IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON EVOLVING TECHNOLOGIES IN ENERGY STORAGE SYSTEMS FOR ENERGY SYSTEMS APPLICATIONS

Received February 11, 2021, accepted April 2, 2021, date of publication April 6, 2021, date of current version April 26, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3071431

A Secure Trust Method for Multi-Agent System in Smart Grids Using Blockchain

RABIYA KHALID[1], OMAJI SAMUEL[1], NADEEM JAVAID[1], (Senior Member, IEEE), ABDULAZIZ ALDEGHEISHEM[2], MUHAMMAD SHAFIQ[3], AND NABIL ALRAJEH[4]

[1]Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan
[2]Department of Urban Planning, College of Architecture and Planning, King Saud University, Riyadh 11574, Saudi Arabia
[3]Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, South Korea
[4]Department of Biomedical Technology, College of Applied Medical Sciences, King Saud University, Riyadh 11633, Saudi Arabia

Corresponding authors: Nadeem Javaid (nadeemjavaidqau@gmail.com) and Muhammad Shafiq (shafiq@ynu.ac.kr)

This work was supported by the King Saud University, Riyadh, Saudi Arabia, under Project RSP-2020/295.

ABSTRACT This paper proposes a blockchain based trust management method for agents in a multi-agent system (MAS). In this work, three objectives are achieved: trust, cooperation and privacy. The trust of agents depends on the credibility of trust evaluators, which is verified using the proposed methods of trust distortion, consistency and reliability. To enhance the cooperation between agents, a tit-3-for-tat (T3FT) repeated game strategy is developed. The strategy is more forgiving than the existing tit-for-tat (TFT) strategy. It encourages cheating agents to re-establish their trust by cooperating for three consecutive rounds of play. Also, a proof-of-cooperation consensus protocol is proposed to improve agents' cooperation while creating and validating blocks. The privacy of agents is preserved in this work using the publicly verifiable secret sharing mechanism. The proposed methods are implemented using MATLAB R2018a while the MAS is simulated using Java Agent DEvelopment framework (JADE). Simulation results validate the effectiveness of the proposed work. From the simulation results, the proposed trust method outperforms an existing fuzzy logic trust method in terms of detecting the cheating behavior of agents in the system. Besides, the proposed T3FT strategy is effective as compared to the existing tit-for-2-tat and TFT strategies in the literature. Moreover, the security analysis of the proposed method is performed. The analysis shows that the proposed work is safe from bad-mouthing and on-off trust related attacks.

INDEX TERMS Blockchain, multi-agent system, multi-secret sharing, proof-of-cooperation, repeated game, tit-3-for-tat, urban planning, trust management system.

ABBREVIATIONS

BTI	Balance trust incentive
BTMS	Blockchain based trust management system
CoC	Cooperation credit
DT	Direct trust
DET	Distributed energy trading
ID	Identity
JADE	Java Agent DEvelopment framework
MAS	Multi-agent system
PoC	Proof-of-cooperation
PVSS	Publicly verifiable secret sharing
NE	Nash equilibrium
RAM	Random access memory
RT	Recommended trust
TEM	Trust evaluation module
TMS	Trust management system
TFT	Tit-for-tat
TF2T	Tit-for-2-tat
T3FT	Tit-3-for-tat
VSS	Verifiable secret sharing

PARAMETERS AND VARIABLES

Γ	Absolute worth of the trust evaluation
$Hash(.)$	Any hash function
$\overline{p}$	Any large prime number
k^*	Average expected time an agent will cooperate
υ_n^*	Best strategy of an agent

The associate editor coordinating the review of this manuscript and approving it for publication was Eklas Hossain.

r_z	Computed share from the ordered polynomial
CF_n	Cooperative factor
V	Cost of privacy
z	Defined threshold by dealer
σ	Discount factor
$tvd_{\{i\}}$	Distorted trust value
U_n	Expected benefit of an agent in the game
y	Expected time a cheating agent will re-establish trust
k	Expected time an agent will cooperate
ψ_n	Expected utility function
$G(.)$	Game theory function
θ	Impact factor of trust evaluation
x	Indeterminate variable of the polynomial
rw^*	Maximized reward
ψ_n^*	Maximized utility
AC	Number of accepted cooperation of an agent
RC	Number of rejected cooperation of an agent
ν	Number of trust evaluation messages
P_p	Ordered polynomial function
f_{p2}	Past feedback
ξ	Payment of each evaluation message
f_{p1}	Present feedback
rw	Reward given to an agent that cooperates
S_z	Secret share of the *nth* agent
α	Sensitivity parameter of $TC_{\{i,j\}}$
β	Sensitivity parameter of TD_i
γ	Sensitivity parameter of $TR_{\{i,j\}}$
N	Set of agents
$s(i)$	Similarity value of *ith* evaluator
Υ	Strategies that an agent selects
$TC_{\{i,j\}}$	Trust consistency when evaluator i interacts with evaluatee j
TD_i	Trust distortion of the *ith* evaluator
π	Trust mapping
Φ	Trust model
$TR_{\{i,j\}}$	Trust reliability when evaluator i interacts with evaluatee j
tv	Trust value of an agent
$F(i,j)$	Tuple denoting *ith* evaluator and *jth* evaluatee

I. INTRODUCTION

A. MOTIVATION

In multi-agent system (MAS), agents are concerned about their privacy and security, which means that revealing their services to other agents is not appropriate for them. Besides, data is exchanged on a wide scale. Each agent should avoid exchanging information with dishonest agents in order to meet the privacy preservation goals of other agents. The exchange of information takes place in a high-risk environment where agents in the system are not indispensable allies. Also, over time, the relationship of trust between agents may not be the same as they change their roles in the cooperation process while limiting access to data. Thus, it is important to design a secure system that will encourage agents' cooperation while ensuring their privacy and trust. The existing works [1]–[4] propose different mechanisms for the distributed energy trading (DET), such as price negotiation, deep participation, bidding and transactive energy management in MAS. However, greater attention is needed to ensure agents' security, cooperation and trust.

B. LITERATURE REVIEW

Today, DET networks are becoming complex due to the rapid increase in the number of energy users [5]. MAS offers a potential solution for a complex network of energy users in residential sectors, commercial offices, hospital buildings, etc. It is made up of autonomous agents communicating with the environment and other agents [6]. MAS has certain features, such as flexibility, scalability, autonomy, etc., which are efficient for optimum energy management in the smart grids [7]. However, there are problems of security, privacy and trust between agents in MAS. The authors in [1] propose a distributed energy trading system with blockchain that facilitates peer to peer energy trading between agents in active distribution networks. The proposed system provides a secure environment for the negotiation of energy trading contracts between agents in the MAS. However, the negotiation approach becomes time-consuming and cumbersome as the number of agents increases. Also, agents' privacy and trust problems are not resolved. In [2], an agent based coordination strategy is proposed, which integrates price response from DET in the coordination process. The proposed strategy minimizes the energy imbalance and maximizes the profit of each agent. However, problems of trust, privacy and security of agents are not addressed. The authors in [3] propose a transactive energy trading system for agents in the MAS. In the system, a reinforcement learning method is used to design the bidding market strategies for the agents. However, the problems of privacy and trust of agents are not resolved. The authors in [4] propose a transactive energy management system for agents in the main grid. The system resolves the problems of energy cost optimization and overloading of the grid. However, the problems of trust, privacy and security of agents are not addressed.

Nowadays, blockchain can provide a secure and decentralized framework for autonomous agents. It is also used to protect agents and enhance their trust in MAS [1]. However, it is vulnerable to malicious peers that degrade the effectiveness of the systems. Contrarily, agents can exchange information about their interactions with other agents in order to decrease the activities of malicious agents [8]. Moreover, trust factors can reduce the cost effect and uncertainty during decision making. Trust values *tvs* can be calculated directly by an agent or obtained from a third party. Without the trust management system (TMS), *tv*s may be manipulated by an evaluator, i.e., an agent that estimates the worth of another agent (known as evaluatee). Thus, making trust decision inaccurate. Several traditional methods like cryptographic mechanisms have been deployed to protect the *tv*s of users. However, these mechanisms alone cannot solve the internal credibility

TABLE 1. A comparative analysis of the proposed scheme with other existing schemes.

Ref.	Energy trading	Objectives	Methods	Privacy	Trust	Cooperation	Security
[1]	✓	Blockchain based settlement system for active distribution networks	Price negotiation mechanism	✗	✗	✗	✓
[2]	✓	Bi-level agent framework for active distribution networks	Deep participation mechanism	✗	✗	✗	✗
[3]	✓	Agent based transactive energy trading	Reinforcement learning method	✗	✗	✗	✗
[4]	✓	Transactive energy management	Event-triggered transactive market algorithm	✗	✗	✗	✗
[8]	✓	BTMS	Weighted trust average method	✗	✓	✗	✓
Our scheme	✓	BTMS	T3FT strategy and PVSS	✓	✓	✓	✓

✓: Considered, ✗: Not considered.

problems of agents in heterogeneous systems. Access control methods have been adopted to restrict unauthorized agents from accessing *tv*s. However, these methods are centralized, which make them unsuitable for a distributed environment. Also, they are inefficient to handle the dynamic behavior of agents. The authors in [9] present a research study on trust mechanisms based on blockchain web technology for big data. In the study, different trust calculation methods are discussed, such as the weighted average method, Bayesian, fuzzy reasoning method, etc. Table 1 provides a comparative analysis of the proposed scheme with other existing schemes in terms of energy trading, objectives, methods, privacy, trust, cooperation and security.

C. CONTRIBUTIONS

This work is an extension of [8]. In [8], a consortium blockchain based trust management system (BTMS) is proposed, which consists of two layers: upper and lower. The former is used for verifying the credibility of agents. Whereas, the latter allows an agent to perform direct trust (DT) and recommended trust (RT) evaluation of other agents during interactions using the weighted trust average method. However, the problems of agent to agent cooperation, privacy and trust management are not addressed. This paper provides a service to the DET network with each energy user participating as an agent in MAS. The service provided is a BTMS, which enhances trust, cooperation, privacy and security of the involved agents. The main contributions of this paper are presented as follows.

1) This study proposes three trust credibility methods: distortion, consistency and reliability. The methods are used to verify the trust evaluation from different evaluators.
2) A repeated game is introduced to model the interactions of agents in order to achieve an efficient agent to agent cooperation. A tit-3-for-tat (T3FT) strategy is proposed, which allows cheating agents to effectively regain the trust if they cooperate thrice in a row as compared to the existing tit-for-tat (TFT) strategy [10].
3) A publicly verifiable secret sharing (PVSS) mechanism is employed to ensure privacy and security of the trust evaluation.
4) A proof-of-cooperation (PoC) consensus protocol is proposed in the consortium blockchain network. The protocol is used for the selection of miners and validation of blocks. It also enhances agents' cooperation.
5) This study analyzes two trust related attacks: bad-mouthing and on-off. In the analysis, it is shown that the proposed system is protected from the attacks.

The remaining paper is organized as follows. Section II provides the proposed system model, and the problem is formulated in Section III. Section IV presents a security analysis of the proposed system, and Section V provides simulation and discussion of results while Section VI concludes the paper.

II. PROPOSED SYSTEM MODEL

In Fig. 1, agents are household energy prosumers that locally produce and consume energy, and also exchange trust evaluation values with the aggregators. They can efficiently utilize the harvested solar energy and control the operational status. Based on the energy information from the smart meters, the energy deficient agents fulfill the energy requirements from other agents having surplus energy. In this way, a DET environment is established. Moreover, if the demand for energy deficient agents cannot be fulfilled by DET, the exact amount of energy is purchased from the grid. Once the energy trading agreement is established, the involved agents securely send the agreement information to the corresponding aggregators through the blockchain. According to the traded amount of energy, the aggregators control the required energy output to satisfy the energy demand of agents. Note that this paper considers the trust state of each agent. However, data loss, line interruption, noise and delay of the proposed system are not considered. They will be considered in the future.

The BTMS proposed in Fig. 1 addresses the problem of feedback sparseness in an existing system [11]. Initially, an agent's DT and RT for trust evaluation are considered. Then, the trust is evaluated using the overall adaptive weight of the combined trust evaluation from different evaluators.

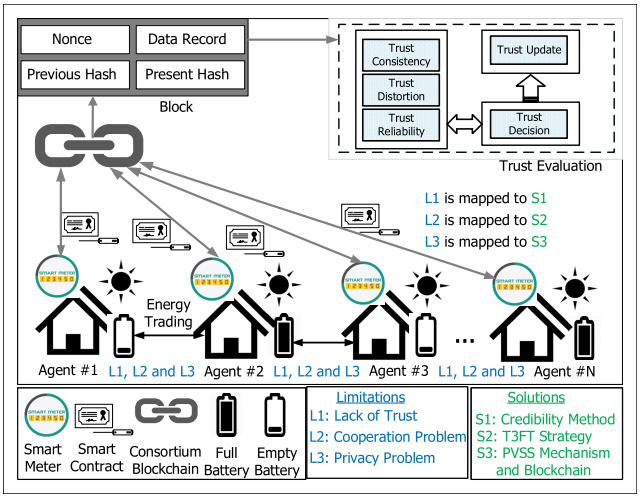


FIGURE 1. The Proposed system model consists of household prosumers that trade energy with each other via DET. Moreover, the identified limitations are denoted by L1-L3, which are directly mapped to the proposed solutions, denoted by S1-S3.

This depends on the frequency of interactions between the evaluators and evaluatees, the number of interactions and the credibility of the evaluators [11]. Next, the credibility of the evaluator is evaluated after each interaction with the evaluatee based on the methods of consistency, distortion and reliability. Besides, all of the agents have a token, known as a balanced trust incentive (BTI) unit, which is used to interact with other agents. BTI is increased if the credibility evaluation of agents is positive, which shows that the evaluators are honest and vice versa. Moreover, credibility evaluation is used to detect both the honest and dishonest behavior of the evaluators in the proposed system.

III. PROBLEM FORMULATION

In conventional trust evaluation methods, DT plays a major role in evaluating users. In DT evaluation, the evaluator has a direct encounter with the evaluatee and gives the DT value between 0 and 1. Where 0 represents dishonest behavior and 1 represents honest behavior. Note that DT boundary is based on the generalized trust evaluation methods that are commonly used in the research community [11]. However, DT is prone to feedback sparseness and malicious attacks [12]. Also, DT evaluation methods that consider the average of direct evaluation value are prone to misjudgement as time relevance is not considered. Nonetheless, DT evaluation methods that combine different weights to determine the dynamic change of evaluatees' behavior are not sufficient to handle the evaluators' credibility [11]. This paper resolves the aforementioned problems by proposing credibility evaluation methods and blockchain. The subsections below discuss the proposed credibility evaluation methods.

1) TRUST DISTORTION

Trust distortion is a change that alters the actual *tv*. The degree of trust distortion TD_i of an evaluator i is calculated as the actual *tv* that is distorted by a random distribution rate. If the evaluator i makes a dishonest evaluation, TD_i is used to determine the evaluator's degree of dishonesty. Therefore, TD_i is formulated based on our scenario as

$$TD_i = \beta tvd_{\{i\}}, \tag{1}$$

where $tvd_{\{i\}}$ is the distorted *tv* of i and $\beta \in [0, 1]$ is the randomly chosen sensitivity parameter of TD_i that regulates the rate of distortion.

2) TRUST CONSISTENCY

If an evaluator i finishes interaction with an evaluatee j, it sends a feedback to the aggregator. Afterwards, aggregator calculates the trust consistency $TC_{\{i,j\}}$ value of i. $TC_{\{i,j\}}$ is used to measure the degree of similarity between the present feedback f_{p1} and the past feedback f_{p2} about j within the range of $[-1, 1]$. Where 1 represents that f_{p1} is similar to f_{p2} and -1 denotes that the f_{p1} is dissimilar to f_{p2}.

$$s(i) = 2\Big(\frac{f_{p1} - f_{p2}}{\max(f_{p1}, f_{p2})}\Big)^2 - 4\Big|\frac{f_{p1} - f_{p2}}{\max(f_{p1}, \quad f_{p2})}\Big| + 1, \tag{2}$$

Eq. (2) is the similarity value, which is a modification of [13]. Unlike the range approach used in [13] that does not calculate the spread of majority values in feedback data, a maximum value between f_{p1} and f_{p2} is considered in this paper. Thus, the trust consistency is calculated as

$$TC_{\{i,j\}} = \alpha\Big(\frac{1}{s(i)} \exp^{-\frac{1}{s(i)}}\Big), \tag{3}$$

where $\alpha \in [0, 1]$ is the sensitivity parameter that determines the weight of $TC_{\{i,j\}}$.

3) TRUST RELIABILITY

Trust reliability is achieved when the trust evaluation is sufficient and error-free to meet the trust evidence. Given these two factors, TD_i and $TC_{\{i,j\}}$, the trust reliability formulation $TR_{\{i,j\}}$ is derived as [13]

$$TR_{\{i,j\}} = \gamma(1 - TD_i) + TC_{\{i,j\}}. \tag{4}$$

$\gamma \in [0, 1]$ is the sensitivity parameter that determines the weight of $TR_{\{i,j\}}$ where $\alpha + \beta + \gamma = 1$. TD_i and $TR_{\{i,j\}}$ range between 0 and 1, whereas $TC_{\{i,j\}}$ ranges between 1 and -1. It implies that the system can sustain the trust evaluation from both honest and dishonest agents.

4) TRUST UPDATE

In the trust update process, unauthorized modification of the trust evaluation is prevented. It implies that the final trust decisions are authenticated and validated by miners, i.e., nodes with high credibility. After validation is completed, the accepted trust evaluation is encapsulated into the blockchain by aggregators.

A. REPEATED GAME THEORY FOR MULTI-AGENT SYSTEM IN THE SMART GRIDS

BTMS is based on game theory that enhances the cooperative behavior of agents. It is observed that in a MAS environment, the assumptions, such as rationality and maximization required to achieve convergence are ignored. Also, new complexities may arise if the agents share and learn new strategies in a non-dynamic environment. Even if the objectives of agents are aligned and all agents hope to maximize their utilities, cooperation is needed to attain global optimum. We consider the dynamic environment in which agents can cooperate to achieve their goals. However, complexities exist when multiple decisions are needed by the agents. These complexities may involve insufficient information about the system. Two rationalities of the agents are considered in this paper: agents who cooperate and agents who refuse to cooperate. The sole aim of BTMS is to ensure that all agents must cooperate. The game theory provides the interactions between self-interested agents and also examines the strategy that maximizes their utilities. Some basic definitions of game theory are provided as follows [14]. Note that the proofs given in this paper are the deductive reasoning about the defined assumptions.

Definition 1 (Game Theory): A normal form of a game is a triad, denoted by $G = \{n, \Upsilon, \psi_n\} \forall n \in N$ where N is the set of agents, Υ is the set of possible strategies that the agent selects and ψ_n is the expected utility function for agent n. For each agent, the choice of the utility function is determined by the strategy set of agent n and other agents [14].

Definition 2 (Best Response): For each agent, an optimal strategy υ_n^* is chosen according to the best responses of all other agents, expressed as $\psi_n^* \geq \psi_n$. Where ψ_n^* is the maximum utility function of the agent n.

Definition 3 (Nash Equilibrium): Υ is said to be in Nash equilibrium (NE) if for each agent, υ_n^* is the best response to the agents' strategy.

In NE, no agent in the game can improve its utility one-sidedly by diverging from the set of equilibrium strategies. Thus, no agent has an incentive to change its strategy unless all of the agents have to change their strategies concurrently in order to overcome NE.

In MAS, due to the problems of limited resources and privacy requirement of each agent, most of the agents have selfish behavior orientations. The game becomes a prisoner's dilemma if the agents refuse to cooperate [14]. In this paper, the trust evaluation of agents is considered as a repeated game. The design requirements of the game consist of rational agents that perform DT evaluation of other agents or request RT evaluation of other agents from their aggregators. A dynamic time is considered to set up the system and for each time slot t, a T3FT strategy is established, which instantly punishes the agents that engage in cheating. The agents that cheat can re-establish the trust if they cooperate for three consecutive plays. We consider the case when agents establish a single-shot game to achieve their cooperation. In the cooperative game $G = \{n, \Upsilon, \psi_n\}$, the strategies that each agent selects are defined as $\Upsilon = \{\text{cooperate, refuse}\}$ and the utility function of the agent n in a game at t is defined as

$$\psi_n(t) = \big(\Gamma\theta - \xi rw\big)\nu, \tag{5}$$

where Γ is the absolute worth of the trust evaluation and θ is the impact factor of the trust evaluation such that $\theta \in [0, 1]$. ξ is the payment for each evaluation message and $\nu = RCV + ACrw$ is the number of trust evaluation messages required by the aggregators. RC is the number of rejected cooperation of agent n, whereas AC denotes the number of accepted cooperation of agent n. V is the cost of a privacy breach when agent n refuses to cooperate and rw is the reward given to agent n for cooperating.

In the repeated game, when the agents refuse to cooperate at t, then in the subsequent time slots, other agents do not cooperate with them. Here, a T3FT strategy is used, which provides instant punishment and the length of the punishment depends on the agents' cooperation. The defaulter agents may regain their trust after cooperating for three consecutive periods. Afterwards, their cheating behavior is pardoned [14].

Definition 4: Let the expected time an agent will cooperate be k. If the expected payoff or benefit is linear in the agent's strategy, the overall expected benefit of the agent in the game at t is expressed as [14]

$$U_n(t) = \sum_{t=1}^{k} \sigma\, \psi_n(t), \tag{6}$$

where σ is the discount factor such that $0 \leq \sigma \leq 1$.

The value of σ is larger if each agent stays longer in the cooperation. Otherwise, the value of σ will be smaller. Thus, $\sigma = \frac{1}{k} - \frac{1}{k+y}$ where y is the expected time the cheating agent will re-establish the trust by cooperating. The agents in our proposed system exhibit different strategies: always cooperating, always cheating and T3FT. In T3FT, it is assumed that the agents always start the game by accepting the cooperation strategy. For each time slot, an agent not only plays the game with other agents, but also learns their strategies. If an agent earns more BTIs in the last play, other agents can copy the strategy in order to enhance their utilities. A certain probability may be considered to learn the behavior of other agents.

B. EQUILIBRIUM OF GAME

After getting the strategies of all of the agents, the equilibrium of the game is important to determine the optimal rw of each agent. The stability of NE is defined as follows.

Definition 5 (Stability of NE): A NE is said to be stable if a small change δ in the probabilities of an agent raises two conditions.

1) In a new situation, any agent that cooperates has no better strategy.
2) Any agent that does not cooperate is playing with a much worse strategy.

If conditions (1) and (2) hold, the agent will move towards NE, which means that NE is stable. Conversely, if (1)

does not hold, NE is unstable. However, if only (1) holds, there will be an infinite number of optimal strategies for the agents that do not cooperate. In this study, we consider the derivation of ψ_n with respect to rw and equating it to zero in order to get the optimum reward rw^*.

$$\frac{\delta\psi_n}{\delta rw} = \frac{(\Gamma\theta - \xi rw)(RCV + ACrw)}{\delta rw} = 0, \tag{7}$$

$$\frac{\delta\psi_n}{\delta rw} = \Gamma\theta AC - \xi RCV - 2\xi ACrw = 0, \tag{8}$$

$$rw^* = \frac{\Gamma\theta AC - \xi RCV}{2\xi AC}, \tag{9}$$

$$\frac{\delta^2\psi_n}{\delta rw^2} = -2\xi AC. \tag{10}$$

The second derivative of Eq. (8) given in Eq. (10) means that the rw^* is the local maximum. Here, the constraint is $rw^* \geq 0$. If $rw^* < 0$, the maximizing rw is zero. Two cases are defined from the lower bound on rw as follows.

1) If $\Gamma\theta AC > \xi RCV$, the amount of reward that maximizes the utility ψ_n is rw^*. By substituting rw^* in Eq. (7), the maximum utility ψ_n^* of the agents is obtained. The agent will accept the utility if $\psi_n^* \geq 0$.
2) If $\Gamma\theta AC < \xi RCV$, $rw^* = 0$, which gives the agent the maximum utility ψ_n. The agent will accept the utility if $\psi_n \geq 0$.

C. BLOCKCHAIN BASED TRUST MANAGEMENT SYSTEM

In BTMS, a smart contract is proposed to implement the trust evaluation module (TEM). TEM ensures consistency in the operations of the agents. It includes three phases: trust evaluation collection, trust uploading, and miner selection and block creation. The important part of TEM is the account and memory creation. All of the agents have accounts that store BTI transaction data in the account pool while BTIs' addresses are stored in the memory pool. Besides, the memory pool is mapped to the account pool for achieving an efficient data audit. Before performing the trust evaluation of an agent, the aggregator must verify that it has enough BTIs.

1) TRUST EVALUATION COLLECTION

In this phase, *tv*s are initially generated either via DT or RT. Afterwards, the generated *tv*s are checked for trust credibility using the methods of TD_i, $TC_{\{i,j\}}$ and $TR_{\{i,j\}}$. If the credibility checking process is passed, the *tv* cannot be locally stored and managed. Instead, it is uploaded to the blockchain. Before uploading trust evaluation values to the blockchain, PVSS is used. Secret sharing is established to protect sensitive information from unauthorized users in the field of information security [15]. Sensitive information includes cryptographic keys and shares. In secret sharing, three actors, such as dealers, participants and combiner are considered. In this study, dealers, also known as blockchain miners, are authorized to distribute shares to the participants. In this study, shares refer to the *tv*s, whereas the secret refers to the cryptographic keys. However, the dealers are not authorized to store shares and secrets. Participants represent the agents that store shares and secrets given to them by the dealers. Combiner is known as the aggregator and is authorized to define a threshold, collect and reconstruct shares of the participants. Also, the combiner can be any participant in the system. Moreover, in an existing scheme [15], Shamir secret sharing is adopted so that the collected shares from fewer agents cannot reveal information about the secret. In this paper, PVSS [16] is employed to detect cheaters who are either dealers, combiner or participants. In verifiable secret sharing (VSS), the *tv*s for the agents represent the secret shared between them. Moreover, a secret sharing is PVSS if it is a VSS scheme that allows any entity, not necessarily the participants to verify the validity of the shares delivered by the dealer. Besides, VSS allows a dealer to distribute the secret S_z between the agents. To distribute the secret S_z into z shares, a $z-1$ ordered polynomial function P_p is required. The shares are calculated as $r_z = P_p(x)$ for $x \neq 0$. The pair (x, r_z) is sent to the agents. Here, $S_z = P_p(0)$. Moreover, z shares (x, r_z) is required to recover P_p and also find the secret $S_z = P_p(0)$. The ordered polynomial P_p is defined as [15]

$$P_p(x) = a_{z-1}x^{z-1} + a_{z-1}x^{z-2} + \cdots + a_1x + a_0 \ (\text{mod } \overline{p}), \tag{11}$$

where x is an indeterminate variable of P_p, $\overline{p}$ is any large prime number that is selected and for each $a_i \in P_p$; $0 \leq i \leq z-1$, $a_{z-1} \neq 0$. The secret is $P_p(0) = a_0$. In order to perform secret sharing as (z, n) threshold sharing, n shares are calculated for each randomly chosen n points (x; $1 \leq i \leq n$ and $x \neq 0 \in P_p$), which is distributed to the agent n. A verifiable hash function, denoted as $Hash(x, r_z)$, is encrypted and the result is broadcast across the blockchain network. Moreover, the share is recovered using the method of Lagrange interpolation [15].

2) TRUST UPLOADING

The agents' credibility values of the trust evaluation are verified based on the methods of TD_i, $TC_{\{i,j\}}$ and $TR_{\{i,j\}}$. Each agent is authorized to upload the encrypted DT evaluation values to the blockchain. The credibility of each agent depends on its cooperation. Once an agent does not cooperate, the T3FT strategy is enforced.

3) BLOCK CREATION AND MINER SELECTION

In BTMS, all miners are periodically elected from the agents to generate a new block. Here, the PoC consensus protocol is proposed for the validation and mining of the block. The cooperation of agents is supported by a set of cooperation credit (CoC) also known as the benefit factor in the repeated game. CoC is added to the BTI of an agent that cooperates and is dynamically determined by the cooperative factor defined as

$$CF_n = \frac{k^*}{k + k^*}, \tag{12}$$

where k^* is the average expected time in which an agent stays longer in the network by cooperating. The election of

Algorithm 1 Smart Contract for the Repeated Game

Υ_n = null ▷ Strategy of the *nth* agent
String Υ_1 = {Accept}
String Υ_2 = {Refuse}
$k = 1; AC = 1; RC = 0$
begin Commit(ID_n, Hash)
if Agent == null **then**
    Agent = sender
    hash = *Hash*
else
    Playgame (ID_n, String Υ_n, hash)
end if
end Commit
begin Playgame(ID_n, String Υ_n, hash)
if sender == Agent{Accept} && H(Υ_n, *rn*) == hash **then** ▷ *rn* is random number
    Υ_1 = {Accept}
else
    if sender == Agent{Refuse} && H(Υ_n, *rn*)==hash **then**
        Υ_2 = {Refuse}
    end if
end if
Evaluategame(ID_n)
end Playgame
begin Evaluategame(ID_n)
if $\Upsilon \neq$ null **then**
    return $ID_n = ID_n$
else
    if Υ = {Accept} **then**
        $k = k + 1; AC = AC + 1$
        return {Accept}
    else
        $k = k - 1; RC = RC + 1$
        return {Refuse}
    end if
end if
end Evaluategame
if $k > 0$ **then**
    An agent gets more benefits for cooperating
else
    An agent is punished for not cooperating
    break
end if

miners is based on the number of commitments to cooperate and the number of BTIs in their wallet accounts. A round-robin mechanism is used to select the leader, known as an aggregator, between agents with the equal worth of BTIs and the number of commitments. Algorithm 1 is the proposed smart contract. The algorithm is deployed on the blockchain. A unique identifier (ID_n) is assigned to all agents. Also, they are given token accounts and wallet addresses, and all transactions are stored in the blockchain using the commit method. In the algorithm, the agents send the hash string of their strategies and a random number to the blockchain. The hash function provides a one-way property, which is only known to the agents. With PVSS, the strategy of an agent cannot be revealed to unauthorized agents in the blockchain.

IV. SECURITY ANALYSIS

The proposed system aims to achieve a secure trust evaluation information of each agent. Besides, the proposed system is safe from external attacks due to the underlying security benefits of the blockchain technology, such as confidentiality, integrity and privacy of agents' data. However, the system is not safe from internal attacks, which is the focus of this study. Considering the internal attacks of the proposed system, the agent can behave either as honest or cheater during the interaction process. Moreover, the security objectives to be achieved in this study are described as follows.

1) Transparency: The trust evaluation mechanism is known to all of the agents in the system. Besides, the repeated game and the PVSS mechanism are known to the agents. This prevents an adversary from manipulating the *tv*s.
2) Verifiability: PVSS mechanism exposes cheaters. It also permits the combiner to reconstruct the shares and secrets.
3) Fairness: Based on the PoC consensus protocol, all agents trust each other and have an equal chance of being selected as the combiner.
4) Privacy: If the three objectives given above are fulfilled, privacy preservation for all of the agents is ensured using PVSS.

Theorem 1: If an adversary intercepts less than $z-1$ shares constructed by P_p, the entire message cannot be correctly reconstructed by it.

Proof 1: Suppose that there is an adversary who initially intercepts and decrypts the shares of $z-1$ generated by P_p. Then, the adversary is required to solve P_p that constructs the shares in order to reconstruct a message. If the adversary cannot reconstruct the message from the shares of $z-1$, the set of shares less than $z-1$ cannot be reconstructed by the adversary.

Definition 6: Let $F(i, j)$ be a tuple that represents the *ith* evaluator and *jth* evaluatee such that $F(i, j) = \{tv, TC_{\{i,j\}}\}$. An interaction between i and j holds if:

$$TC_{\{i,j\}} = \begin{cases} 1, & \text{if the interaction happens honestly,} \\ 0, & \text{if the interaction does not happen,} \\ -1, & \text{if the interaction involves a cheater.} \end{cases}$$

Theorem 2: Suppose that *ith* evaluator provides a dishonest trust evaluation of *jth* evaluatee, then the proposed system is vulnerable to bad-mouthing attack.

Proof 2: It is assumed that *jth* evaluatee may have a past encounter with other evaluators that provide their trust evaluation's feedback to the blockchain. Since j has multiple evaluators and using DT and RT evaluation methods, the

bad-mouthing attack is prevented. Moreover, this attack occurs when an agent provides a dishonest recommendation [17].

Theorem 3: At any time t, an evaluator i acts honestly, and at $t+1$, it acts maliciously by concealing its activities. Thus, the system is vulnerable to an on-off attack.

Proof 3: At the time t, an evaluator provides an honest trust evaluation of an evaluatee. Whereas at $t+1$, it behaves maliciously by providing a dishonest trust evaluation of that evaluatee with the hope that it will not be detected [18]. To address this type of attack, once the malicious node is detected, its BTI is completely reduced to 0. It implies that such evaluator can no longer participate in the interaction process with other evaluatees.

V. SIMULATION AND RESULTS

In this section, the proposed MAS is simulated using the Java Agent DEvelopment framework (JADE) [19] while simulation of the proposed methods are performed using MATLAB R018a. The proposed system is implemented on a personal computer furnished with Intel i5 quad-core processor having 1.60 GHz speed and 8 GB RAM. The parameters used for the simulations are given in Table 2, which are taken from [8], [20] and [21]. The following limitations are addressed in this section: **L1:** lack of trust, **L2:** cooperation problem and **L3:** privacy problem.

TABLE 2. Parameters used for simulation.

Parameter	Values	Parameter	Values
$Tmax$	100	T	2.5
rw	2	P	1
S	0.5	q	0.5
rad	3	p	0.1
α	0.2	RV	0.7
β	0.4	λ	0.5
γ	0.4	N	100

A. SCENARIO OF THE EXPERIMENT

Motivated by the work of [20], the proposed T3FT strategy is designed. The iterated prisoner's dilemma strategy where the agents are either always cooperating or always cheating is also considered. Tit-for-tat (TFT) strategy allows an agent to choose the exact action as other agents did in the last round. Moreover, tit-for-2-tat (TF2T) strategy is derived from the TFT strategy and it allows an agent to always cheat if the other agents cheat twice in a row [20]. In the prisoner's dilemma strategy, two possibilities are considered: cooperate (C) and cheat, i.e., defect (D). To encourage the cooperative behavior of agents, certain benefits are awarded to them. If the agents decide to cooperate, they earn rewards rw; otherwise, they are punished (P). If an agent decides to cheat another agent that cooperates, the agent that cooperates gets the "sucker" payoff (S), whereas the agent that cheats gets the maximum temptation (T). The parameters used for the repeated game are given in Table 2. From the table, the maximum number of iterations is denoted by $Tmax$, the probability of migrating from one coalition to another is denoted by q. We consider the migration radius as rad and the probability of an agent to imitate another agent is denoted by p.

B. TRUST EVALUATION

The validations of the proposed solutions to **L1** are presented in this subsection. The performance evaluation of agents concerning DT and RT is compared with an existing scheme of [21].

In Fig. 2, it is observed that both DT and RT have different values for each agent. In this paper, we consider 7 agents for the performance evaluation. It is also observed that the proposed DT has the least scores for agent-2 and agent-6 as compared to the work done in [21]. The least scores occur as a result of the weighted average method, whereas the work of [21] uses a fuzzy logic trust model. Moreover, our proposed method has also achieved the least scores for the RT as compared to the fuzzy logic model for all of the agents.

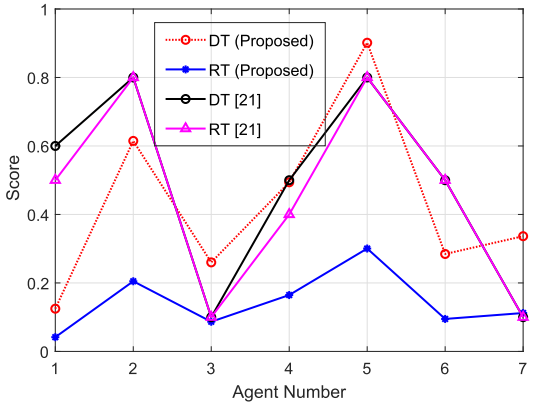


FIGURE 2. Evaluation of RT and DT by different schemes.

Fig. 3 shows the effect of sensitive parameter β on TD_i as the number of interactions increases. β is a weighted value that adjusts the convergence rate of TD_i. For the analysis, three values of β, 0.2, 0.4 and 0.6, are considered. If the TD_i scores converge to 0, it implies that there is a higher degree of distortion in tvs. Contrarily, if the TD_i scores converge to 1, it means that there is no distortion in tvs. To analyze the degree of TD_i, different β values show distinct behavior of the evaluators. It is observed that for a larger value of β, convergence is fast and stable, whereas for a smaller value of β, convergence is slow and unstable. For simplicity, if the degree of distortion is high, it means that the evaluators make a dishonest evaluation. On the other hand, if the degree of distortion is low, it indicates that the evaluators are honest with their evaluation.

Fig. 4 shows the effect of α on $TC_{\{i,j\}}$ as the number of interactions increases. The sensitive parameter α is used to measure the degree of how consistent two trust feedback values from the same evaluator are. If the consistency score is 1, it implies that the two feedback values are similar. Otherwise, if the consistency score is -1, it means that the two feedback values are dissimilar. Two cases are considered

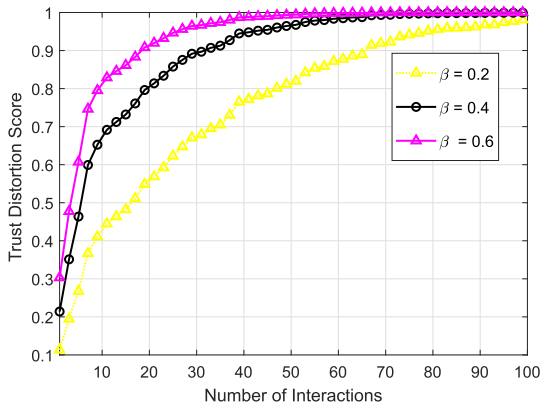


FIGURE 3. Effect of β on distortion.

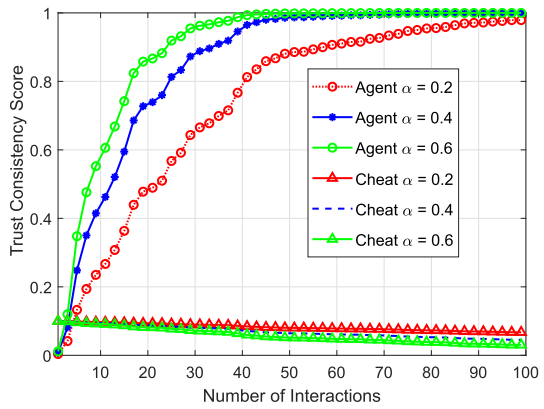


FIGURE 4. Effect of α on consistency.

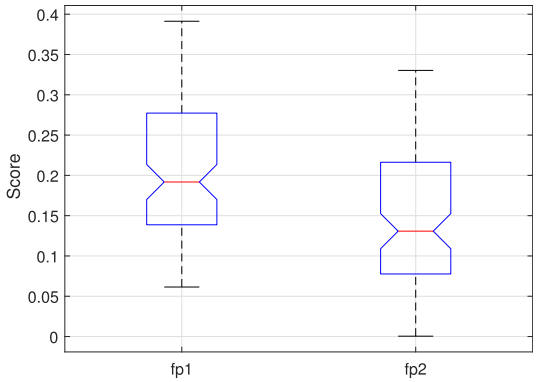


FIGURE 5. Feedback of an agent.

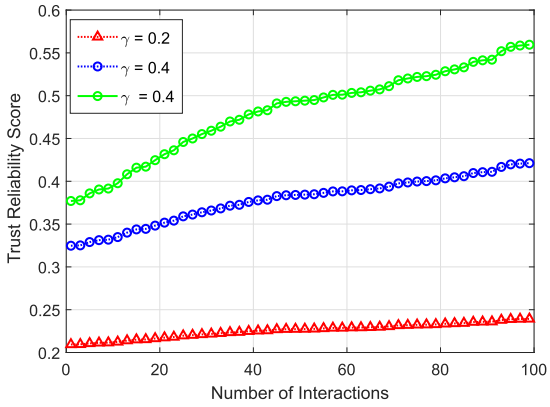


FIGURE 6. Effect of γ on reliability.

in this study. The first case considers $TC_{\{i,j\}}$ from the honest agents and the second case considers $TC_{\{i,j\}}$ from dishonest agents, which are known as cheaters. The cheaters are agents who behave dishonestly by manipulating their trust evaluation values and also refuse to cooperate. Three values of α, 0.2, 0.4 and 0.6, are considered for both cases. For the honest agents, the $TC_{\{i,j\}}$ values start from 0 and converge to 1. It implies that the honest agents provide two similar feedback values. Moreover, a larger value of α attains fast convergence to 1, whereas a smaller value of α shows slow convergence to 1. For the cheaters, the $TC_{\{i,j\}}$ values start from 0.1 and converge to -1. It means that the system can detect cheaters based on their feedback values that are not similar.

Fig. 5 shows two feedback values, which are denoted by f_{p1} and f_{p2} obtained from the same evaluator. A Wilcoxon signed-rank test is employed to analyze the similarity between the two feedback values [22]. It is also used to determine whether the two feedback values are selected from the same distribution or not. It is obvious from the figure that the two feedback values are not evenly distributed. It implies that there is trust inconsistency between the two feedback values.

In Fig. 6, the effect of γ on $TR_{\{i,j\}}$ as the number of interactions increases is shown. The sensitive parameter γ is the weighted value that adjusts the rate of convergence for $TR_{\{i,j\}}$. Considering the condition $\alpha + \beta + \gamma = 1$, we set some sensitivity parameters equal to one another. Moreover, a larger parameter value is considered for γ. It is observed that a larger value of γ gives higher $TR_{\{i,j\}}$. On the other hand, a smaller value of γ provides lower $TR_{\{i,j\}}$. The $TR_{\{i,j\}}$ score tells us about the usability of the trust evaluation. Fig. 6 shows that $TR_{\{i,j\}}$ depends on both TD_i and $TC_{\{i,j\}}$. If TD_i is low and $TC_{\{i,j\}}$ is high, it ensures higher $TR_{\{i,j\}}$. However, if both TD_i and consistency are low, $TR_{\{i,j\}}$ is moderate. On the other hand, if TD_i is high and $TC_{\{i,j\}}$ is low, $TR_{\{i,j\}}$ is weak.

C. EVALUATION OF THE REPEATED GAME STRATEGY

In this subsection, the validations of the proposed solutions to **L2** are discussed. The proposed T3FT strategy is compared with existing strategies: TF2T, TFT [23], always cooperating and always cheating [20]. We analyze the utility of each agent that chooses to cooperate as shown in Fig. 7. From the figure, it is seen that the agents that implement our proposed T3FT strategy get the highest utility than those that consider other strategies: TF2T, TFT, always cooperating and always cheating. It is also observed that the agents who do not cooperate, get the least utility. It implies that the BTIs of such agents are reduced in the blockchain and they cannot participate with other agents in the future. Moreover, the agents may adopt our

TABLE 3. Validating solutions based on identified problems.

Limitations to be addressed	Solutions Proposed	Validations
L1: Lack of trust	**S1**: We propose DT and RT evaluation methods. The credibility of the tvs is verified by the methods of TD_i, $TC_{\{i,j\}}$ and $TR_{\{i,j\}}$	Figs. 2, 3, 4, 5 and 6 evaluate the efficiency of the BTMS
L2: Cooperation problem	**S2**: We propose T3FT, which is a repeated game strategy	Figs. 7, 8 and 9 analyze the proposed T3FT strategy
L3: Privacy problem	**S3**: We use PVSS mechanism and consortium blockchain	Security analysis validates the proposed system

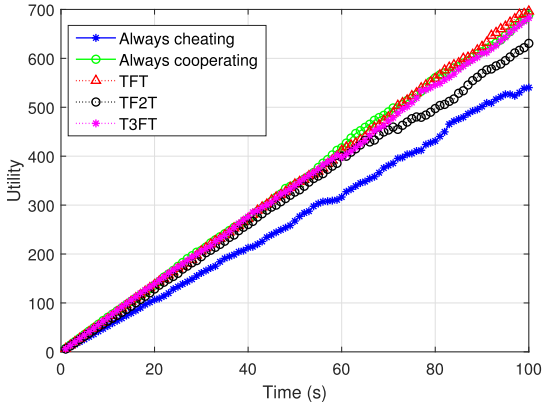


FIGURE 7. Comparison of the proposed strategy with other existing strategies based on utility.

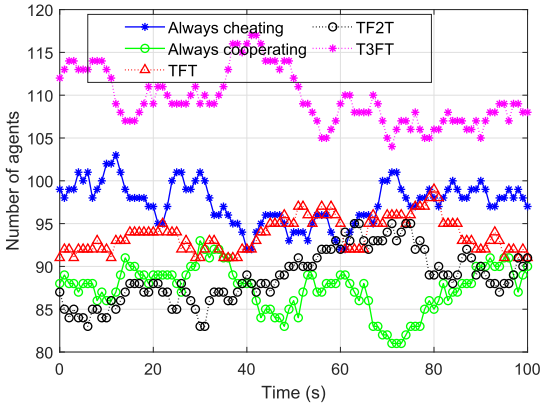


FIGURE 8. Comparison of the proposed strategy with exiting strategies based on number of agents.

proposed strategy in order to renew the trust by cooperating for three consecutive plays.

In Fig. 8, it is observed that our proposed T3FT strategy outperforms the other strategies with the highest number of agents. Moreover, for each time slot, agents that adopt the proposed T3FT strategy are 23.22% as compared to 18.70% for TF2T and 19.48% for TFT strategy. Contrarily, the number of agents that always cheat is more than those that always cooperate. It implies that the existing TF2T, TFT, always cooperating and always cheating strategies are not suitable for our proposed scenario. Hence, our proposed T3FT strategy provides remedies for the limitations of TF2T, TFT, always cooperating and always cheating strategies. Fig. 9 shows the strategy of the agents for 100 iterations. According to Fig. 8 and Fig. 9, the agents who implement the proposed T3FT strategy are represented by magenta color and those which implement TFT and TF2T strategies are represented by red and blue color, respectively. From the figures, it is observed that the agents with magenta color are more than the agents with red or blue color. It implies that more agents implement our proposed T3FT strategy.

We validate the solutions to **L3** using the PVSS mechanism and consortium blockchain. PVSS is used to protect the shares of agents from unauthorized agents, whereas consortium blockchain limits the number of agents in the network. It implies that the proposed system prevents an adversary from direct access to the agents' shares.

D. MAPPING OF PROBLEMS WITH THE PROPOSED SOLUTIONS

In this subsection, we show that the identified limitations are mapped to the proposed solutions and then validated by the

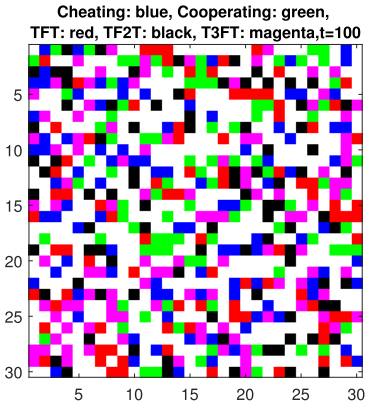


FIGURE 9. Heat map showing the strategy planning of different strategies for 100 iterations.

simulation results. Table 3 provides detailed information on how the solutions are mapped to the identified limitations and how they are validated.

VI. CONCLUSION

In this paper, three problems are addressed for agents in MAS. Firstly, the lack of trust between agents is addressed by the proposed method of trust credibility. The trust credibility values of the evaluators are validated based on the methods of TD_i, $TC_{\{i,j\}}$ and $TR_{\{i,j\}}$. Secondly, the problem of agents' cooperation is resolved using the proposed T3FT strategy. The strategy enables the agents to renew their trust if they cooperate for three continuous periods of the game. Thirdly, the problem of privacy of the agents is solved through the blockchain and PVSS mechanism. Besides, a PoC consensus

protocol is proposed to enable the efficient selection of miners for block creation and validation. Simulations are performed to evaluate the effectiveness of the proposed methods. From the results, it is observed that $TR_{\{i,j\}}$ depends on TD_i and $TC_{\{i,j\}}$. Also, the proposed trust method outperforms the fuzzy logic method in terms of efficient detection of malicious agents' behavior. Moreover, the number of agents that adopt the proposed T3FT strategy is 23.22% as compared to 18.70% for the TF2T strategy and 19.48% for the TFT strategy. It implies that more agents are willing to cooperate in order to maintain their trust after behaving selfishly. Also, the agents that implement the T3FT strategy get more utility from the cooperation. Furthermore, security analysis shows that the proposed system is able to circumvent bad-mouthing and on-off trust related attacks.

The robustness of the proposed PoC consensus protocol will be thoroughly investigated in the future to increase network throughput. We intend to propose a blockchain based coalition formulation protocol in the MAS, which is not exhaustively addressed in the literature.

REFERENCES

[1] F. Luo, Z. Y. Dong, G. Liang, J. Murata, and Z. Xu, "A distributed electricity trading system in active distribution networks based on multi-agent coalition and blockchain," *IEEE Trans. Power Syst.*, vol. 34, no. 5, pp. 4097–4108, Sep. 2019.

[2] S. Hu, Y. Xiang, J. Liu, C. Gu, X. Zhang, Y. Tian, Z. Liu, and J. Xiong, "Agent-based coordinated operation strategy for active distribution network with distributed energy resources," *IEEE Trans. Ind. Appl.*, vol. 55, no. 4, pp. 3310–3320, Jul. 2019.

[3] H. S. V. S. K. Nunna, A. Sesetti, A. K. Rathore, and S. Doolla, "Multiagent-based energy trading platform for energy storage systems in distribution systems with interconnected microgrids," *IEEE Trans. Ind. Appl.*, vol. 56, no. 3, pp. 3207–3217, May 2020.

[4] M. S. H. Nizami, M. J. Hossain, and E. Fernandez, "Multiagent-based transactive energy management systems for residential buildings with distributed energy resources," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 1836–1847, Mar. 2020.

[5] Y. Ren, Q. Zhao, H. Guan, and Z. Lin, "A novel authentication scheme based on edge computing for blockchain-based distributed energy trading system," *EURASIP J. Wireless Commun. Netw.*, vol. 2020, no. 1, pp. 1–15, Dec. 2020.

[6] X. Linyun, P. Li, Z. Wang, and J. Wang, "Multi-agent based multi objective renewable energy management for diversified community power consumers," *Appl. Energy*, vol. 259, no. 1, 2020, Art. no. 114140.

[7] M. W. Khan, J. Wang, M. Ma, L. Xiong, P. Li, and F. Wu, "Optimal energy management and control aspects of distributed microgrid using multi-agent systems," *Sustain. Cities Soc.*, vol. 44, no. 1, pp. 855–870, Jan. 2019.

[8] O. Samuel, N. Javaid, A. Khalid, M. Imrarn, and N. Nasser, "A trust management system for multi-agent system in smart grids using blockchain technology," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Taipei, Taiwan, Dec. 2020, pp. 1–6.

[9] Q. Liu and X. Zou, "Research on trust mechanism of cooperation innovation with big data processing based on blockchain," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, pp. 1–11, Dec. 2019.

[10] S. Kopelman, "Tit for tat and beyond: The legendary work of anatol rapoport," *Negotiation Conflict Manage. Res.*, vol. 13, no. 1, pp. 60–84, Feb. 2020.

[11] D. Shehada, C. Y. Yeun, M. J. Zemerly, M. Al-Qutayri, Y. Al-Hammadi, and J. Hu, "A new adaptive trust and reputation model for mobile agent systems," *J. Netw. Comput. Appl.*, vol. 124, pp. 33–43, Dec. 2018.

[12] J. Yuan and X. Li, "A reliable and lightweight trust computing mechanism for IoT edge devices based on multi-source feedback information fusion," *IEEE Access*, vol. 6, pp. 23626–23638, 2018.

[13] K. Zhao, S. Tang, B. Zhao, and Y. Wu, "Dynamic and privacy-preserving reputation management for blockchain-based mobile crowdsensing," *IEEE Access*, vol. 7, pp. 74694–74710, 2019.

[14] L. Hui-Jia, Q. Wang, S. Liu, and J. Hu, "Exploring the trust management mechanism in self-organizing complex network based on game theory," *Phys. A, Stat. Mech. Appl.*, vol. 542, Mar. 2020, Art. no. 123514.

[15] S. Kandar and B. C. Dhara, "A verifiable secret sharing scheme with combiner verification and cheater identification," *J. Inf. Secur. Appl.*, vol. 51, Apr. 2020, Art. no. 102430.

[16] C. Lin, H. Hu, C.-C. Chang, and S. Tang, "A publicly verifiable multi-secret sharing scheme with outsourcing secret reconstruction," *IEEE Access*, vol. 6, pp. 70666–70673, 2018.

[17] S.-S. Zhang, S.-W. Wang, H. Xia, and X.-G. Cheng, "An attack-resistant reputation management system for mobile ad hoc networks," *Procedia Comput. Sci.*, vol. 147, pp. 473–479, 2019. [Online]. Available: https://www.sciencedirect.com/journal/procedia-computer-science

[18] X. Liu, Y. Liu, A. Liu, and L. T. Yang, "Defending ON–OFF attacks using light probing messages in smart sensors for industrial communication systems," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 3801–3811, Sep. 2018.

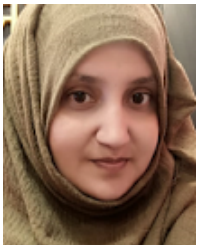
[19] *Java Agent Development Framework (JADE)*. Accessed: Sep. 17, 2020. [Online]. Available: https://jade.tilab.com/

[20] R. Jan and B. Lucas, "Lecture with computer exercises: Modelling and simulating social systems with MATLAB: Evolution of different strategies in the iterated prisoner's dilemma," Swiss Federal Inst. Technol. Zirich, Project Rep., 2009, pp. 1–60. [Online]. Available: http://webarchiv.ethz.ch/soms/teaching/MatlabSpring10/projects/hs2009_1500_ruegg_braun_migration.pdf

[21] A. Alnasser and H. Sun, "A fuzzy logic trust model for secure routing in smart grid networks," *IEEE Access*, vol. 5, pp. 17896–17903, 2017.

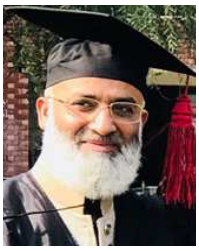
[22] P. Grzegorzewski and M. Śpiewak, "The sign test and the signed-rank test for interval-valued data," *Int. J. Intell. Syst.*, vol. 34, no. 9, pp. 2122–2150, Sep. 2019.

[23] T. N. Cason and V.-L. Mui, "Individual versus group choices of repeated game strategies: A strategy method approach," *Games Econ. Behav.*, vol. 114, pp. 128–145, Mar. 2019.



RABIYA KHALID received the M.C.S. degree from the Mirpur University of Science and Technology, Mirpur, Pakistan, in 2014, and the M.S. degree in computer science with a specialization in energy management in smart grid from the Communications Over Sensors (ComSens) Research Laboratory, COMSATS University Islamabad, Islamabad, Pakistan, in 2017, under the supervision of Dr. Nadeem Javaid, where she is currently pursuing the Ph.D. degree under the same supervision. She is also working as a Research Associate with the ComSens Research Laboratory, COMSATS University Islamabad. She has authored more than 20 research publications in international journals and conferences. Her research interests include data science and blockchain in smart/micro grids.

OMAJI SAMUEL received the B.Sc. degree in statistics/computer science from the Federal University of Agriculture Makurdi, Nigeria, in 2009, and the M.S. degree in information security from COMSATS University Islamabad, Islamabad, Pakistan, in 2015. He is currently pursuing the Ph.D. degree in computer science from the Communication over Sensors (ComSens) Research Laboratory under the supervision of Dr. Nadeem Javaid. He is also the Outstanding Student of the ComSens Research Laboratory. He has authored over 20 research articles in technical journals and international conferences. His research interests include data science, optimization, security and privacy, energy trading, blockchain, and smart grid.



NADEEM JAVAID (Senior Member, IEEE) received the bachelor's degree in computer science from Gomal University, Dera Ismail Khan, Pakistan, in 1995, the master's degree in electronics from Quaid-i-Azam University, Islamabad, Pakistan, in 1999, and the Ph.D. degree from the University of Paris-Est, France, in 2010. He is currently an Associate Professor and the Founding Director of the Communications over Sensors (ComSens) Research Laboratory, Department of Computer Science, COMSATS University Islamabad, Islamabad. He has supervised 126 masters and 20 Ph.D. theses. He has authored over 900 articles in technical journals and international conferences. His research interests include energy optimization in smart/micro grids, wireless sensor networks, big data analytics in smart grids, blockchain in WSNs/smart grids, and so on. He was a recipient of the Best University Teacher Award from the Higher Education Commission of Pakistan, in 2016, and the Research Productivity Award from the Pakistan Council for Science and Technology, in 2017. He is also an Associate Editor of IEEE Access and an Editor of the *International Journal of Space-Based and Situated Computing* and *Sustainable Cities and Society*.

ABDULAZIZ ALDEGHEISHEM received the bachelor's degree in planning and urban design from the College of Architecture and Planning, King Saud University, the master's degree in city planning from the University of Pennsylvania, Philadelphia, USA, in 2001, and the Ph.D. degree in urban planning and spatial information from the University of Illinois at Urbana–Champaign, USA, in 2006. He also received a Certificate in Urban and Regional Planning Studies from MIT, Cambridge, Massachusetts, USA. He worked as the Head of the Department of Urban Planning, in 2012. He worked as an Adviser in a number of government agencies and supervised many projects and specialized studies. He is currently the Dean of the College of Architecture and Planning, King Saud University, and an Associate Professor with the Department of Urban Planning, College of Architecture and Planning, KSU. He also works as an Adviser with the Vision Realization Office (VRO) at the University, and the Supervisor of the Traffic Safety Technologies Chair. He is interested in the role of spatial information in urban planning and management, also he focuses on areas related to urban planning, spatial management, and smart city technologies.

MUHAMMAD SHAFIQ received the master's degree in information technology (IT) from the University of the Punjab, Gujranwala, Pakistan, in 2006, the M.S. degree in computer science from the University Institute of Information Technology, Arid Agriculture University, Rawalpindi, Pakistan, in 2010, and the Ph.D. degree in information and communication engineering from Yeungnam University, South Korea, in February 2018. He was with the Faculty of Computing and IT, University of Gujrat, Gujrat, Pakistan, as a Faculty Member, from 2010 to 2014, and formerly held the same position with the Department of Computer Science and IT, Federal Urdu University, Islamabad, Pakistan. His research interests include the Internet of Things (IoT), cognitive radio-based IoT networks-architecture and design, mobile ad hoc networks, wireless sensor networks, performance, management, and security, 5G cellular networks, admission control, and mobility management, device-to-device communications, medium access control protocols, Internet routing protocols, spectrum trading and auctions, information systems, design, and access control, and human–computer interaction.

NABIL ALRAJEH received the Ph.D. degree in biomedical informatics engineering from Vanderbilt University, USA. He worked as a Senior Advisor with the Ministry of Higher Education, where his role was implementing development programs, including educational affairs, strategic planning, and research and innovation. He is currently a Professor of health informatics with King Saud University and the Rector of Prince Mugrin Bin Abdulaziz University. He is also a Board Member of several private Universities in Saudi Arabia.