circumstance, the system as integrated in the edge gateway, will not allow sending the corresponding data transaction to further blockchain peers. Besides, it will update the reputation of source PMU and will include the latest status along with data transaction and source identities [Mendel and Wu 2017].

#### 4.3 RSU Reputation Updating

The probability distribution function (PDF) can be applied to determine the system's reputation. For example,  $\beta$  distribution seems to be promising for a collaborative detection model. Considering further smooth and secure preservation aligned with blockchain, the proposed model incorporates a novel reputation updating algorithm based on the degree of the detection level [Li et al. 2017].

**4.3.1 Reputation Algorithm.** The Alg. 1 takes input parameters from the previous detection phase. Parameters include system detection level and status which is either *true* or *false*, identities of the PMU or any other similar sensors or MEMS along with the corresponding values of the membership variables. The respective functions or subroutine initializes the required system parameters such as initial reputation and associated values of the RSU.

Once values are set, the algorithm checks if and only if the status is true or false. It updates the particular RSU (identified with the ID) status and exit process if any false data are found within the system,

**Algorithm 1:** IAVS RSU reputation updating on false data discovery.

---

```

Input :S – status either true or false
         R – reputation level
         L – RSU or sensor identities
         A – Error
         V – Weight
         D – detection level /* received data from fuzzy system */
Output:(ID,Rt,D) – returns after algorithm execution
1 init := (ID, R, D, A, V) /* initializes after fuzzy detection */
2 for ID ← IDi /* for all identities n × IDi */
3 do
4   R ← getStatus (ID, D, R) /* get requisite values (ID) */
5   if (status == true) then
6     S ← updateRep (R, ID): /* update PMU or sensor reputation */
7   end
8 end

```

---

as predicted by the earlier detection phase. After finalising the detection and reputation updating process, the data are ready to be sent to the blockchain for further verification and storage. The next section discusses how the IAVS detection status and reputation level are validated by the associated blockchain network and successfully stored for future maintenance and preservation. Next, the IAVS data and the corresponding reputation need to be transformed into a blockchain transaction. Figure 7 shows the sample IAVS transaction to be transported over the internet.

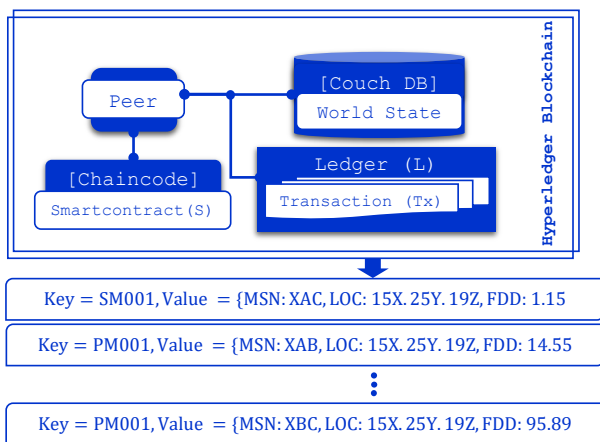


Fig. 7. Sample IAVS transaction belongs to the ledger and typical world state database (i.e. Couch DB) with interaction with chaincode smart contract.

## 5 BLOCKCHAIN VERIFICATION AND DATA PRESERVATION

In the proposed IAVS data verification and preservation process, the Consortium blockchain plays an indispensable role. The PMU needs to get registered with the blockchain-based key generating and distribution (KGD) system which is built upon the agreement of

the blockchain peers [Yang and Tan 2011]. KGD are the blockchain peers that commence the process of device registration. It starts with system parameters and outcomes of the partial secret ( $PS$ ). It eliminates the requirement of a trusted third party (TTP) such as the Certificate Authority of PKI. Before posting the transaction, IAVS RSU or sensors obtain public-private key pairs upon the completion of the registration process. The following part discusses how to source devices are registered to the blockchain network. Then how it verifies particular transactions submitted to it.

### 5.1 Registering RSU

At the beginning, multi-party IAVS stakeholders agree to build and share over the consortium blockchain (BC). Suppose, several RSUs cooperatively form the BC network that facilitates the key generating and distribution (KGD) peers [Li et al. 2019]. Blockchain KGC peers broadcast the system parameters ( $Y$ ) all IAVS RSU have knowledge about. KGD peers keep their individual signer's secret such as  $S_1, S_2, \dots, S_n$ . With the help of Edge computation capacity or its own ability, interested IAVS RSU creates their own secret value  $X_1, X_2, X_3, \dots, X_j$  generates respective public keys using  $X_j$  and the system parameter  $Y$ , where  $j$  is the number of interesting devices at particular time  $t$  and  $n$  is the number of co-signing blockchain peers [Huang et al. 2020].

RSU server will contact the KGD with their identities  $ID_1, ID_2, \dots, ID_j$ . Upon receiving the request, KGD will generate a partial private secret  $PS_1, PS_2, \dots, PS_i$  for all requested devices and will co-sign co-sign  $ID_i$  and  $PS_i$  using co-signers private key  $S_n$ . KGD sends the signed message back to the RSU Edge. The sensor device itself or edge node (e.g. Azure IoT edge or Dell Gateway) will verify if the message comes from the KGD, and if yes, it will generate private - private key pairs ( $Pk_1, Pk_2, \dots, Pk_i, Sk_1, Sk_2, \dots, Sk_i$ ) using ( $PS_i, X_i, Y$ ). Note that only each PMU will be able to create the private key because it is the only entity who knows his private secrets  $X_j$ . Alg. 2 illustrates the step by process with the necessary explanations.

### 5.2 Transaction Verification and Preservation

Once RSUs are successfully registered to the KGD upon the certificate-less cryptography and multi-signature-based authentication, the RSU proceed further to send and store data. Usually, data gets transaction fashioned before sending it to the blockchain network. The transaction includes the identity of the RSU along with the action and timestamp at the time ( $T$ ) of action ( $ACT$ ). There can be different types of actions such as *store* data at a specific DHT address ( $ADS$ ), *update* previously inserted data or *access* permission of the particular data. To verify a transaction  $T_x = (ID_j, T, ACT)$ , the blockchain peers have to meet two conditions: *i*) Either the public key ( $PK_j$ ) obtained associates with the identity ( $ID_j$ ), *ii*) or any other public parameters can the signed transaction ( $T_x$ ) be verified [Cho et al. 2020; Kumar et al. 2020].

RSA (Rivest-Shamir-Adleman) based digital signature algorithm (DSA) or elliptic curve digital signature algorithm (ECDSA) can be used. Considering the lesser key-size facility, we opted for the

**Algorithm 2:** IAVS RSU registration with blockchain KGD.

---

```

Input :IDj – identities of the j'th number of vehicle
        Y – system parameters /* prime numbers, primitive roots etc
        */
Output:(Pk, Sk) – public and private key pairs /* for all devices
        at t */
1  setup( $1^\lambda$ ) → (Y)          /* system parameters (Y) initialization */
2  for ID ← IDj do
3    porocedure keyGen (Y, ID): /* key using system Y and identities */
4    Xj ← genSk (Y, IDj)      /* IAVS generates own secret keys */
5    requestSend (IDj) /* IAVS send interests to join consoritum BC */
6    PSj ← genPS (IDj)       /* KGDs generates partial secret */
7    multiSig(Sn, IDj, PSj) /* multi-sign using S of n cosigners */
8    responseReceived (IDj)   /* IAVS receives PS from KGD */
9    V[0,1,⊥] ← verify ()      /* verify the multisignatures */
10   if V ← ⊥ then
11     Skj ← genSk (Y, IDj, Xj) /* sets IAVS device private key */
12     Pkj ← genPk (Y, Xj)     /* sets IAVS device public key */
13   end
14 end

```

---

ECDSA in our evaluation setup inside the apache Kafka framework of the hyperledger Iroha framework [Li et al. 2019].

**Algorithm 3:** IAVS Transaction (Tx) verification and storing.

---

```

Input :Tx – IAVS transactions
        L – access control lists
        σ – signaturues of the Tx
        IDj – identities of the j'th number of RSU Servers
        Y – system parameters /* prime numbers, primitive roots etc
        */
Output:(Vid, VTx, S) – set & return verification and storing flag
        true
1  create := (ID, L, Tx, σ, ADS) /* creates Tx using L ID and ADS */
2  signTx (Tx, Sk)              /* sign creates transactions */
3  castTx (Tx, σ)              /* broadcasts the original Tx and the signed one */
4  for Tx ← Txi              /* for all transaction n × Tx */
5  do
6    V1 ← verID (ID, Pk, Y)    /* verifies the identities (ID) */
7    V2 ← verTx (Tx, ID, Pk, σ) /* verifies the transactions (Tx) */
8    if (V1 || V2) then
9      S ← storeDHT (Tx, ID): /* store Tx into DHT and set S true */
10   end
11 end

```

---

Here, the signature algorithm can be represented as a triple /4-tuple of probabilistic polynomial-time algorithms (G, S, V) or (G, K, E, D) that includes generation (G), signing (S), verification (V), key-distribution (K), encryption (E) and decryption (D) respectively. Upon successful verification, the address (ADS) is stored in the DHT while the pointer belongs to the blockchain peers who verify. The following **Alg. 3** shows how the mechanism happens. Besides, the identities ID<sub>j</sub>, here the devices require the Access Control List (ACL) before Transaction

(Tx) creation and signing (σ). The industry 4.0 devices along with the RSU Gateway are solely responsible to create the ACL list (L) in addition to signature (σ) generation and transaction (Tx) publishing. However, the same L will be required later to access data. The algorithm as shown in **Alg. 3**, outcomes three different flags (V<sub>1</sub>, V<sub>2</sub>, S) set after successful execution. If the identities belong to the derived public keys, V<sub>1</sub> := true, while the certificateless signature meets the condition as discussed earlier, (V<sub>2</sub> := true). The blockchain peers do the transaction (Tx) verification in response to the reception. Interchangeable verification procedure works in case of data access. Similarly, upon RSU data transactions (Tx) are written into the DHT, the third flag gets set, (S := true). After that, a new block is added to the blockchain and subsequently, the ledger gets updated including the Tx Pointer (Tp). Figure 8 shows the communication sequence among client, consensus and smartcontract.

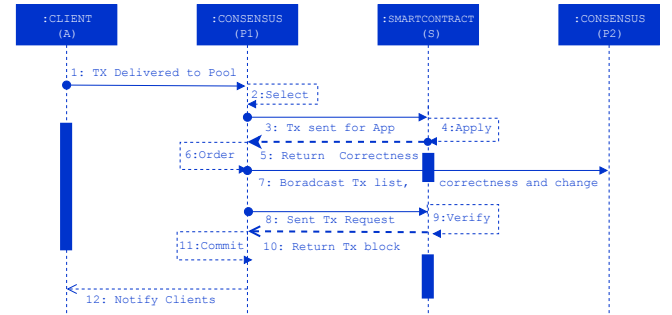


Fig. 8. Communication sequence of a typical IAVS within the blockchain network. It employs the cycle among client devices that submit data, consensus peers and smart contact

### 5.3 Smart Contract and Consensus Implementation

The implementation required writing chain codes (CC, special smart contract for Hyperledger blockchain) against the respective ledger. The initial chain codes provide authentication, access control and authorisation while others ensure logging besides the validation. Being a platform-independent platform Hyperledger supports any language to write its codes, however, because of relevant online resources, we preferred mostly *Go* and in some test-cases *Java*. To adapt multi-signature-based certificateless environment after eliminating certificate authority (CA) and membership service provider (MSP), the dependencies of the open-source *shim* package needed customization [Huang et al. 2020; Truong et al. 2020]. By default, it provides ledger/other CC accessing APIs, state variables or (Tx) context. Considering the data\_pointer represents the cipher-text of the IIoT data. Assuming an encryption function  $\mathbb{E}$  with public key (Pk<sub>j</sub>):  $data\_pointer = \mathbb{E}(mQAPk_j, device.id_j)$ . A third-party entity (K<sub>j</sub>) with a shared private key (Sk<sub>j</sub>) can decrypt the device.id as well using an opposite decryption function  $\mathbb{D}$ .  $device.id = \mathbb{D}(Sk_j, data\_pointer)$ . The policy in the *IIoT – ledger1.1* is simply defined as an access control list (ACL). Figure 9 depicts the communication among client devices (edge gateway), smart-contract and consensus protocols. Firstly, the transaction (Tx) is submitted to the blockchain network



as a proposal using a smart contract. The SDK of the network provides the application environment to check if it is valid. Once valid it needs to be consented to by the consensus peers. In doing so it broadcast the  $Tx$  among all collaborating peers of the consortium and updates the ledger [Wang et al. 2019a].

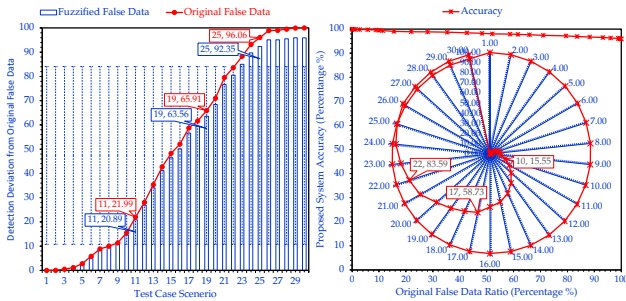


Fig. 9. Detection deviation and accuracy of the proposed AI-enabled detection technique. It shows corresponding data for selected 30 test cases

## 6 EVALUATION AND RESULT ANALYSIS

The proposed model was tested on *FuzzyTech* simulation tool and the detected data and its preservation were purposefully verified on the consortium blockchain platform namely hyperledger fabric. The following section discusses the obtained result accordingly. To evaluate the proposed system accuracy we have implemented Mamdani fuzzy inference system (FIS) on a Windows 10 enterprise operating system working on *Intel Core(TM) i5-7200U* CPU with 8 GB RAM 2.50 and 2.71 GHz capacity.

### 6.1 Detection Accuracy

The built system was debugged for several cases. Among all debugs, there were 30 test cases used to visualise the chart fuzzy system accuracy. Figure 9 shows the detection trend of the system. The detection was made using the fuzzy input and respective MF based on the rules considered. The rule extraction section of the manuscript explains the notations used for each rule. The initial portion of Figure 9 shows the detection deviation from the original injection of false data. The latter portion presents the accuracy of the system. Two rules were used based on the variation of Error and Weight; therefore, the accuracy shown is only the accuracy of the selected MFs, which actually differs for higher number rules. It shows that it has higher accuracy when IAVS RSUs have fewer anomalies, and the accuracy slightly decreases with a higher injection of false data. Further work will be undertaken to improve this finding. The corresponding receiver operating characteristic (ROC) curve (see Figure 10) presents the possible cut-offs for sensitivity and specificity among the 30 test cases. It shows the system has maximum sensitivity with fewer false data, which portrays the most usable cut-off. The highest cut-off has the maximum true positive rate and the minimum false positive detection.

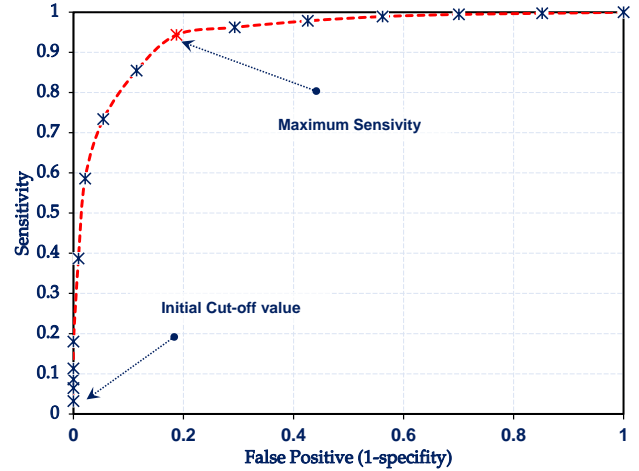


Fig. 10. Receiving operating characteristic (ROC) analysis of the proposed detection technique based on the considered test cases. It marks the initial cut-off and maximum sensitivity region of the proposed Fuzzy-enabled model.

Table 4. The throughput (TP), success rate (SR) and delay latency (DL) for READ and WRITE operation of the IAVS transaction ( $Tx$ ). The above values are calculated based on the workload (WL or  $Tx$  per second) as shown in the left-most column.

WL	READ			WRITE		
	TP	SR	DEL	TP	SR	DEL
100	100	9.7	0.01	100	9.7	0.01
200	220	9.6	0.01	185	9.3	0.31
300	340	9.5	0.01	175	7.8	1.48
400	390	9.3	0.02	145	6.1	4.38
500	470	8.8	0.05	85	4.9	5.25
600	370	7.5	2.26	60	3.8	6.16
700	330	6.5	5.43	40	3	7.43
800	250	5.5	6.12	30	2	8.22
900	170	4.5	6.41	20	1.1	8.94
1000	110	3.5	6.68	10	0.5	9.92

### 6.2 Blockchain Network Performance

The HLF benchmarking results shows the performance based on four measurement metrics success rate ( $\rho$ ), latency ( $\Delta t$  and  $L$ ) and the Throughput ( $P$ ) and the resource consumption ( $W$ ) for different test cases. Figure 11 shows the system performance under a different number of workloads ( $W$ ) ranging from 0.1k to 1k workload where the HLF network occupies two (02) chain codes, four (04) peer nodes and three (03) OSNs running on apache Kafka for practical byzantine fault tolerance (PBFT) consensus. As seen in the figure the *WRITE* has 185 at 0.2k workload ( $W$ ) with a maximum success rate of 93% and an average delay of 5 seconds. On the other hand, *READ* operation seems to have higher throughput (up to 470 at maximum) on a similar success rate at its best. The average delay seems to be half of the write's delay as the write has to incorporate

OSNs on Apache Kafka. Table 4 shows the throughput (TP), success rate (SR) and delay (DEL) latency of the blockchain deployment [Truong et al. 2020].

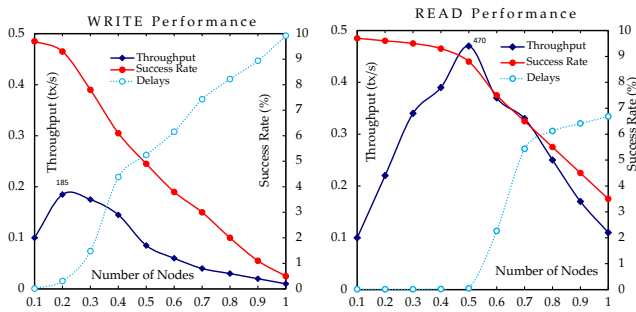


Fig. 11. READ and WRITE performance of the deployed blockchain network that securely record data and reputation and store data to the associated distributed hash table (DHT)

The benchmark evaluation explicitly illustrates that the setup configured has lower performance for a higher number workload ( $W$ ) though the theoretical solution proves the consortium blockchain has significant adaptability for a higher number of nodes. As investigated deep inside, the local workload processing bottleneck affects throughput and latency. Hyperledger  $T_x$  flow works demand enough responses against the submitted  $T_x$  proposals, in case the responses are queued due to network overhead, bandwidth or processing loads consequences of the latency raising. On top of that, the general purpose workstation configuration slower the evaluation for higher workloads [Wang et al. 2019a].

## 7 CONCLUSION

In today's IAVS data integrity attacks like FDI are an ongoing concern. If the system has inaccurate data, any activities based on that anomalous data will be in vain and can result in operational failure, financial cost and loss of lives. The proposed blockchain and Fuzzy-enabled false data-detection system should help filter anomalous data before sending it for further processing. Communication between the RSU and storage devices happens with collaborative verification, which ensures the system's security and data safety. The system obviates the PKI-driven trusted CA and the established centralised system. Thus, it can eliminate SPOF and single-party dependency. The respective evaluation and results show that the proposed model has comparatively higher accuracy. The blockchain network's performance justifies the proposed model's applicability for the RSU and Vehicles. Future scope includes improving the accuracy of the number of behaviour rules and justifying the scalability for massive networks.

## REFERENCES

M. Aazam, S. Zeadally, and K. A. Harras. 2018. Deploying Fog Computing in Industrial Internet of Things and Industry 4.0. *IEEE Transactions on Industrial Informatics* 14, 10 (2018), 4674–4682. <https://doi.org/10.1109/TII.2018.2855198>

N. Z. Aitzhan and D. Svetinovic. 2018a. Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams.

*IEEE Transactions on Dependable and Secure Computing* 15, 5 (2018), 840–852. <https://doi.org/10.1109/TDSC.2016.2616861>

N. Z. Aitzhan and D. Svetinovic. 2018b. Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. *IEEE Transactions on Dependable and Secure Computing* 15, 5 (2018), 840–852. <https://doi.org/10.1109/TDSC.2016.2616861>

Adnan Anwar, Abdun Naser Mahmood, and Mark Pickering. 2017. Modeling and performance evaluation of stealthy false data injection attacks on smart grid in the presence of corrupted measurements. *J. Comput. System Sci.* 83, 1 (2017), 58–72.

Zoleikha Abdollahi Biron, Satadru Dey, and Pierluigi Pisu. 2018. Real-time detection and estimation of denial of service attack in connected vehicle systems. *IEEE Transactions on Intelligent Transportation Systems* 19, 12 (2018), 3893–3902.

Eunsang Cho, Jeongnyeo Kim, Minkyung Park, Hyeonmin Lee, Chorom Hamm, Soobin Park, Sungmin Sohn, Minhyeok Kang, and Ted Taekyoung Kwon. 2020. TwinPeaks: An approach for certificateless public key distribution for the internet and internet of things. *Computer Networks* 175 (2020), 107268. <https://doi.org/10.1016/j.comnet.2020.107268>

Kakan C Dey, Li Yan, Xujie Wang, Yue Wang, Haiying Shen, Mashrur Chowdhury, Lei Yu, Chenxi Qiu, and Vivekgaatham Soundararaj. 2015. A review of communication, driver characteristics, and controls aspects of cooperative adaptive cruise control (CACC). *IEEE Transactions on Intelligent Transportation Systems* 17, 2 (2015), 491–509.

Tien Tuan Anh Dinh, Rui Liu, Meihui Zhang, Gang Chen, Beng Chin Ooi, and Ji Wang. 2018. Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering* 30, 7 (2018), 1366–1385.

Zubair Baig Erwin Adi, Adnan Anwar and Sherali Zeadalli. 2020. Machine learning and data analytics for the IoT. *Neural Computing and Applications* 32 (2020).

Vincent Gramoli. 2020. From blockchain consensus back to Byzantine consensus. *Future Generation Computer Systems* 107 (2020), 760–769. <https://doi.org/10.1016/j.future.2017.09.023>

D. Huang, X. Ma, and S. Zhang. 2020. Performance Analysis of the Raft Consensus Algorithm for Private Blockchains. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 50, 1 (2020), 172–181. <https://doi.org/10.1109/TSMC.2019.2895471>

Hyo Jin Jo, In Seok Kim, and Dong Hoon Lee. 2015. Efficient and privacy-preserving metering protocols for smart grid systems. *IEEE Transactions on Smart Grid* 7, 3 (2015), 1732–1742.

Zhiyang Ju, Hui Zhang, and Ying Tan. 2020. Distributed deception attack detection in platoon-based connected vehicle systems. *IEEE transactions on vehicular technology* 69, 5 (2020), 4609–4620.

SAHU AMIYA Kumar, Sharma Suraj, and Puthal Deepak. 2020. Lightweight Multi-Party Authentication and Key-Agreement Protocol in IoT Based e-Healthcare Service. *ACM Trans. Multimedia Comput. Commun. Appl.* 0, ja (2020). <https://doi.org/10.1145/3398039>

Beibei Li, Rongxing Lu, Wei Wang, and Kim-Kwang Raymond Choo. 2017. Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system. *J. Parallel and Distrib. Comput.* 103 (2017), 32–41.

R. Li, T. Song, B. Mei, H. Li, X. Cheng, and L. Sun. 2019. Blockchain for Large-Scale Internet of Things Data Storage and Protection. *IEEE Transactions on Services Computing* 12, 5 (2019), 762–771. <https://doi.org/10.1109/TSC.2018.2853167>

Shang Li and Xiaodong Wang. 2015. Cooperative change detection for voltage quality monitoring in smart grids. *IEEE Transactions on Information Forensics and Security* 11, 1 (2015), 86–99.

Wenjia Li and Houbing Song. 2015. ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE transactions on intelligent transportation systems* 17, 4 (2015), 960–969.

Xin Li, Minmei Wang, Huazhe Wang, Ye Yu, and Chen Qian. 2019. Toward Secure and Efficient Communication for the Internet of Things. *IEEE/ACM Trans. Netw.* 27, 2 (2019), 621–634. <https://doi.org/10.1109/TNET.2019.2893249>

Gaoqi Liang, Junhua Zhao, Fengji Luo, Steven R Weller, and Zhao Yang Dong. 2016. A review of false data injection attacks against modern power systems. *IEEE Transactions on Smart Grid* 8, 4 (2016), 1630–1638.

J. M. Mendel and D. Wu. 2017. Critique of “A New Look at Type-2 Fuzzy Sets and Type-2 Fuzzy Logic Systems”. *IEEE Transactions on Fuzzy Systems* 25, 3 (2017), 725–727. <https://doi.org/10.1109/TFUZZ.2017.2648882>

Esther Mengelkamp, Benedikt Notheisen, Carolin Beer, David Dauer, and Christof Weinhardt. 2018. A blockchain-based smart grid: towards sustainable local energy markets. *Computer Science-Research and Development* 33, 1-2 (2018), 207–214.

Michael Mylrea and Sri Nikhil Gupta Gourisetti. 2017. Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In *2017 Resilience Week (RWS)*. IEEE, 18–23.

John A Nix. 2016. Secure PKI communications for machine-to-machine modules, including key derivation by modules and authenticating public keys. <https://patentimages.storage.googleapis.com/24/4d/11/4e1186842d8b5a/US9998280.pdf> US Patent 9,288,059.

Jonathan Petit and Steven E Shladover. 2014. Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent transportation systems* 16, 2 (2014), 546–556.

- Ziaur Rahman, Ibrahim Khalil, Xun Yi, and Mohammed Atiquzzaman. 2021. Blockchain-Based Security Framework for a Critical Industry 4.0 Cyber-Physical System. *IEEE Communications Magazine* 59, 5 (2021), 128–134. <https://doi.org/10.1109/MCOM.001.2000679>
- Ziaur Rahman, Xun Yi, and Ibrahim Khalil. 2022. Blockchain based AI-enabled Industry 4.0 CPS Protection against Advanced Persistent Threat. *IEEE Internet of Things Journal* (2022), 1–1. <https://doi.org/10.1109/JIOT.2022.3147186>
- Mingshun Sun, Ali Al-Hashimi, Ming Li, and Ryan Gerdes. 2020. Impacts of constrained sensing and communication based attacks on vehicular platoons. *IEEE transactions on vehicular technology* 69, 5 (2020), 4773–4787.
- T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella. 2017. On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration. *IEEE Communications Surveys Tutorials* 19, 3 (2017), 1657–1681. <https://doi.org/10.1109/COMST.2017.2705720>
- N. B. Truong, K. Sun, G. M. Lee, and Y. Guo. 2020. GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. *IEEE Transactions on Information Forensics and Security* 15 (2020), 1746–1761. <https://doi.org/10.1109/TIFS.2019.2948287>
- F. Tschorsch and B. Scheuermann. 2016. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Communications Surveys Tutorials* 18, 3 (2016), 2084–2123. <https://doi.org/10.1109/COMST.2016.2535718>
- L. Wang. 2017. A New Look at Type-2 Fuzzy Sets and Type-2 Fuzzy Logic Systems. *IEEE Transactions on Fuzzy Systems* 25, 3 (2017), 693–706. <https://doi.org/10.1109/TFUZZ.2016.2543746>
- S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Wang. 2019a. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 49, 11 (2019), 2266–2277. <https://doi.org/10.1109/TSMC.2019.2895123>
- S. Wang, A. F. Taha, J. Wang, K. Kvaternik, and A. Hahn. 2019b. Energy Crowdsourcing and Peer-to-Peer Energy Trading in Blockchain-Enabled Smart Grids. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 49, 8 (2019), 1612–1623. <https://doi.org/10.1109/TSMC.2019.2916565>
- M. Wollschlaeger, T. Sauter, and J. Jasperneite. 2017. The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0. *IEEE Industrial Electronics Magazine* 11, 1 (2017), 17–27. <https://doi.org/10.1109/MIE.2017.2649104>
- Guomin Yang and Chik How Tan. 2011. Certificateless cryptography with KGC trust level 3. *Theoretical Computer Science* 412, 39 (2011), 5446 – 5457. <https://doi.org/10.1016/j.tcs.2011.06.015>
- Mahdi Zamani, Mahnush Movahedi, and Mariana Raykova. 2018. RapidChain: Scaling Blockchain via Full Sharding. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. Association for Computing Machinery, 931–948. <https://doi.org/10.1145/3243734.3243853>
- Chunheng Zhao, Jasprit Singh Gill, Pierluigi Pisu, and Gurcan Comert. 2021. Detection of false data injection attack in connected and automated vehicles via cloud-based sandboxing. *IEEE Transactions on Intelligent Transportation Systems* 23, 7 (2021), 9078–9088.

Received 27 March 2023; revised April 2023; accepted June 2023