Important declarations

Please remove this info from manuscript text if it is also present there.

Associated Data

Data not supplied by the author for this reason:
The article is based on modeling and implementation rather than data focus under the project. We are happy to provide further documents if required.

Required Statements

Competing Interest statement:
No competing Interest. Thanks

Funding statement:
No funding

Blockchain and AI-enabled false data detection and reputation preservation for smartgrid cyber-physical system

Rahman Ziaur [Corresp., 1], **Xun Yi** [2], **Ibrahim Khalil** [2], **Adnan Anwar** [3]

[1] Computer Science and Engineering, RMIT University, Melbourne, VIC, Australia

[2] Computer Science and Engineering, RMIT University, Melbourne, Victoria, Australia

[3] School of IT, Deakin University, Melbourne, VIC, Australia

Corresponding Author: Rahman Ziaur
Email address: rahman.ziaur@rmit.edu.au

Since the beginning of this decade, several incidents report that smart grid false data injection attacks cause huge industrial damage and loss of lives. For example, forging the metering status is an immensely growing attack that leads to end-user conflict by abolishing trust with service providers. Looking after those sensitive data, only using conventional cloud-driven and centralized techniques such as supervisory control and data acquisition (SCADA) system can be misused to maliciously update the device legitimate status. As investigated, the existing centralized false data detection approach based on state and likelihood estimation have a reprehensible trade-off in terms of trust, cost, and efficiency. Blockchain with Artificial Intelligence has shown its potentials to solve trust and detection challenges encountered by today's Smart grid cyber-physical 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 smart grid rules and behaviors. Besides improving the detection accuracy and eliminating single point of failure, the contributions include the appropriation of fuzzy AI functions within the edge node before authorizing status data by a Blockchain network. Finally, thorough experimental evaluation validates the effectiveness of the proposed model.

Blockchain and AI-enabled False Data Detection and Reputation Preservation for Smart grid Cyber-physical System

Ziaur Rahman[1], **Xun Yi**[1], **Ibrahim Khalil**[1], **and Adnan Anwar**[2]

[1]**School of Computer Science & Software Engineering, RMIT University, VIC 3000**
[2]**School of Information Technology, Deakin University, VIC 3220**

Corresponding author:
Ziaur Rahman[1]

Email address: rahman.ziaur@rmit.edu.au

ABSTRACT

Since the beginning of this decade, several incidents report that smart grid false data injection attacks cause huge industrial damage and loss of lives. For example, forging the metering status is an immensely growing attack that leads to end-user conflict by abolishing trust with service providers. Looking after those sensitive data, only using conventional cloud-driven and centralized techniques such as supervisory control and data acquisition (SCADA) system can be misused to maliciously update the device legitimate status. As investigated, the existing centralized false data detection approach based on state and likelihood estimation have a reprehensible trade-off in terms of trust, cost, and efficiency. Blockchain with Artificial Intelligence has shown its potentials to solve trust and detection challenges encountered by today's Smart grid cyber-physical 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 smart grid rules and behaviors. Besides improving the detection accuracy and eliminating single point of failure, the contributions include the appropriation of fuzzy AI functions within the edge node before authorizing status data by a Blockchain network. Finally, thorough experimental evaluation validates the effectiveness of the proposed model.

INTRODUCTION

The world has experienced a significant number of cyberattacks since the beginning of the industrial transformation, specifically at the age of Industry 4.0. According to the Internet Crime Complaint Center of US FBI, 95% of the recorded breaches targeted critical Industry 4.0 infrastructure such as Smart grid, public hospital records, etc. In July 2020, Texas's State power grid system was hacked where the attacker tried to spoof the system's monitoring tools to inject false data purposing to bully the whole system. This was not the first time; a similar scenario happened in Dec 2015 when a massive blackout impacted due to Ukrain's power grid attack. The recent incidents reveal that the global Smart grid ecosystem is extremely vulnerable to cyber intrusions. Distributed ledger, popularly known as Blockchain, has immense potential to secure the smart grid cyber-physical system for flawless power management. Rule based AI technique such as Fuzzy logic, Blockchain protocols has the potential to detect anomalous events based on the system behaviors. Instead of centralized monitoring, distributed and transparent control by both consumer and service provider can be amazingly advantageous if there is a reliable peer responsible for tracking continuous and desired power delivery. False data injection attack is an unprecedented attack that often raises conflict against the reliable operation of the physical energy grid and imbalances the supply-demand chain. Adding false data or compromising grid metering appliances usually happens for different reasons. Any unauthorized intermediaries or even trusted stakeholders intentionally or mistakenly can deliberately inject malicious data from any of its connected power sensors. If the system control is maintained based on the trust employed through a trusted third party (i.e., service provider), the chance of potentials threat rises exponentially. In line with that, preserving incorrect or faulty grid data can easily foster conflict among the end-users and trusted service providers. Conventionally, the data associating smart meter(SM),

phasor management unit (PMU) is maintained by a cloud from the provider side. Consumers are allowed to see their bills and consumption but barely have any control authority Wollschlaeger et al. (2017). At this point, if any grid account is compromised with unwanted data the sole responsibility goes to those are entitled to control the system such as SCADA Ali et al. (2019); Anwar et al. (2015); Anwar et al. (2017). Not only data forgery, but either negligible or erroneous data may also appear due to technical errors sometimes, whatever the reasons are, that deserve proper preservation for extensive record-keeping and monitoring. In the smart grid system, this status history often constructs a reputation that is necessarily important for further decision making, cost measuring, and predictive maintenance Wang et al. (2019b).

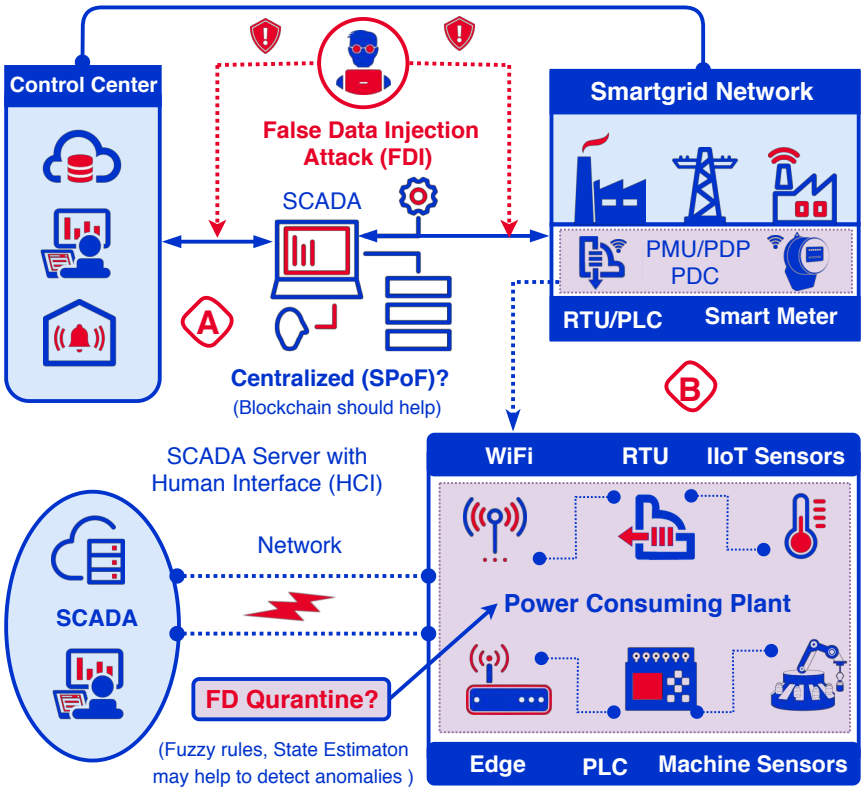


Figure 1. A) False Data Injection (FDI) in a SCADA-controlled Smartgrid CPS B) False Data Filetering (Quarantine) Challenges.

Challenges and Perspectives

As the existing detection approaches demand proper revision towards ensuring transparency and accuracy, the research community has expressed their deep concern for convincing solutions. However, blockchain either permissioned or public has already proved its ability to preserve transparent data transmission and sharing generated from distributed network with desired anonymity and immutability. It works through adaptable consensus Gramoli (2020) and smart contract mechanism. False data attack is a new kind of attack against the smart grid operation that consequences with specific disruption because of misleading information allegedly appended into its one of the major operational module names state estimator Wang et al. (2019b). Detecting infected data, assuring how much the grid is compromised should be done in a way that is confidentially secure. Due to it's immutable, efficient, reliable and enormously accessible behaviors, blockchain can be an exciting solution in response to this false data injection and transparency problem Li et al. (2019). Throughout this work, we have proposed a smart grid system model aligned with blockchain to detect anomalous data. Next, a reputation preservation process is proposed. To secure status data while travelling from sensors (e.g., PMU, smart meters) to blockchain ledger, we have incorporated a customized digital signature mechanism, Fuzzy Rule based detection accuracy which works following Infected Data Detection (IDD) algorithm Mendel and Wu (2017) Wang (2017). Besides, we have designed another functional algorithm that is capable to communicate with the blockchain ledger.The fuzzy based

detection methods shows convincing accuracy and blockchain aligned reputation preservation process brings transparent and secure outlook of the smart grid management Li et al. (2017).

Contributions and Organizations

This article motivates to address and demonstrate a Blockhain and AI-enabled false data detection and reputation preservation for smart grid cyber-physical system (CPS) Aazam et al. (2018) Li et al. (2017). The specific contributions claimed are as follows.

- The proposed AI-enabled false data detection technique is able to filter data anomalies based on the behavior rules. As justified in the later sections, the fuzzy-based model has comparatively higher accuracy and sensitivity.
- The proposed model incorporates a novel reputation preservation mechanism based on the detected data and measurement devices such as PMU, smart meters, etc. The reputation status of the measurement units helps authority to be aware of that devices and protect system from being attacked.
- Blockchain based transaction verification ensures the trust and security built through a collaborative way instead of relying on a single party. It eliminates PKI-driven certificate authority (CA) and centralized SCADA system which shields the smartgrid CPS apart from single-point-of failure.

Therefore, the rest of the article is organized as follows. Background and Related work section explains the suitability of Blockhain and AI-aligned approach for false data detection and preservation along with security assumption and trust model. As one of the core components, Anomaly detection and preservation section explains fuzzy rule specification based on the smartgrid stable behavior and addresses a novel reputation updating algorithm Li et al. (2017) . The next core section namely Blockchain and Data preservation discusses the device registration and communication process including the respective algorithms. The evaluation and result analysis section justifies the contributions as claimed above through required graphical representation.

BACKGROUND AND RELATED WORKS

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

Terms/Notations	Elaboration & Description
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
MF	Membership Functions
MSP	Membership Service Provider
ML	Machine Learning
P2P	Peer to Peer Network
SC	Smart Contract

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

Blockchain Technology for Smart Grid CPS

The emerging blockchain technology has shown immense potentials to secure and enhance the smart grid operations and management. Because of its self-governing smart contract protocols and consensus driven block verification, its integration to the smart grid increases data and communication integrity and security Taleb et al. (2017). As shown in the Fig 2, blockchain is an expanding and unchangeable list of records consisting of blocks that are connected to each other using a secure and immutable hash algorithm. The network works on the distributed peer-to-peer (P2P) network constituted by the smart grid stakeholders such as power source, service provider, distributor, consumers, etc. Unlike centralized cloud-driven service or SCADA blockchain ensures multi-party authorization which in essence eliminates the Single-point-of-failure (SPoF) Tschorsch and Scheuermann (2016).

Blockchain suitability for Smartgrid

Before storing a grid transaction into an associated ledger it needs to be consented by the contributory peers through a special process called consensus mechanism. Earlier generation Blockchain such as Bitcoin (BTC), Ethereum (ETH) incorporate Proof-of-Work (PoW) type of consensus which is often criticised because of its significantly slower transaction processing rate. Based on the joining right blockchain can be either public or consortium in nature where only authorized users are allowed to join and contribute. Apart from the PoW, consortium Blockchain such as Corda, Hyperledger (HLF), Ripple incorporate fault tolerance consensus techniques, i.e. Byzantine/Crash Fault Tolerance, etc. The later kind exclude longer identity and transaction verification, thus has higher throughput and negligible delay latency Li et al. (2019). For example, for a BTC and ETH the transaction processing rate (known throughput, Tx/s) ranges from 4 to 15 Tx/s where HLF an process 3,000 to 20,000 Tx/s. As excluding computation-intensive validation, it eliminates conventional reward or incentives which makes consortium BC a great alternative for real time and critical infrastructure such as Smartgrid, Industrial IoT (IIoT) etc Truong et al. (2020).

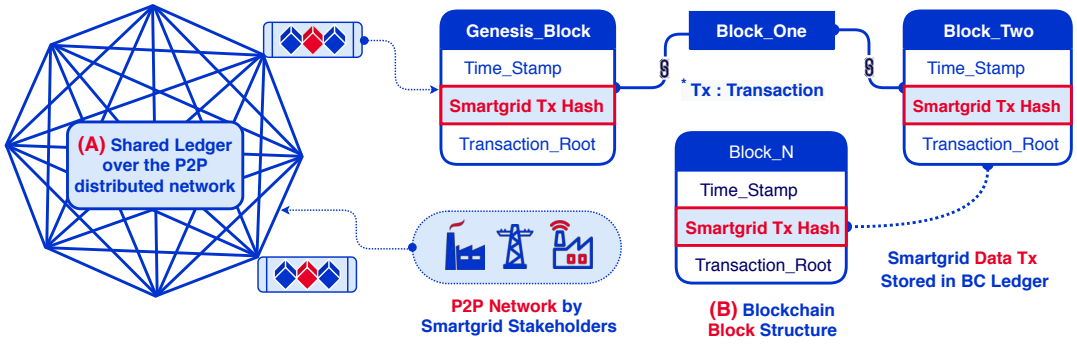


Figure 2. Sample Blockchain structure consisting of Smartgrid transaction (Tx. A) Peer to peer (P2P) network where Blockchain peers comminicate with each other. B) Blockchain Block structure

Fuzzy Logic for FDD

Fuzzy logic (FL) is a form of AI reasoning that does decision in a way similar to humans. It's computer-digestible logic block takes precise input and outcomes a definite output equivalent to real-world reasoning. Smart grid follows particular rules and behaviour that can be logically translated into input membership functions (MF) of AI fuzzy logic Mendel and Wu (2017). Thus, the several MFs together build intelligence for a required decision of the smart grid CPS. Unlike Boolean logic or probability theory, its decision making process relies on the degrees of truth factor between $TRUE$ and $FALSE$. Though, FL is based on the levels of probabilities of input variables towards the purposeful output, it is actually a subset of artificial intelligence (AI) and can be trained using software, hardware or both. The fundamental FL architecture contains minimum 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 $\mu_f : y \rightarrow [0,1]$. The advanatges of FL system are as follows Wang (2017).

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

- It can dynamically work with the imprecise, anomalous input data. The reasoning and decision making can be made within less power constraints which can save system deployment costs.

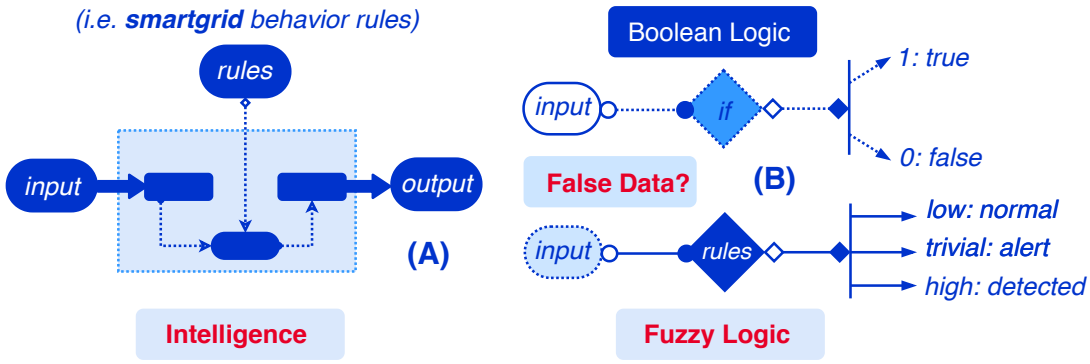


Figure 3. Fuzzy Logic (FL) components and salient characteristics that makes it distinct from its counterpart name Boolean Logic.

The Figure 2 shows the basic components of fuzzy logic and how it varies from Boolean logic. The rule can be any certain conditions or any behaviour. For example, in smart grid variation of active power within one time interval can be assumed less than an experienced threshold. The edge-node trained with this smart grid behaviours can detect data status, identify the source device if such condition (as by MF) does not meet. The difference of Active Power P, flowing into a bus and flowing out the bus ought to be less than an experienced threshold. The considered rules will be explained in later section of the paper.

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 Anwar et al. (2017, 2016). Li et al. (2017) proposed a secure model for data attack detection. Work above seems to have better performance as claimed through their co-simulation based evaluation. In Li and Wang (2015) Liang et al. (2016) 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 contact was explained by the authors to enhance the security and resilience of the power gridMengelkamp et al. (2018) Mylrea and Gourisetti (2017). 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 algorithmLi et al. (2017). In work, the authors have considered distributed host based effort instead of the distributed ledger, and the rules assumed to evaluate seems to be not exceeding four host monitors. We have extracted 14 rules throughout our investigations, but even this number not seems to be that large portraying an entire grid scenario. 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 arisen 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 light-weight privacy preserving technique for distributed smart metering has also claimed the speed of authentication Dinh et al. (2018).

DESIGN CONCEPTS AND SYSTEM MODEL

The proposed design concepts include three different components. Firstly, a fuzzy-based false detection technique in the edge-end that filters data before sending it to Blockchain network. Secondly, the Blockchain authenticates data and generating source devices upon a certificateless and collaborative signing process Kumar et al. (2020) Aitzhan and Svetinovic (2018a). Finally, only the verified data are stored in the storage node. Considering the salient features the proposed framework incorporates

permssioned blockchain and Distributed Hash Table (DHT) mechanism for demonstration and evaluated demonstration Wang et al. (2019a) Truong et al. (2020). However, it supports any type of blockchain and storage service. Figure 4 shows the the high-level view of the proposed detection and reputation preservation approach. The communication flow of the proposed system can be divided into three different parts that are discussed as follows.

Sensor to Edge Communication

Smart grid Cyber-physical system employs mainly power sources, service providers and consumers. The Industrial Internet of Things (IIoT) sensors are connected to the Global Remote Terminal Unit (RTU) and the source or consumer machine sensor i.e., Micro-electrical Mechanical System (MEMS) are connected to Programmable Logic Controller (PLC) Jo et al. (2015). The IIoT or MEMS send data to the destination through the constituted Edge devices irrespective of sources either wired or wireless Aitzhan and Svetinovic (2018b); Erwin Adi and Zeadalli (2020) . For example, if MEMS are attached with an WiFi Edge protocols upon PLC, the source power consumption data is dynamically transported to the internet over the edge devices. Portion A of Figure 4 shows the sensor-edge communication where the proposed fuzzy rules work to detect any data anomalies Mendel and Wu (2017).

Blockhain ensures Secure Data Transport

Instead of conventional SCADA system, the edge data is authenticated via a blockchain network to reduce the chance of single-point-of-failure(SPoF) and centralized trust. The proposed solution incorporates a certificate-less multi-signature based device and data authentication over the peer-to-peer 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 delay latency the proposed model constitutes consortium blockcahin. It establishes a secure communication with the smart grid sensors/MEMS and validate transported data. Potion B of Figure 4 depicts the secure data transport using Blockchain. The later section explains the multi-signature based, certificate-less authentication on the Blockhain Zamani et al. (2018) Cho et al. (2020).

Reputation Preservation and Storing

The reputation preservation algorithm works within the detection model update the reputation of sensor devices. Once the sensors/MEMS seems to be generating false data, it will update its individual status. The reputation along with the data-transaction will be recorded in the Blockchain ledger and data will be stored in an off-chain storage. Considering its salient feature, the proposed framework incorporates Distributed Hash Table (DHT) such as Interplanetary File System (IPFS), Kademlia, etc Huang et al. (2020). Reputation preservation happens in the earlier portion as shosn by A and portion C of Figue 4 portrays the storage mechanism. However, storing data directly in the Blockchain network, even in an encrypted form threatens consumer or stakeholder privacy and in essence it does not comply the privacy standards Li et al. (2019).

Threat Model

The design principles of the proposed model is based on considered threat model. The decentralized blockchain ensures that an attacker is unable to corrupt the consortium network. Any unauthorised peer or adversary cannot modify the blockchain ledgers which will imply the resource that is compromised. The threat model includes that an unauthorised party or adversary is unable to impersonate as the associated multi-signature cannot be tempered or forged. Therefore, the security threats can be generalized into two broad categories. Firstly, an internal party or peer disguising in a Byzantine way who probably has been granted access to smartgrid data Zamani et al. (2018). Secondly, an honest or trusted peer 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 contract contains token validation technique which is refreshingly expired after a particular time or transaction protects the network from being compromised with the latest type of threat. However, the blockahin ledger will record the reputation of the malicious peers and would block temporarily or permanently. Byzantine Fault Tolerance (BFT) or Crash Fault Tolerance (CFT) technique ensures the system running smoothly even after some peers have been suspended. Besides the security threats, the model considers the privacy of the stakeholders and its data. The encryption and partial secret of the multi-signature ensures the pseudo-anonymity whereas,

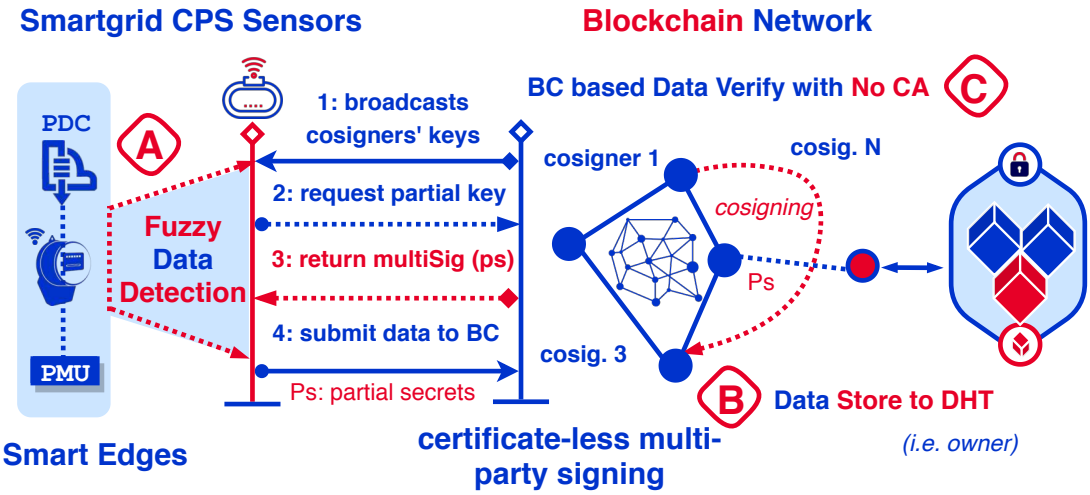


Figure 4. High level representation of the propsed Blockchain and AI-aligned False Data Detection and Reputation Preservation for Smartgrid CPS. A) Sources devices (i.e. PMU, smart meter, etc) send data through edge gateway B) Client submit data-transaction to Blockchain network (i.e. Key generation and distribution (KGD) consortium) C) Upon successful verification data-transaction along with detection status and reputation are recorded in the Ledger and data are stored in Distributed Hash Table Storage (i.e., IPFS, Kademila, etc).

consortium blockahin itself only allows authorized peers which meets the privacy challenges of the smart grid CPS Gramoli (2020).

Trust Assumption

The proposed model assumes that peers constitute Blockchain network are honest or semi-honest. The model obviates the Membership Service Providers which are equivalent Certificate Authority (CA) on Public Key Infrastructure (PKI) Nix (2016). As investigated throughout the centralized SCADA or CA it increases the chance of being compromised and SPoF. Besides, the Elliptic Curve (EC) based cryptgraphic primitives and hash function are assumed to be particularly secure. This means the attackers are not able to extract keys using reveres exponentiation, break the hash algorithms or temper the multi-signatures. In addition, the model considers that the data transfer occurs over the insecure network or internet. The next section discusses the proposed false data detection and preservation mechanism Yang and Tan (2011).

ANOMALY DETECTION AND UPDATING REPUTATION

As mentioned earlier, In usual operational circumstances, the smart grid operates on normal stable status. That means, associated state parameters and variables differ in an interchangeably balanced manner. For example, the power-grid follow specific behaviors according to Kirchhoff's current/Voltage law, demand-response constraints, etc Yang and Tan (2011). Thus, any variable state changes due to system fault or demand variation on a particular bus(transmission line) consequences corresponding state changes and produces anomalous data. However, smart grid anomaly can be identified if any variable change occurs on one bus without affecting the parallel variables Li et al. (2019) . The anomalies may occur because of PMU (Phasor Measurement Unit) breakdown or malicious activities. In this paper, we only focus on anomalous data generated from a possible compromised PMU, thus the paper concentrates on measurement data. As discussed in the related work section, there are several existing approaches to determine smart grid device malfunction. Being motivated from there concept Li et al. (2017) Li and Wang (2015), Mylrea and Gourisetti (2017), we have proposed a Fuzzy based system to filter data quality before processing it further. The fuzzy based technique works upon several rules extracted from smart grid normal operation behaviour. The following subsection explains those rule specification.

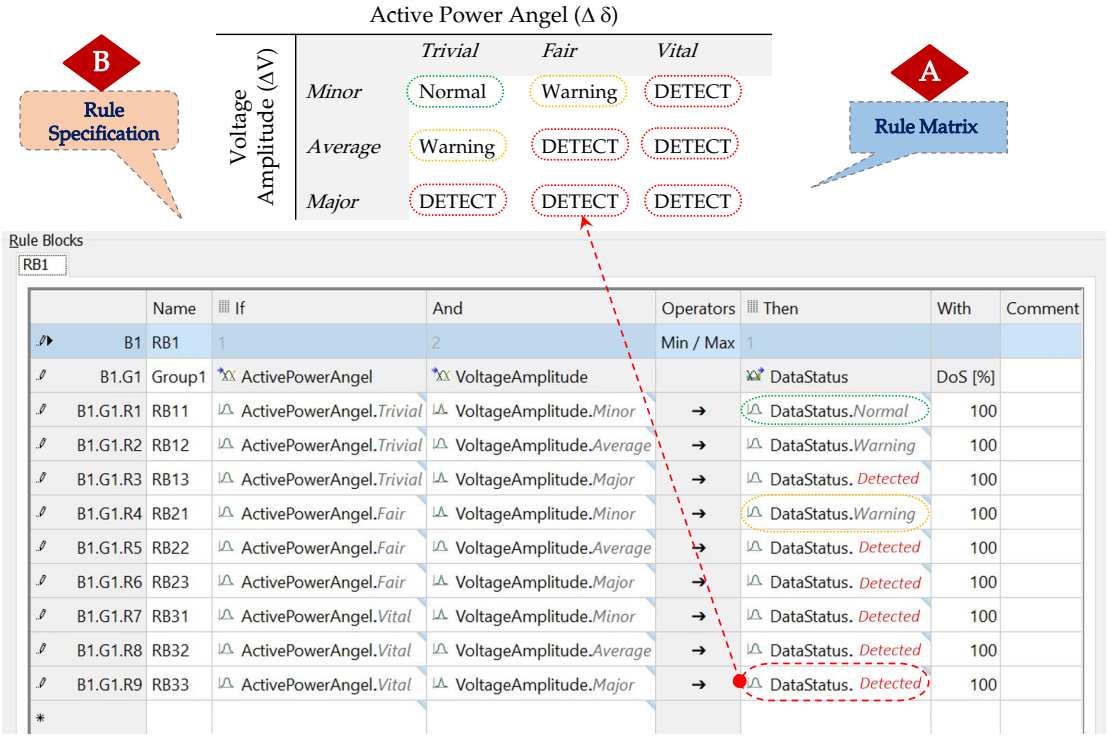


Figure 5. Behavioural Rule extraction and its corresponding fuzzy representation. A) Rule mtraix for different status B) Rule specifications

Rule Specifications

When a smart grid CPS is under usual operation all of its state variables follows particular constraints and hold desired properties. For example, power (P) meets the following conditions.

- $P_{min} < P^t < P_{max}$ power at time t should very in an range of (P_{main}, P_{max}).
- $\mid P^t - P^{t-1} \mid < P_\Delta$ power variation at t interval should be less than the threshold.

The following Table 1 shows similar rules considered. These are some fundamental rule specifications to detect false data due to the anomalous PMU activities.

Sl	Behaviour Rules	Variable Description
1	$\Delta L_{Mvar} < L_{Mvar\Delta}$	System Load $Mvar$ and its variation
2	$\lvert F_i^t - \widehat{F}_i^t \rvert \leq \tau_F$	Power flow measured at t of i'th PMU
3	$\Delta\delta < \delta_\Delta$	Active Power Angle δ
4	$\Delta V < V_\Delta$	Voltage amplitude V variation
5	$\Delta L_{MW} < L_{MW\Delta}$	System Load L_{MW} and its variation

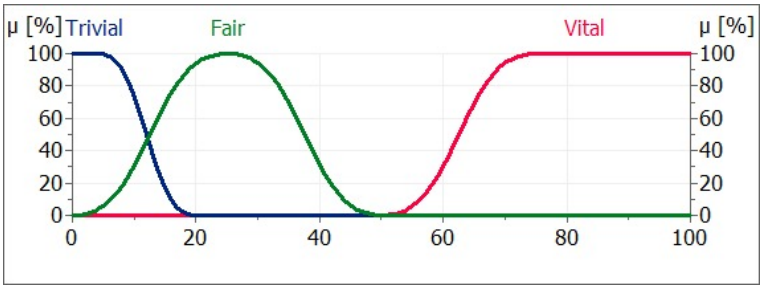
Table 2. Typical behaviour of power system rule examples

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

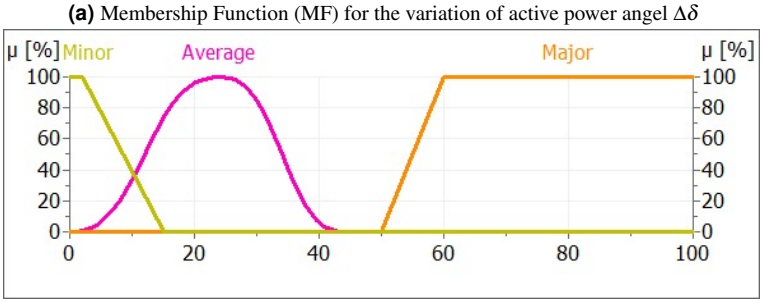
- Variation of P within one time interval t should be less than an experienced threshold $P_{thershold}$
- Absolute difference of active power P, flowing into a bus and flowing out the bus ought to be less than an experienced threshold.

The following Figure shows the rule-matrix that works to filter the data quality. First of it needs to classify the behaviour in different state Li and Wang (2015). For example, as per the Rule 4 of Table 2, the variation of voltage amplitude should not be always less than a measured threshold. The threshold

can be calculated following up the dynamic nature of the power system and previous records Liang et al. (2016). However, as settled that the voltage variation $| V_1 - V_2 |$ at a time t should be always less than the threshold $| V_t |$. Considering the severity of the difference it Fuzzy system classify, it as *minor*, *average* or *major*. Similarly, for active power angel it can be *trivial*, *fair* or *vital*. Based on the rule matrix as demonstrated by Figure 5(A), the corresponding fuzzy rules are listed by Figure 5(B). For example, if $\Delta\delta$ is *trivial* and ΔV is *minor* then fuzzy system will not mark it as *normal* and will send it to the blockchain peers for further processing. In different case, it will either *detect* data as anomalous or send it with a *warning* flag Mengelkamp et al. (2018) Mylrea and Gourisetti (2017).



(a) Membership Function (MF) for the variation of active power angel $\Delta\delta$



(b) Membership Function (MF) for the variation of voltage amplitude ΔV

Figure 6. Input MF definitions based on Smartgrid behavior rules

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 modeling include 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 ΔV is implemented with a *triangular* function, the detection varies from the *trapezoidal* MF. Targeting the maximum throughput, the proposed evaluation runs with the *gaussain* and its variant $SP-line$ MF. In a normalized $SP-line$ MF μ_i^m of order m (degree $(m-1)$ for the fuzzy subset $[a,b]$ over R (Real number range) the variation $\Delta : a = k_0 < k_1 < .... < k_{n+1} = b$ as $\mu : [a,b] \rightarrow [0,1]$. Here m_i is the multiplicity of the knot k_i.

Figure 2 depicts the respective membership of functions of based on the degree of variation of both voltage and active power angel as mentioned earlier. During the range selection of the demonstration, we have changed ranges to different level. For example, the following Figure 6 shows that if the variation exceeds about 50% then severity is classified as *vital* for Active Power Angel and *major* for Voltage Amplitude. However, based on the previous record of smart grid PMU data the ranges could varied to improve the system performance Wang (2017).

Following the similar process, the output membership functions has been selected. The *gaussian* and $SP-line$ seems to be brings the higher accuracy in compare to *trapezoidal* and *triangular* MF. The threshold basically depends on the previous record of the smartgrid CPS, however, it has been finalized one-fourth (25%) of the system over all deviation. That means it verdicts the *detected* if the average variation of $\Delta\delta$ and ΔV exceeds 25% altogether. Figure 7 shows the sample false data detection after

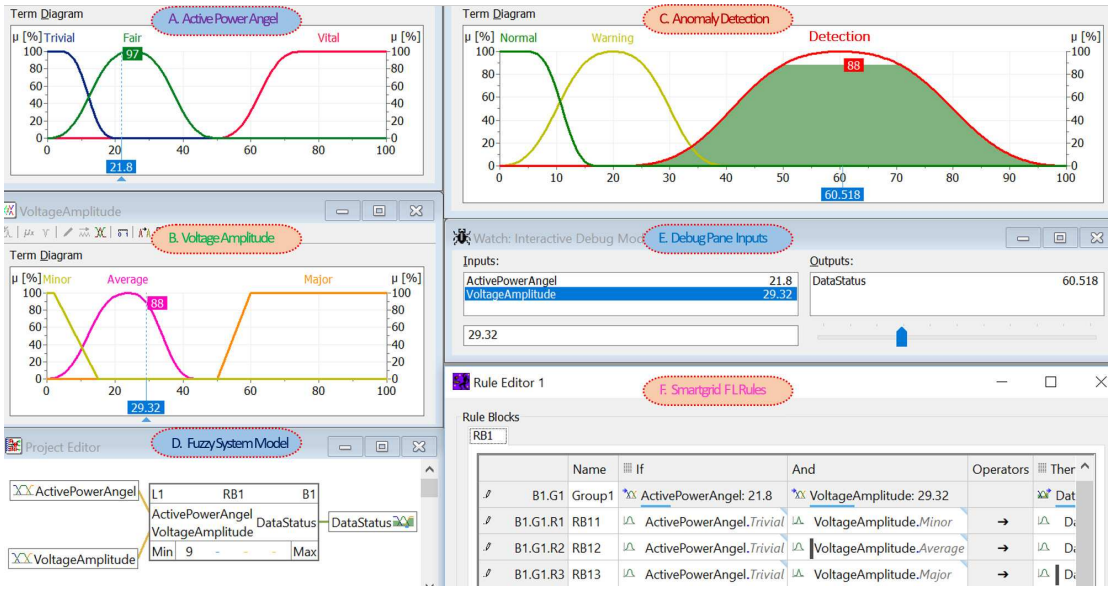


Figure 7. Complete debugging scenario of the fuzzy detection system. In includes A)-C) Input and output membership functions(MF), D) fuzzy system model, E) debugging pane and F) extracted behavior rules.

debugging the MF and its configured behavior rules. Here A and B are the input MF configuration based on $\Delta\delta$ and ΔV as explianed earlier Wang (2017). C depicts the corresponding output. For example, for a particular case, $\Delta\delta$ becomes 20% and ΔV varies in 30% 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 that latest status along with data transaction and source identities Mendel and Wu (2017).

PMU Reputation Updating

The probability distribution function (PDF) can be applied to determine the system reputation. For example, β distribution seems to be promising for a host-based 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).

Reputation Algorithm

The algorithm 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, i.e. $\Delta\delta$ (A) and ΔV (V). The respective functions or subroutine initializes the required system parameters such as initial reputation, associated values of the PMU.

Algorithm 1: Smart grid PMU reputation updating based on detection.

```
Input  : S – status either true or false
         R – reputation level
         L – PMU or sensor identities
         A – active power angel
         V – voltage amplitude
         D – detection level                          /* received data from fuzzy system */
Output : (ID,R_t, D)   – returns after algorithm execution
1 init := (ID, R, D, A, V)                            /* initializes after fuzzy detection */
2 for ID ← ID_i                                       /* for all identities n × ID_i */
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
```

Once values are set it checks if and only if the status are *true* or *false*. It updates the particular PMU (identified with the *ID*) status and exit process if the there is any false data found within the system as predicted by the earlier detection phase. After finalizing the detection and reputation updating process, now the data are ready to send to Blockchain for further verification and storing. The next section discusses how the smart grid detection status and reputation level are validated by the associated blockchain network and successfully stored for future maintenance and preservation. The smart grid data and the corresponding reputation now need to be transformed into blockchain transaction. Figure 8 shows the sample smartgid transaction to be transported over the internet.

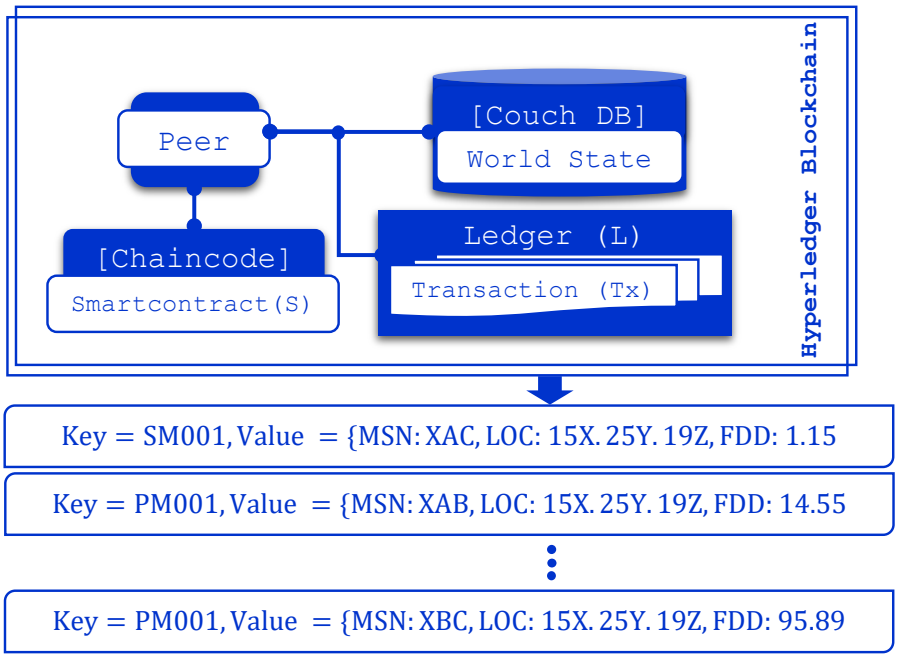


Figure 8. Sample smartgrid transaction belong to the ledger and typical world state database (i.e. Couch DB) with an interaction with chaincode smartontract.

BLOCKCHAIN VERIFICATION AND DATA PRESERVATION

In the proposed smartgrid data verification and preservation process, Consortium blockchain plays an indispensable rule. The PMU needs to get registered with the blockchain-based Key Generating and Distribution (KGD) system which is built upon 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 the partial secret (*PS*). It eliminates the the requirement of trusted third party (TTP) such as Certificate Authority of PKI. Before posting the transaction, smart grid PMU or sensors obtain public-private key pairs upon the completion of the registration process. The following part discusses how source devices are registered to the blockchain network. Then how it verifies particular transaction submitted to it.

Registering PMU

At the beginning, multi-party smart grid stakeholders agrees to build and share over the consortium blockchain (BC). Suppose, the owner (Bob), Buyer (Elen) and Insurer (Peter) along with other stakeholders cooperatively form the BC network that facilitates the Key Generating and Distribution (KGD) peers Li et al. (2019). Blockchain KGC peers broadcasts the system parameters (Y) all smart grid PMU have knowledge about. KGD peers keep their individual signer's secret such as S_1,S_2...S_n With the help of Edge computation capacity or its own ability, interested smartgrid device creates their own secret value $X_1, X_2, X_3 ... X_j$ generates respective public keys using X_j and the system parameter Y, where j is the number of interested devices at particular time t and n is the number of co-signing Blockchain peers Huang et al. (2020). PMU devices will contact the KGD with their identities $ID_1, ID_2, ...ID_j$. Upon receiving the request, KGD will generate a partial private seccret $PS_1, PS_2 ... PS_i$ for all requested devices and will cosign co-sign ID_i and PS_i using co-signers private key S_n. KGD sends the signed message back to the IIoT 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 $(Pk_1, Pk_2, ..., Pk_i, Sk_1, Sk_2, ..., Sk_i)$ 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.

Algorithm 2: Smartgrid Device Registraton with Blockchain KGD.

Input : ID_j – identities of the $j'th$ number of IIoT devices
Y – system parameters `/* prime numbers, primitive roots etc */`
Output : (Pk, Sk) – public and private key pairs `/* for all devices at t */`

```
setup(1^λ) → (Y)                                   /* system parameters (Y) initialization */
for ID ← ID_j do
    porocedure keyGen (Y, ID):                     /* key generation using system Y and identities */
    X_j ← genSk (Y,ID_j)                           /* IIoT devices generates own secret keys */
    requestSend (ID_j)                             /* devices send interests to join consoritum BC */
    PS_j ← genPS (ID_j)                            /* KGDs generates partial secret */
    multiSig(S_n, ID_j, PS_j)                      /* multi-sign using private keys S of n cosigners */
    responseReceived (ID_j)                        /* IIoT device receives PS from KGD */
    V[0,1,⊥ ] ← verify ()                          /* verify the certificate-less multisignatures */
    if V ← 1 then
        Sk_j ← genSk (Y,ID_j,X_j)                  /* sets IIoT device private key */
        Pk_j ← genPk (Y,X_j)                       /* sets IIoT device public key */
    end
end
```

Transaction Verification and Preservation

Once IIoT devices are successfully registered to the KGD upon the certificate-less cryptography and multi-signature based authentication, the sensor devices proceed further to send and store data. Usually, data gets transaction fashion before sending it to the blockchain network. The transaction includes the identity of the IIoT devices along with the action and timestamp at the time (T) of action (ACT). There can be different type 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 the ECDSA in our evaluation setup inside the Apache Kafka Framework of the Hyperledger

Irroha framework Li et al. (2019).

Algorithm 3: Smartgrid Transaction (Tx) verification and storing.

Input : T_x – IIoT data transactions
L – access control lists
σ – signaturues of the T_x
ID_j – identities of the $j'th$ number of IIoT devices
Y – system parameters /* prime numbers, primitive roots etc */

Output : $(V_{Id}, V_{Tx}, \mathsf{S})$ – set & return verification and storing flag *true*

```
create := (ID,L,Tx,σ,ADS)                          /* creates Tx using L ID and ADS */
signTx (Tx, Sk)                                    /* sign creates transactions */
castTx (Tx, σ)                                     /* broadcasts the original Tx and the signed one */
for Tx ← Tx_i                                      /* for all transaction n×T_x */
 do
    V1 ← verID (ID, Pk, Y)                         /* verifies the identites (ID) */
    V2 ← verTx (Tx,ID, Pk, σ)                      /* verifies the transactions (Tx) */
    if (V1 || V2) then
        S ← storeDHT (Tx, ID):                     /* store Tx into DHT and set S true */
    end
end
```

Here, the signature algorithm can be represented as a triple /4-tuple of probabilistic polynoimial-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_j, here the devices require the Access Control List (ACL) before Transaction (Tx) creation and signing (σ).The industry 4.0 devices along with the Edge Gateway are solely responsible to create the ACl list (L) in addition to signature (σ) generation and transaction(T_x) publishing.However, the same L will be required later to access data. The algorithm as shown in **Alg**.3, outcomes three different flags (V_1, V_2, S) set after successful execution. If the identities belong to the derived public keys, $V_1 := true$, while the certificate-less signature meets the condition as discussed earlier, $(V_2 := true)$.The Blockchain peers do the transaction (T_x) verification in response to the reception. Interchangeable verification procedure works in case of data accessing. Similarly, upon IIoT data transaction (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 T_x Pointer (Tp).

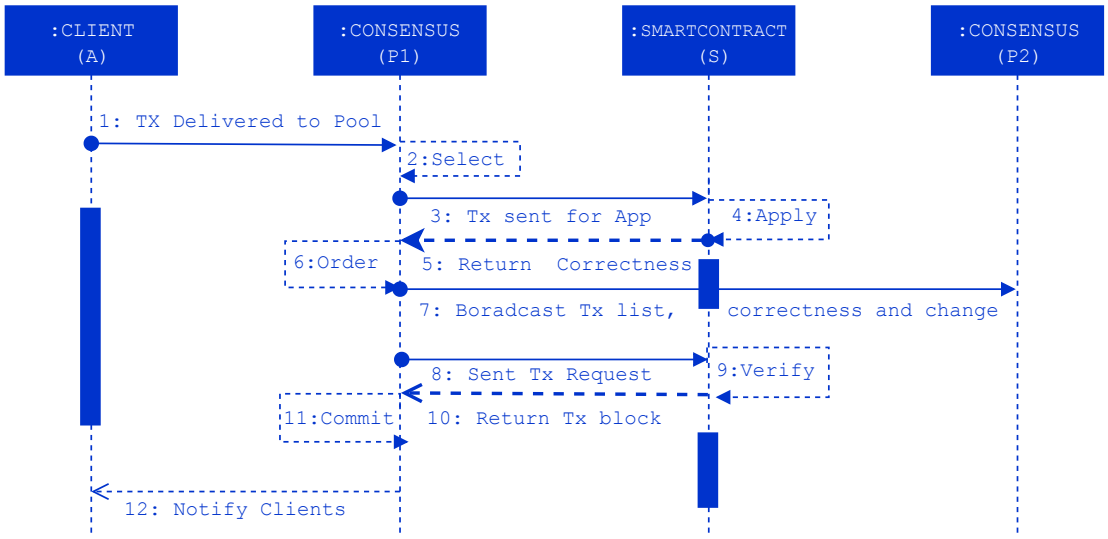


Figure 9. Communication sequence of a typical smartgrid tarnsaction within the Blockchain network. It employs the cycle among client devices that submit data, consensus peers and smart contact

Smart Contract and Consensus Implementation

The implementation required writing chaincodes (CC, special smart contract for Hyperledger Blockchain) against the respective ledger. The initial chaincodes provides authentication, access control and authorisation while other ensures logging besides the validation.Being an 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 certificate-less environment after eliminating Certificate Authority (CA) and Membership Service Provider (MSP), the dependencies of the open-source *shim* package needed customization Truong et al. (2020) Huang et al. (2020). By default it provides ledger/other CC accessing APIs, state variables or (T_x) context. Considering the data_pointer represents the cipher-text of the IIoT data.Assuming an *encryption* function $\mathbb{E}$ with public key (Pk_j):$data\_pointer = \mathbb{E}(mQAPk_j, device.id_j)$. A third party entity with a shared private key (Sk_j) 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 device (Edge Gateway), smart-contract and consensus protocols. Firstly, the transaction (Tx) is submitted to Blockchain network as a proposal using smart contract. The SDK of the network provide the application environment to check if the it valid. Once valid it needs to be consented by the consensus peers. In doing so it broadcast the Tx among all collaborating peers of the consortium and update the ledger Wang et al. (2019a).

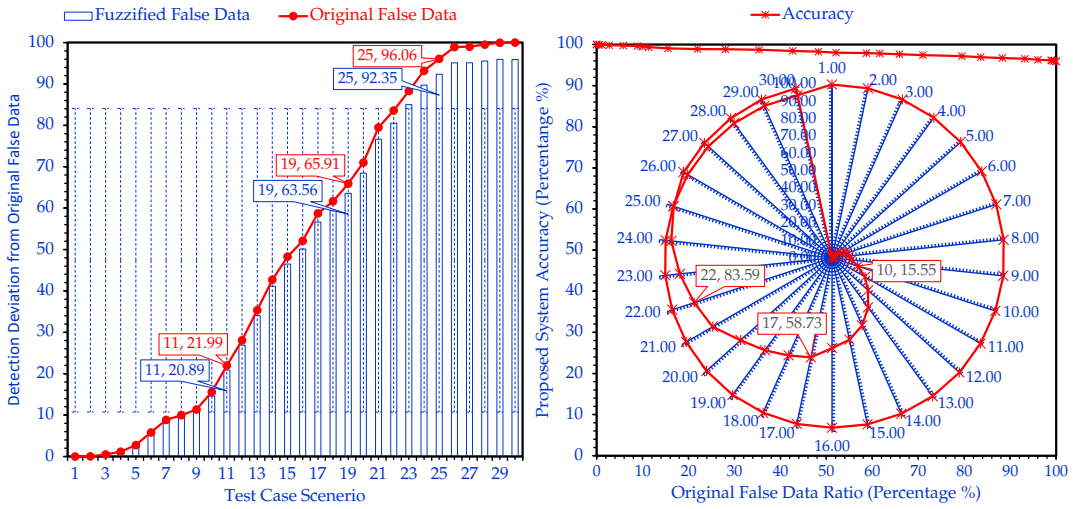


Figure 10. Detection deviation and accuracy of the proposed AI-enabled detection technique. It shows corresponding data for selected 30 test cases

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 Ledger 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 8GB RAM 2.50 and 2.71 GHz capacity.

0.1 Detection Accuracy

The built system were debugged for several cases. Among all debug, there have 30 test cases have been used to visualize the chart fuzzy system accuracy. The Figure 10 shows the detection trend of the system. The detection was made using the fuzzy input and respective membership function based on the rules considered. The rules rule Extraction section of the manuscript contains each rule by explaining the notation used. First the initial portion of Figure 10 shows the detection deviation from the original false data injected. The later portion presents the accuracy of the system. As we have considered two rules based on the variation of active power angel and voltage amplitude, therefore, the accuracy shown is only

the accuracy of the the selected membership functions which actually differs for higher number rules. It shows that it has higher accuracy when smart grid PMUs have less anomalies, and the accuracy slightly goes down for higher injection. That we have been trying to improve as a future scope of this project. The corresponding receiver operating characteristic (ROC) curve,of Figure 11 presents a graphical way between sensitivity and specificity for possible cut-off of those 30 test cases considered. It shows the system has maximum sensitivity with lesser false data which also portrays most usable cut-off. The highest cut-off has the maximum true positive rate together with the fewer false positive detection.

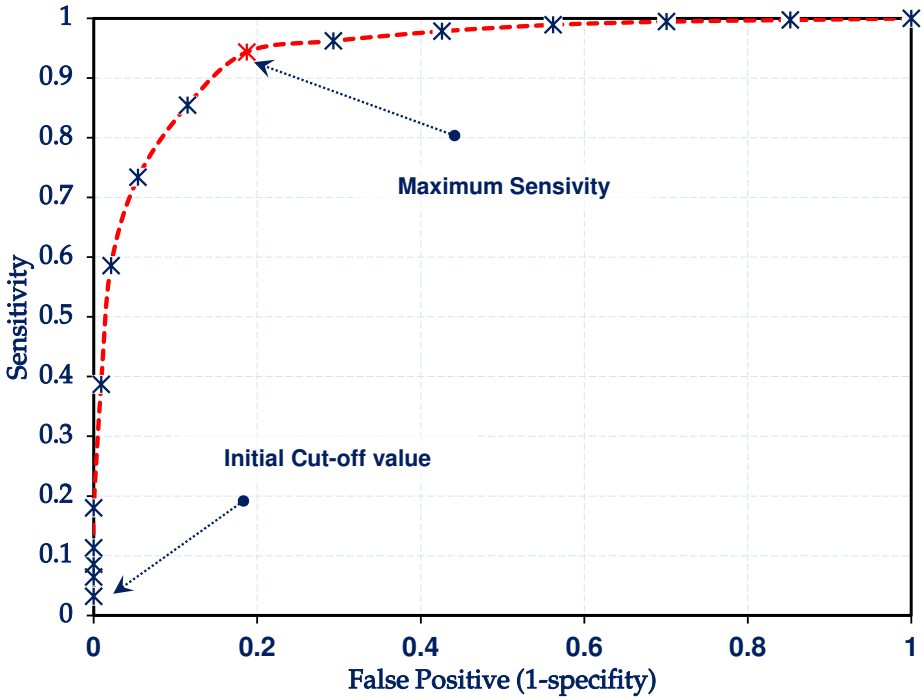


Figure 11. Receiving Operating Characteristic (ROC) analysis of the proposed Detection technique based on the considered test cases. It marks the initial cut-off and maximum sensitivity region of the proposed AI-enabled model.

0.2 Blockchain Network Performance

The HLF benchmarking results shows the performance based on four measurement metrics success rate (ρ), latency (Δ t and L) and the Throughput (P) and the resource consumption (W) for different test cases. Figure 12 shows the system performance under different number of workload (W) ranging from 0.1k to 1k workload where the HLF network occupies two (02) chaincodes, 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 the maximum success rate of 93% and average delay of 5 seconds. On the other hand, $READ$ operation seems to have higher throughput (up to 470 in maximum) on the similar success rate at its best. The average delay seems to be half of the write's delay as write has to incorporate OSNs on Apache Kafka. Table 3 shows the throughput (TP), success rate (SR) and delay (DEL) latency of the Blockchain deployment Truong et al. (2020).

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

	READ			WRITE		
WL	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
	110	3.5	6.68	10	0.5	9.92

Table 3. The Throughput (TP), Success Rate (SR) and Delay Latency (DL) for READ and WRITE operation of the smartgrid transaction (Tx). The above values are calculated based on teh Work Load (WL or Tx per second) as shown in the left-most column.

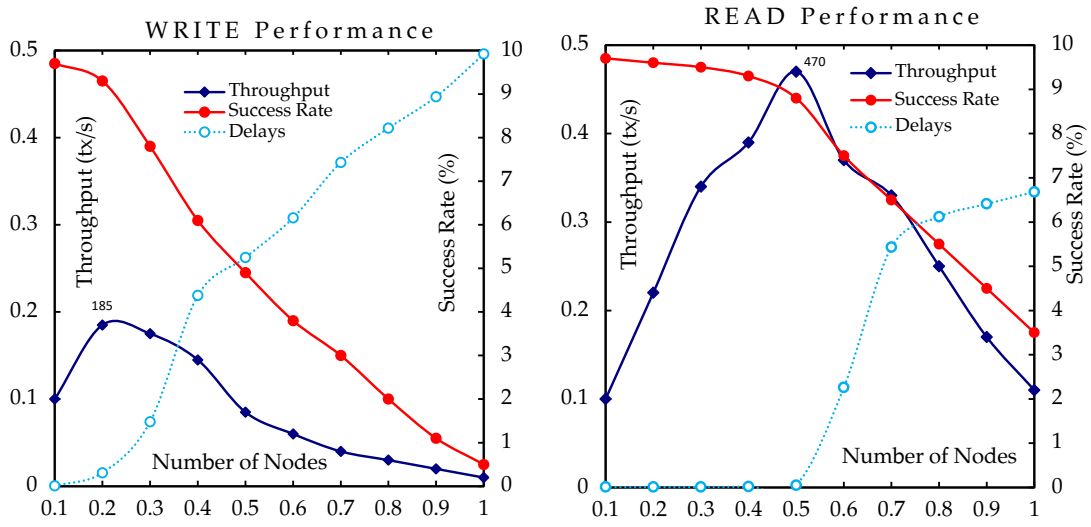


Figure 12. READ and WRITE performance of the deployed Blockchain network that securely record data and reputation and store data to the associated Distributed Hash Table (DHT)

1 CONCLUSION AND FUTURE SCOPE

In today's smart grid cyber-physical system, data integrity attacks like false data injection has been an ongoing concern. If the system has inaccurate data then any activities based on that anomalous data should go in vain and as a critical system it can outcome with operational failure, financial cost and live loss. The proposed blokchain and AI-enabled false data detection should help filtering anomalous data before sending it to further processing. The communication between smart grid edge and storage devices happen with a collaborative verification which in essence ensure the system's security and data safety. The system obviates the PKI-driven trusted certificate authority and the established centralized SCADA system. Thus it is able to eliminate the single-point of failure and single party dependency. The respective evaluation and result analysis section show that the proposed model has comparative higher accuracy. The performance of the blockchain network justifies the applicability of the proposed model for the PMU and sensors. The future scope include improving the accuracy for number of behavior rules and justifying the scalability for massive network.

REFERENCES

Aazam, M., Zeadally, S., and Harras, K. A. (2018). Deploying fog computing in industrial internet of

things and industry 4.0. *IEEE Transactions on Industrial Informatics*, 14(10):4674–4682.

Aitzhan, N. Z. and Svetinovic, D. (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):840–852.

Aitzhan, N. Z. and Svetinovic, D. (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):840–852.

Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., and Rehmani, M. H. (2019). Applications of blockchains in the internet of things: A comprehensive survey. *IEEE Communications Surveys Tutorials*, 21(2):1676–1717.

Anwar, A., Mahmood, A. N., and Ahmed, M. (2015). *False Data Injection Attack Targeting the LTC Transformers to Disrupt Smart Grid Operation*, pages 252–266. Springer International Publishing.

Anwar, A., Mahmood, A. N., and Pickering, M. (2016). *Intelligence and Security Informatics*, chapter Data-Driven Stealthy Injection Attacks on Smart Grid with Incomplete Measurements, pages 180–192. LNCS, Springer, Cham.

Anwar, A., Mahmood, A. N., and Pickering, M. (2017). Modeling and performance evaluation of stealthy false data injection attacks on smart grid in the presence of corrupted measurements. *Journal of Computer and System Sciences*, 83(1):58 – 72.

Anwar, A., Mahmood, A. N., and Tari, Z. (2017). Ensuring data integrity of opf module and energy database by detecting changes in power flow patterns in smart grids. *IEEE Transactions on Industrial Informatics*, 13(6):3299–3311.

Cho, E., Kim, J., Park, M., Lee, H., Hamm, C., Park, S., Sohn, S., Kang, M., and Kwon, T. T. (2020). Twinpeaks: An approach for certificateless public key distribution for the internet and internet of things. *Computer Networks*, 175:107268.

Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., and Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering*, 30(7):1366–1385.

Erwin Adi, Adnan Anwar, Z. B. and Zeadalli, S. (2020). Machine learning and data analytics for the iot. *Neural Computing and Applications*, 32.

Gramoli, V. (2020). From blockchain consensus back to byzantine consensus. *Future Generation Computer Systems*, 107:760–769.

Huang, D., Ma, X., and Zhang, S. (2020). Performance analysis of the raft consensus algorithm for private blockchains. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 50(1):172–181.

Jo, H. J., Kim, I. S., and Lee, D. H. (2015). Efficient and privacy-preserving metering protocols for smart grid systems. *IEEE Transactions on Smart Grid*, 7(3):1732–1742.

Kumar, S. A., Suraj, S., and Deepak, P. (2020). Lightweight multi-party authentication and key-agreement protocol in iot based e-healthcare service. *ACM Trans. Multimedia Comput. Commun. Appl.*, 0(ja).

Li, B., Lu, R., Wang, W., and Choo, K.-K. R. (2017). Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system. *Journal of Parallel and Distributed Computing*, 103:32–41.

Li, R., Song, T., Mei, B., Li, H., Cheng, X., and Sun, L. (2019). Blockchain for large-scale internet of things data storage and protection. *IEEE Transactions on Services Computing*, 12(5):762–771.

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

Li, X., Wang, M., Wang, H., Yu, Y., and Qian, C. (2019). Toward secure and efficient communication for the internet of things. *IEEE/ACM Trans. Netw.*, 27(2):621–634.

Liang, G., Zhao, J., Luo, F., Weller, S. R., and Dong, Z. Y. (2016). A review of false data injection attacks against modern power systems. *IEEE Transactions on Smart Grid*, 8(4):1630–1638.

Mendel, J. M. and Wu, D. (2017). Critique of "a new look at type-2 fuzzy sets and type-2 fuzzy logic systems". *IEEE Transactions on Fuzzy Systems*, 25(3):725–727.

Mengelkamp, E., Notheisen, B., Beer, C., Dauer, D., and Weinhardt, C. (2018). A blockchain-based smart grid: towards sustainable local energy markets. *Computer Science-Research and Development*, 33(1-2):207–214.

Mylrea, M. and Gourisetti, S. N. G. (2017). Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In *2017 Resilience Week (RWS)*, pages 18–23. IEEE.

Nix, J. A. (2016). Secure pki communications for machine-to-machine modules, including key derivation by modules and authenticating public keys. US Patent 9,288,059.

Taleb, T., Samdanis, K., Mada, B., Flinck, H., Dutta, S., and Sabella, D. (2017). On multi-access edge computing: A survey of the emerging 5g network edge cloud architecture and orchestration. *IEEE Communications Surveys Tutorials*, 19(3):1657–1681.

Truong, N. B., Sun, K., Lee, G. M., and Guo, Y. (2020). Gdpr-compliant personal data management: A blockchain-based solution. *IEEE Transactions on Information Forensics and Security*, 15:1746–1761.

Tschorsch, F. and Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys Tutorials*, 18(3):2084–2123.

Wang, L. (2017). A new look at type-2 fuzzy sets and type-2 fuzzy logic systems. *IEEE Transactions on Fuzzy Systems*, 25(3):693–706.

Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., and Wang, F. (2019a). Blockchain-enabled smart contracts: Architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 49(11):2266–2277.

Wang, S., Taha, A. F., Wang, J., Kvaternik, K., and Hahn, A. (2019b). Energy crowdsourcing and peer-to-peer energy trading in blockchain-enabled smart grids. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 49(8):1612–1623.

Wollschlaeger, M., Sauter, T., and Jasperneite, J. (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):17–27.

Yang, G. and Tan, C. H. (2011). Certificateless cryptography with kgc trust level 3. *Theoretical Computer Science*, 412(39):5446 – 5457.

Zamani, M., Movahedi, M., and Raykova, M. (2018). Rapidchain: Scaling blockchain via full sharding. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, page 931–948. Association for Computing Machinery.

Figure 1

Challenges

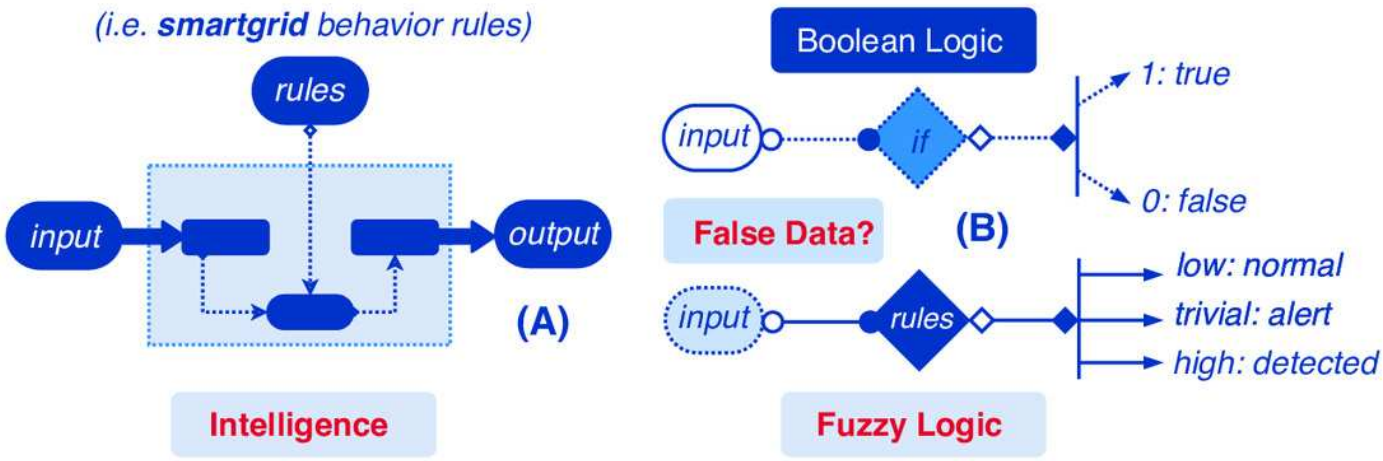


Figure 2

Blockchain and challenges

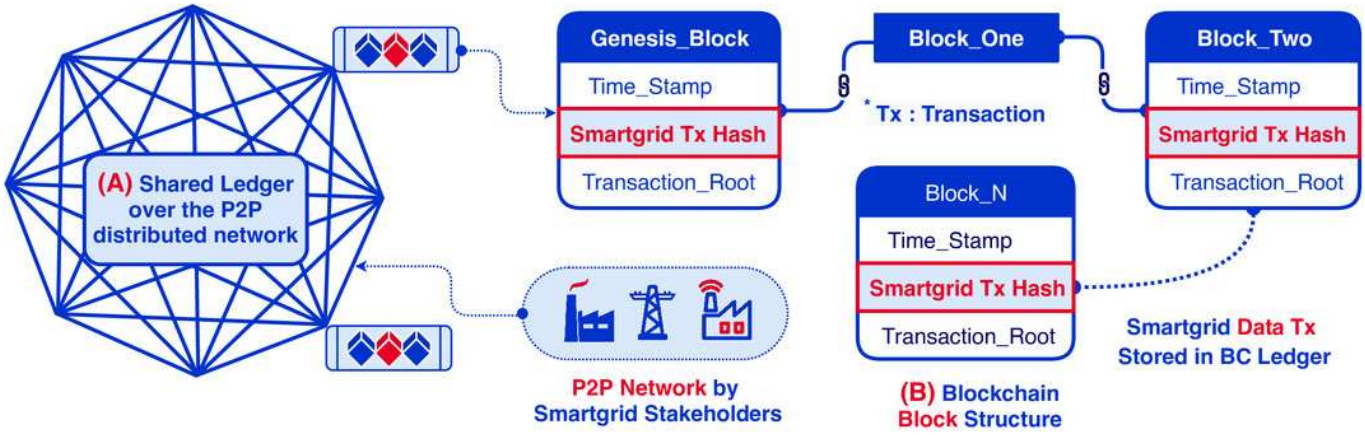


Figure 3

High level diagram

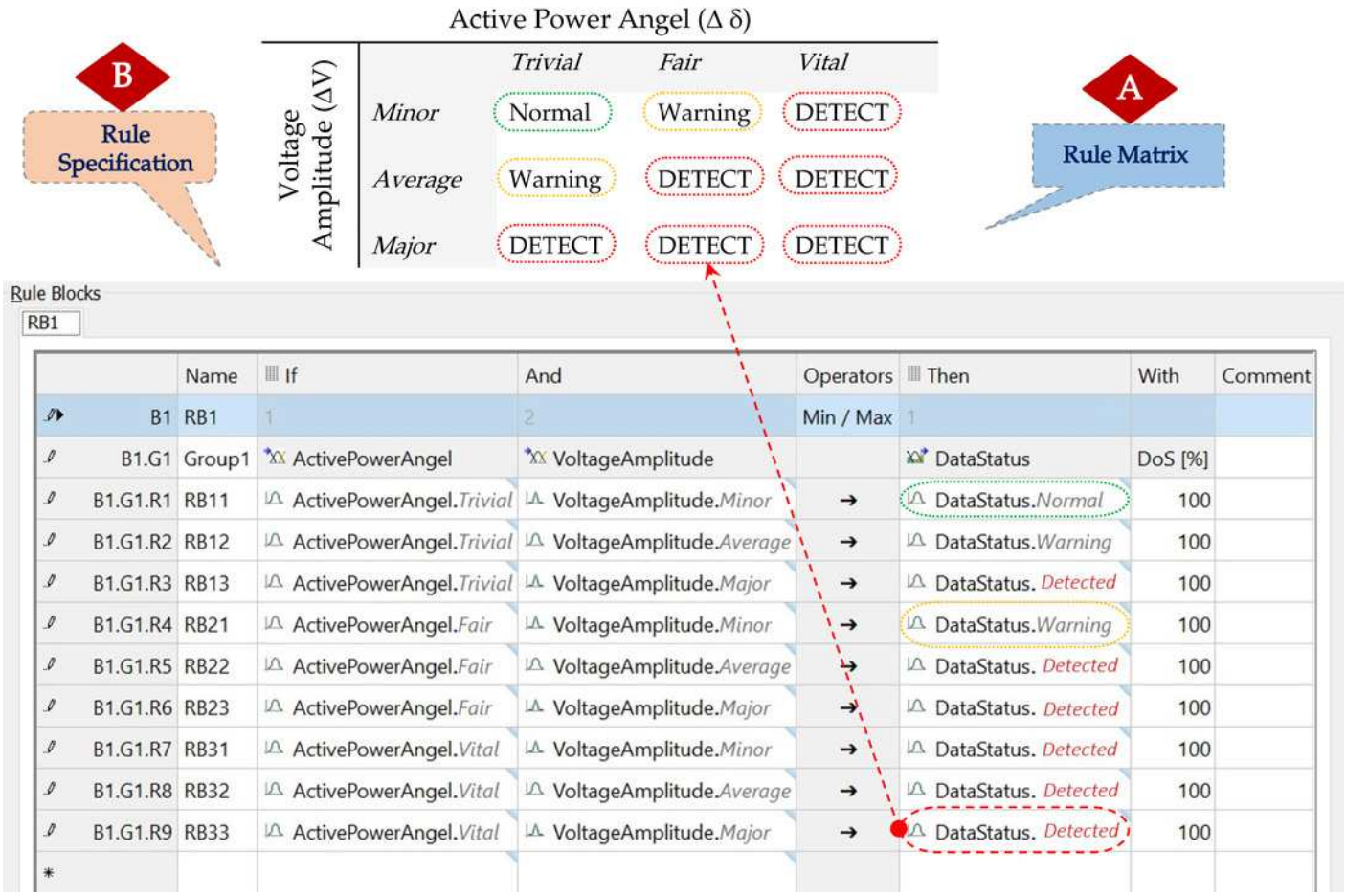


Figure 4

Smart grid system model

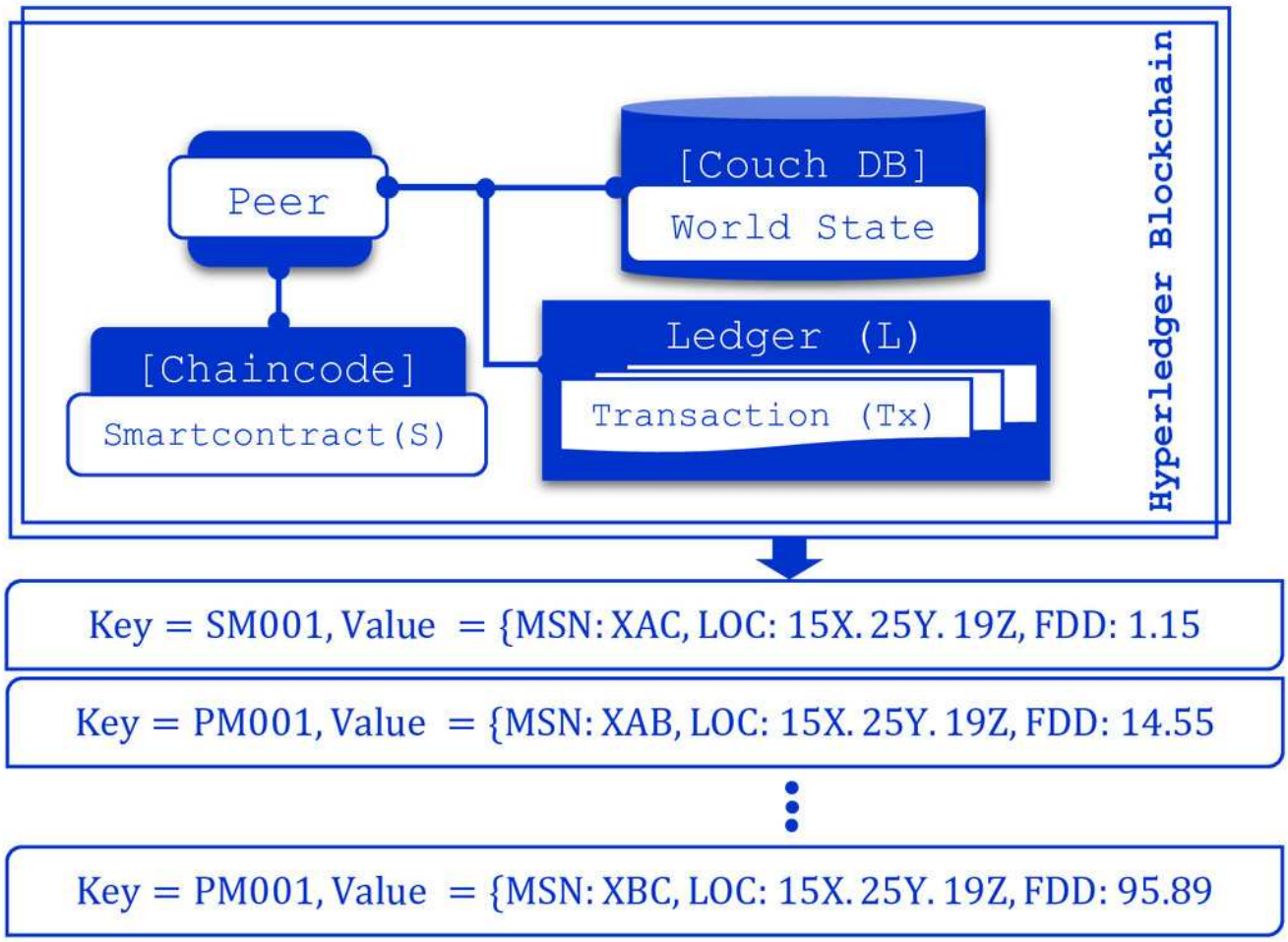


Figure 5

model specification

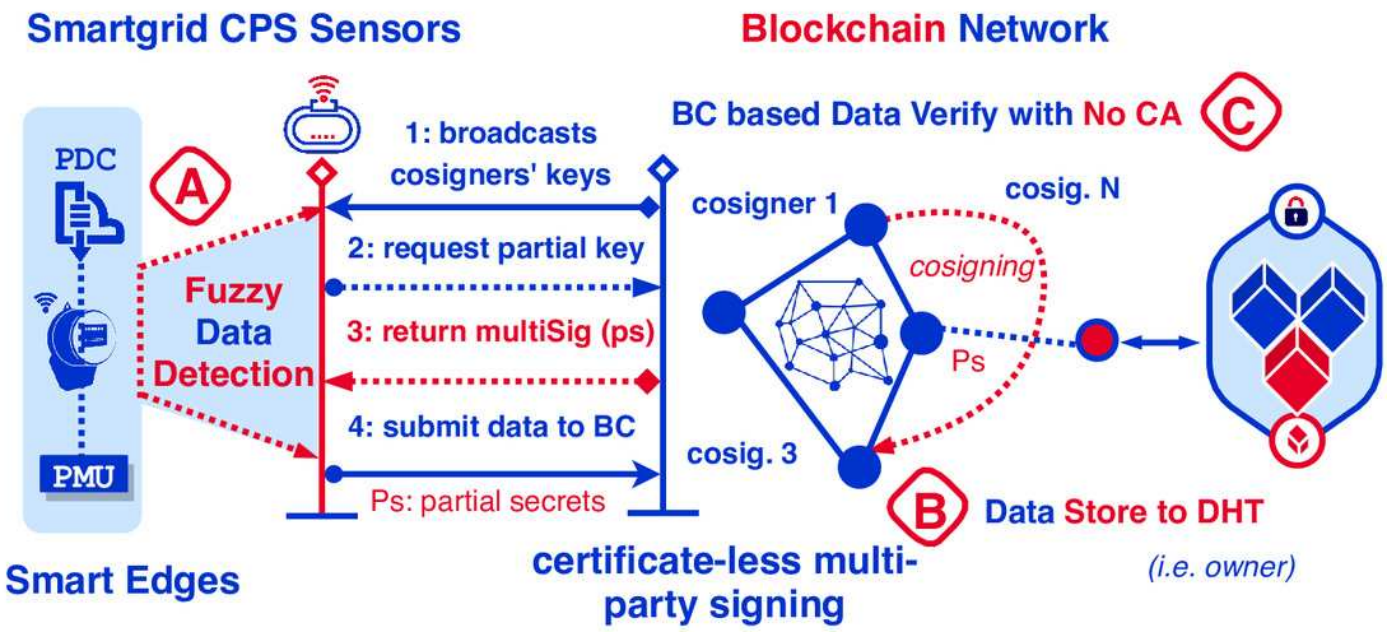


Figure 6

Blockchain test model

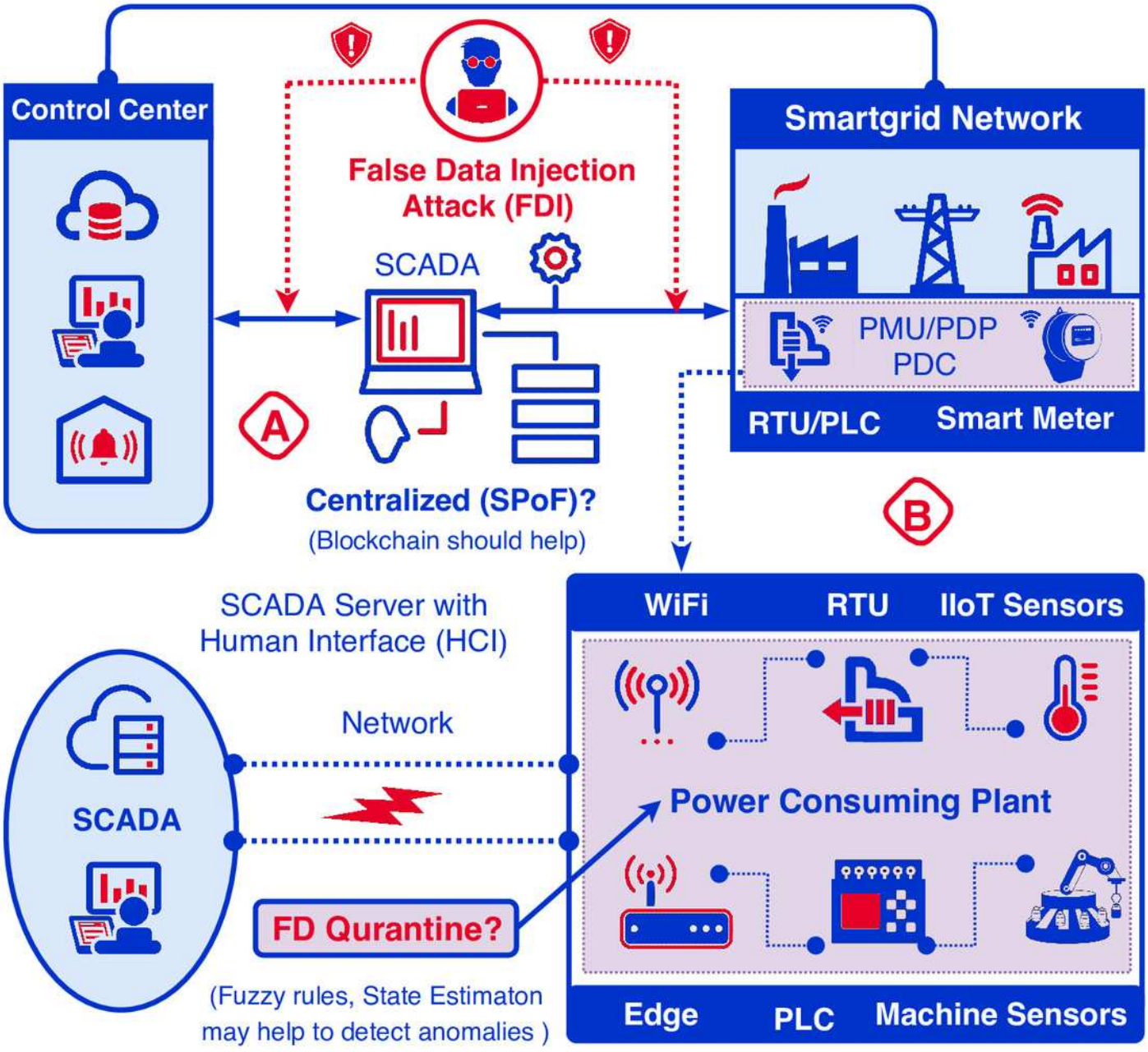


Figure 7

BC system for Smartgrid