IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 10, 2020, accepted June 23, 2020, date of publication June 29, 2020, date of current version July 9, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3005541

Blockchain and Trust for Secure, End-User-Based and Decentralized IoT Service Provision

BESFORT SHALA[1,2], ULRICH TRICK[1], ARMIN LEHMANN[1], BOGDAN GHITA[2], AND STAVROS SHIAELES[3], (Member, IEEE)

[1]Research Group for Telecommunication Networks, Frankfurt University of Applied Sciences, 60318 Frankfurt, Germany
[2]Centre for Security, Communications and Network Research, University of Plymouth, Plymouth PL4 8AA, U.K.
[3]Security Research Group, School of Computing, University of Portsmouth, Portsmouth PO1 2UP, U.K.

Corresponding author: Besfort Shala (shala@e-technik.org)

This work was supported by the Faculty of Computer Science and Engineering, Frankfurt University of Applied Sciences, Germany.

ABSTRACT Building trust relationships between different decentralized entities in the IoT ecosystem is essential. Hereof, the combination of blockchain technology and trust evaluation techniques is recently considered as an efficient measure. However, both technologies within the IoT are still facing some limitations which are addressed in this research. First, this publication reviews various blockchain-based trust approaches and depicts their strengths and limitations regarding their usage in decentralized IoT communities. Then, an optimized trust model with a multi-layer adaptive and trust-based weighting system is proposed. Additionally, different trust metric parameters and their mathematical models used for trust evaluation are presented. Moreover, this publication presents a novel approach for incentivization processes in the IoT marketplace using control loops and smart contracts. Thereby, participants are motivated to continuously improve their behavior. Finally, the proposed trust model is proved to be reliable. The experimental results conducted from different scenarios show that the presented approach provides more resiliency against various attacks than existing ones.

INDEX TERMS Blockchain, Internet of Things, services, trust, smart contract.

I. INTRODUCTION

A. BACKGROUND

The traditional IoT ecosystem for service provision relies on commercial service providers which create IoT services for specific business processes running in centralized infrastructures. The integration of end-users in the service provision process enables flexibility, decentralization, service variety and energy efficiency in the marketplace. Local resources have a high potential to support smart environments for other service consumers in the IoT ecosystem [1]. However, the lack of centralized coordination and the presence of inexperienced end-users acting as service providers are associated with minimal trustworthiness between entities in a decentralized IoT ecosystem. This has a negative impact on the overall security of the network and a countermeasure against this bottleneck is the design of trust management systems. The ITU-T [2] also highlights the necessity of trust for ICT infrastructures and services.

The literature provides a considerable amount of publications [3]–[5] dealing with trust management systems in different domains (IoT, WMN (Wireless Mesh Networks), MANET (Mobile Ad-Hoc Networks), VANET (Vehicular Ad-Hoc Networks), P2P (Peer to Peer) Networks). However, traditional approaches suffer from a low decentralization level of their trust systems, missing initial trust score evaluations, insecure trust data storage and uncomplete trust models. The blockchain technology provides convenient optimization elements in order to overcome trust and data integrity issues. Recently, the blockchain technology has also attracted researchers to integrate its features in trust management processes within IoT. However, the blockchain technology in its current form is not suitable to be integrated into IoT systems due to security issues, such as the overall trustworthiness of the participating nodes. Moreover, limitations regarding the consensus-building within the network should be optimized and adapted to the specifications of the IoT community. Furthermore, decentralized issues should be considered, and trust-building processes be merged within the blockchain processes in order to maximize the benefits of using blockchain.

The associate editor coordinating the review of this manuscript and approving it for publication was Hong-Ning Dai.

B. MOTIVATION AND KEY CONTRIBUTIONS

The security limitations of decentralized IoT service provision approaches, the deficits of existing trust management systems and several challenges for blockchain integration in IoT highlights the importance to design an optimized framework. Previous works have initially addressed issues, such as the lack of trust in end-user based IoT ecosystem [18], by providing a decentralized approach for trust evaluation. The authors in [19], [20] provide an optimized trust framework where blockchain is integrated for integrity reasons. Moreover, they optimize the consensus methods used by the participants in the blockchain network. However, they do not consider an incentivization system to motivate low trusted peers to increase positively their performance. Furthermore, the works in [18]–[20] lack details on the trust metric parameters and the mathematical model. Additionally, they do not present a trust aggregation scheme for the gathered trust information. Finally, prior works do not highlight the performance of the trust model in relation to others.

The main contributions of this paper are summarized as follows:

1. Reviews recently published blockchain-based trust approaches in the IoT field which aim to benefit from the blockchain technology. The review consists of the definition of several criteria relevant for the assessment based on the characteristics of decentralized IoT ecosystems.
2. Proposes an optimized and blockchain-based trust approach considering strengths and limitations derived from the related work and covering several relevant trust aspects in IoT. Moreover, this publication presents a blockchain-based trust evaluation process using a lightweight and trust-based consensus protocol for decision making in the P2P network.
3. Presents different trust metrics and accordingly describes their mathematical models used for further trust computations.
4. Presents a multilayer weighting system combined with blockchain principles to aggregate the overall trust score of peers in fully decentralized IoT marketplaces.
5. Introduces conceptionally a novel concept of combining control loops, blockchain and trust to motivate good participation of service providers in the network. In order to realize the incentivization process using control loops, smart contracts are integrated.
6. Evaluates the proposed holistic trust model by highlighting its resiliency against trust attacks and by showing its strengths in contrast to other existing models.

C. PAPER ORGANIZATION

This publication is structured as follows: Section 2 presents a review of blockchain-based trust approaches in IoT and summarizes challenges for an ideal trust management system considering the different characteristics of decentralized IoT networks and the special nature of end-user-based environments. Section 3 presents an optimized trust model for evaluating the trustworthiness of IoT services. Moreover, it defines the mathematical model of all trust metrics and their corresponding sub-metrics used for trust evaluation. Additionally, it presents a novel concept to combine blockchain, trust and control loops to optimize the overall trust in the IoT marketplace. Section 4 introduces the integration of blockchain for trust data storage and trust evaluation. Furthermore, it presents a novel multi-layer and trust-based weighting system to increase the trustworthiness of the trust model. Finally, section 5 shows the experimental results of the proposed trust model against several attacks.

II. CHALLENGES FOR A TRUSTED AND BLOCKCHAIN-BASED TRUST MANAGEMENT SYSTEM

A. BLOCKCHAIN IN DIFFERENT APPLICATION FIELDS

Blockchain has now gained much attention in the academia and industry and its integration in different applications is increasing permanently. The diversity of blockchain publications enrich different sectors, such as healthcare, finance, energy, media telecommunication, Internet of Things [52]. For instance, approaches in the healthcare sector try to optimize data security [33] and authentication schemes [34] for electronic health records. Other authors propose to integrate the blockchain technology in the energy sector in order to enable decentralized electricity load verification, decentralized energy marketplace, P2P energy load management or energy consumption reporting [35], [36]. Blockchain is also introduced to support processes in Artificial Intelligence (AI) [37] or P2P applications [38]. Different blockchain-based approaches aiming to benefit from its tamper-proof and decentralization feature are also present in the field of VANETs [39], [40]. Some other authors dealt with scalability issues and resource constraints when implementing blockchain in IoT devices by proposing an optimized blockchain framework with a light-weight consensus method [49], [50]. Others integrate blockchain to mitigate security issues and problems with centralized entities in Federated Learning processes (a cooperative approach to distributed learning) [51]. The powerful combination of blockchain and smart contracts (self-executing codes) within IoT is highlighted in [31], [32], [57], [58]. Several researchers propose approaches to optimize data integrity [41]–[43] or the access control systems [44]–[46] in IoT networks. In the context of IoT, specifically in the Industrial IoT, different blockchain-based approaches are also present [47], [48], [56].

The following subsection presents a review of relevant blockchain-based trust approaches in IoT.

B. REVIEW OF BLOCKCHAIN-BASED TRUST APPROACHES IN IOT

One of the key limitations of traditional trust management approaches is the insecure data storage leading to unreliable trust information about peers in a network. Trust information used to build trust relationships among peers can be manipulated and misused by malicious peers. Another problem

is the missing leader or centralized entity for coordinating several decision-making processes in the community. However, a centralized component should be avoided to limit autocracy behavior in a network and to overcome single-point-of-failure issues. To overcome this, the blockchain technology provides the possibility through cryptographic principles and related consensus protocols to securely store information in its ledgers and thus to increase the integrity level of that information. Smart contracts in combination with blockchain enable the automation of processes in a network without the need of a coordinator. The benefits of these technologies and their integration for decentralized M2M/IoT services are initially introduced by the authors of this publication in [6]. The combination of blockchain technology and trust management systems to enhance the overall privacy, security and trust level is introduced in different application fields such as in P2P networks [26], Vehicular Networks [25], [27], MANETs [30], Robotics [28], Autonomous Systems [29]. Some surveys, such as in [9] reviewed several existing blockchain-based approaches introduced within that domains. However, recently published publications aiming to integrate blockchain for trust management optimization in IoT are not addressed. In the following, the most relevant trust approaches are reviewed concluding with their strengths and limitations for using them in decentralized IoT communities.

A blockchain-based trust system was proposed in [10], where the lack of trust between different IoT domains is identified. Every domain has its own manufacturer, which creates a root of trust suitable only for devices within the single domain to communicate securely. The authors in [10] introduced initially a distributed credit-like system (using a platform called obligation chain) including a reputation mechanism which enables every service provider to accept or decline obligations of service consumers. The obligation chain is a distributed ledger used to store signed obligations (done outside the chain) between service providers and service consumers. To protect against malicious nodes, the authors propose to use so-called proof of commitments for service providers and proof of fulfilments for service consumers, which are using the information regarding obligations and fulfilments stored in the distributed ledger. The cooperation between a service provider and consumer is done by exchanging terms of use (created by service providers) and obligations (defined by consumers). The authors used a combination of their introduced obligation chain and the standard bitcoin blockchain to access the credibility of the obligation issuer. On top of the obligation chain, a three-way handshaking protocol is proposed to bridge trust between different domains. This protocol consists of the setup, spend, and fulfilling phase, using information stored in the distributed ledger to handle service handlings between service providers and service consumers. Reputation scores of service consumers are stored in the distributed ledger and evaluated locally (by every service provider when required) based on the average obligations fulfilled on time by the consumer.

Similarly, the authors in [11] presented a blockchain-based trust management system to evaluate the trustworthiness of devices and to securely store and share trust information in the blockchain via transactions. The proposed system relies on a network model with different manufacturing zones containing physical resources such as IoT devices, an authenticator acting as authorization entity, a trust manager managing and evaluating the trustworthiness of the zone members, miners collecting trust information in a block, broadcasting them and verifying other blocks. For trust evaluation, the authors are using direct observations of the packet delivery behavior and recommendations from other nodes. Specifically, the entities cooperativeness, competence, community of interest and the credibility toward recommendations are used as trust metrics. For blockchain activities, the authors propose to use a private blockchain called multichain using a round-robin algorithm for approving transactions minimizing complex computation resources. The trust computation of the trust manager will also consider the experience scores computed from devices based on their communication with direct neighbors.

The authors in [12] propose a blockchain-based approach combined with smart contracts to evaluate the trust of IoT devices. The authors propose to use smart contracts to set endorsement policies for new transactions. Thus, after a transaction is proposed by a client (IoT device), other nodes called endorsing peers, will evaluate them concluding with the acceptance or rejection of the transaction. Transactions with chain code are only accepted if the trust score of participants is high enough. Blockchain activities are done by peer nodes considered as trustworthy. Only authorized clients can join the blockchain networks (permissioned) and the participants are assigned with trust points which are updated based on rating resulting from interactions between two participants. Interactions between two nodes are enabled using smart contracts which check the trust points in relation to the thresholds. Balance of trust points is stored in the blockchain. The authors refer to trust evaluations in two cases. Trust evaluation using Packet Delivery Rate as trust indicator and performed directly after each interaction between two participants and trust evaluation done by the blockchain nodes after a peer initiates a transaction proposal (seems more to be a trust checking smart contract).

The authors in [13] present a dynamic trust evaluation system which uses a consortium blockchain to track interactions among supply chain participants. The trust score is assigned based on these transactions and has a special focus on this trust data. Therefore, raw data including supply chain data (produced by sensor devices), trade events between entities, and regulatory endorsements are stored off the chain. Their hash values are sent to the blockchain via transactions which trigger smart contracts to automatically calculate trust and reputation scores based on the provided data.

The blockchain is used among others to store the hashes of the supply chain data and the digital profiles of all entities (containing the trust information). Smart contracts are also used to include quality assessments between the participants

to incentivize participants to contribute trustworthily. Entities joining for the first time the network (without past reputation), will be assigned with a minimum trust score by default. The authors in [13] state that the overall trust score of an entity is calculated based on the overall reputation score and some other feature scores (e.g. consumer feedback) and the weighting factors for the trust evaluation are determined by the business network administrator which also manages the blockchain network and defines the business network model.

The authors in [14] introduce a trust management architecture where trust values of service providers are stored in the blockchain. The system architecture proposed in [14] consists of one layer with distributed IoT devices providing services to each other and a second layer with distributed fog nodes which are responsible for the management and control of IoT objects. The fog nodes also maintain a blockchain which is used by the IoT devices to store trust information in it. The transactions in the blockchain are validated by the fog nodes using the Proof of Stake (PoS) Algorithm. The trust model used in [14] to evaluate the trust level of IoT objects considers only honest IoT devices for reporting recommendations (based on the interaction experience) about other IoT service providers sending to its managing fog (home fog node). Interaction experience means the recommendation of an IoT device toward other IoT service providers regarding a used service. The transactions containing trust information are sent by the home fog node to other fog nodes part of the blockchain for validation (which are using the Proof of Stack algorithm for consensus). A Distributed Hash Table is used to store information about available services provided by potential service providers.

The authors in [15] propose a blockchain-based approach for improving end-to-end trust in different IoT applications. Therefore, they introduce a layered trust architecture for IoT blockchain where trust is considered for data observation and blockchain validation. Data observation includes data from different sources such as from IoT devices where the hash values of these data are stored off-the-chain and in the blockchain (via transactions) for integrity reasons. For trust management, the authors introduce a data trust module and a gateway reputation module. While the data trust module evaluates the trustworthiness of observation data based on behavioral information of the data source and related information from other sources, the reputation module provides reputation information about participants to the blockchain and to the application layer. The presented trust model in [15] relies mainly on the confidence of the observations taken between the nodes, the confidence of the data sources, the reputation of data sources, and the evidence taken from other observations. The gateway nodes participate in block generation, validation and distributed consensus in the private blockchain network where only nodes with permission can participate and no competition for block generation among them is required. Based on the information included in blockchain transactions the gateway nodes (are selected periodically) calculate the evidence and the sensor reputations to assign trust values for the sensor observations. The generated block includes transactions containing observation data, public key and signature of data sources, assigned trust value for the observation and the updated reputation of the data source. Furthermore, the authors propose a reputation-based block validation by considering validations of data stored in the blockchain with data provided by nodes and the reputation scores of block generating nodes.

In addition, the authors in [16] propose to use a behavior monitor system in IoT-blockchain infrastructures that can store IoT device data and classifies normal or malicious behavior based on these data. Their system model considers different declared IoT-zones used for different IoT use-cases where each zone has its local blockchain network used to store all kind of communications between devices in the form of blockchain transactions. Every zone has its master node selected based on the resource capability and used for main blockchain activities, such as for creating new blocks. Moreover, the master node centrally processes all incoming and outgoing transactions to and from a zone. The authors propose a behavior monitor for each zone (configured on the master node) which classifies the behavior of every device and compute a level of trust on each zone using learning neural networks such as deep auto-encoders.

The authors in [17] present a blockchain-based trust evaluation for IoT devices (with focus on the home network), where reported histories stored in a blockchain are used to compute the trust scores for each class of devices. Initially, the authors propose to isolate groups of devices in network slices using their own defined SDN-based home controller. Through a simplified risk assessment scale, users are able to assign desired trust levels to those isolated slices. The controllers then use this information to check if the devices are meeting the user's expectation. Therefore, the current trust score of the devices is evaluated and compared to the expected trust level. The trust score is evaluated using the proposed trust assessment system which consists of the Terms of Use (TERMS), where the properties and capabilities of a device designed by its manufacturer are specified. Deviations and reports are also part of the trust assessment system where the first one defines the behaviors that do not follow the TERMS and the second one is the behavior feedback monitoring done by network controllers of devices. All these three elements (with crowd-sources nature) are stored in the blockchain and used to compute the trust scores of devices based on observed behavior history. The authors also introduce an analyzer element as a local trust assessment entity in home networks believing that global trust assessments are not suitable in environments with different policies and security or privacy requirements. The analyzers are used to analyze the data from the blockchain and to do based on this information the trust evaluation for the devices.

The existing trust approaches in IoT [10]–[17] summarized above provide interesting facts regarding the combination of blockchain and trust to enhance the credibility of services

in decentralized networks. In this context, IoT environments where end-users act as service providers removing the need for centralized, dependable, or specialized entities urge the consideration of trusted environments enabled by trust management approaches fulfilling special requirements. Thus, different aspects of existing trust approaches are considered in the review by focusing on general, blockchain-based and trust-based factors which are derived throughout the evaluation or are defined initially based on the special characteristics and needs of an end-user based and decentralized IoT service provision approach. The following factors (elements) are considered in the assessment of existing blockchain-based trust approaches in IoT.

Initially, the decentralization regarding the IoT environment, the trust management and the blockchain activities are highly considered to avoid monopolization, aristocracy, and other problems arising with centralized approaches. Besides, the power of end-users is emphasized in the introduction of this publication and in this context, the integration of end-users in trust and blockchain activities is recommended to be also in line with end-user-based service provision. Another point is the trust incentivization in order to motivate peers to participate actively and trustworthy in different community activities. The incentivization should also include punishments for passive or not-well behaving activities. Another element considered in the evaluation is the level of suitability of existing trust approaches in order to be used for autonomous and decentralized IoT application provision (ADIoTAP), where end-users are acting as service providers. Next to them is the information storage type used in the approaches is derived. Considered type solutions are centralized or local storage nodes, Distributed Hash Tables or blockchain-based ledgers.

Blockchain-based factors start with the trust data storage, defining whether trust information is stored in the blockchain (on-chain) or outside (off-chain). Two other important elements considered are the blockchain type (could be private or public blockchain) and the blockchain operation mode (closed - permissioned or open - permissionless). To enable decision-making in decentralized networks respectively in blockchain networks and to ensure that all nodes have the same copy of the ledger, another blockchain feature analyzed in existing approaches and relevant for decentralized IoT services is the consensus protocol. Moreover, the consensus should consider the lightweight characteristics of IoT devices and fog nodes part of the IoT network. Additionally, an emerging protocol in this context is a smart contract, used to automate processes based on a contract between participants without third parties. Therefore, the integration of it and the smart contract use case (for what it is used in the approach) are assessed.

The trust score assignment is part of the trust-based aspects to be reviewed in existing approaches. It consists of whether a trust approach considers both initial trust scores and ongoing trust scores or only one of them when evaluating a peer or application. Next to them, the trust evaluation entity is responsible to evaluate the trust score of a peer or service. This can be done locally or by distributing the task among nodes. Another trust-based element is the trust model and its completeness. That means how complex the model and how many metrics (attributes) does it cover in the trust evaluation. The trust evaluation of an entity produces many trust values which need to be aggregated in order to build the overall trust score of that entity. Therefore, different trust aggregation techniques such as weighted sum, Bayesian models, fuzzy-based algorithms etc. can be used for this process. Finally, the trust management approach should be resilient against different trust attacks performed by one or many peers in the IoT community (trust attack resiliency).

The existing approaches use some features of blockchain, such as the well-known and safe data storage feature using cryptographic principles. However, they do not benefit from the whole potential of blockchain techniques by merging blockchain activities and consensus protocols with trust models. Moreover, they do not provide a holistic trust model covering issues of new services and new service providers in the context of IoT. Next to them, they do not optimize some blockchain drawbacks such as limitations of existing consensus methods.

The assessment has also shown that most of the approaches are using private and closed blockchains focusing more on nodes controllability rather than in transparency for their approaches. Additionally, they do not consider the special nature of end-user made IoT services, where the end-user probably has less technical knowledge and creates IoT services without considering standardized service lifecycle processes. Most of the reviewed approaches are not fully decentralized by using local super nodes for all activities without the possibility to contest outcomes of their tasks. In this context. The trustworthiness of the super nodes is not considered resulting in low credibility regarding their results. Their resiliency against trust attacks (such as bad-mouthing attacks) varies from moderate to low opening the doors for malicious nodes to harm the system. Only a few of the evaluated approaches [12], [13], [15] include reward/punishment systems in the network to incentivize good behavior among the nodes. The benefits of process automation and fully decentralization is also mostly ignored in existing IoT trust approaches. Only the authors in [12] and [13] use smart contracts for checking the trust score respectively computing it. The computation and aggregation of the trust score are addressed only in [11], [13], [15] by using weighted average or machine learning techniques in order to get the final score.

Table 1 shows the outcomes of the evaluation of different blockchain-based trust approaches in IoT. The different characteristics derived through the assessment of the approaches concludes with a low suitability level for using them in end-user based and decentralized IoT service provision approaches.

TABLE 1. Assessment of blockchain-based trust approaches in IoT.

Elements	[10]	[11]	[12]	[13]	[14]	[15]	[16]	[17]
Decentralization	partially	partially	not	partially	fully	fully	not	partially
End-User Integration	no	no	no	no	no	no	no	partially
Trust Incentivization	no	no	yes	yes	no	yes	no	no
Data Storage Type	locally, blockchain	locally, blockchain	blockchain	blockchain	DHT, blockchain	blockchain	blockchain	locally, blockchain
Trust Data Storage	off-chain	on-chain	on-chain	on-chain	on-chain	on-chain	on-chain	off-chain
Blockchain Type	public	private	private	consortium	public	private	private	n/a
Blockchain Operation Mode	open	closed	closed	closed	open	closed	closed	n/a
Consensus Protocol	PoW	Round Robin	n/a	n/a	PoS	periodical selection	individual	n/a
Smart Contract Integration	no	no	yes	yes	no	no	no	no
Smart Contract Use Case	n/a	n/a	check trust score	calculate trust score	n/a	n/a	n/a	n/a
Trust Score Assignment	ongoing	ongoing	ongoing	ongoing	ongoing	ongoing	ongoing	ongoing
Trust Evaluation Entity	local, individual, untrusted	local, individual, untrusted	local, individual, untrusted	distributed, untrusted	local, individual, untrusted	distributed, trusted	local, individual, untrusted	local, individual, untrusted
Trust Model Completeness	low	moderate	low	moderate	low	moderate	low	low
Trust Aggregation	n/a	weighted average	n/a	weighted sum	n/a	n/a	machine learning	n/a
Trust Attack Resiliency	low	low	low	moderate	low	moderate	low	low
Suitability for ADIoTAP	low	low	low	low	moderate	moderate	low	low

III. HOLISTIC TRUST MODEL FOR IOT

A. SYSTEM MODEL

As mentioned in the introduction the end-user together with its personal environment has high potential to support smart environments with their own local resources to enhance the service variety for the community. Thus, this research considers a system model with a completely decentralized IoT ecosystem [1] shown in Fig. 1.

The IoT ecosystem consists of a decentralized P2P network with many end-users in the roles of service providers and service consumers. Every end-user has the ability to manage (1) IoT devices available in their personal environments to design/configure easily IoT services themselves. Moreover, they have the possibility to provide (2) the functionality of local IoT devices to other end-users as a service. New services are announced and registered by storing (3) their service descriptions in the P2P overlay network. Other end-users can retrieve (4) existing descriptions and subscribe to a service in order to consume it (5). The whole workflow is realized without the use of centralized entities (central service providers) or centralized execution environments for IoT. Therefore, every end-user can use their own devices such as routers, smartphones or notebooks as local execution environments, which also fulfil the hardware requirements to act as execution systems for service provider activities. The end-users have also the possibility to cooperate with each other in order to create a complex IoT service (service composition). More details on the decentralized service provision approach can be found in [1].

The decentralized character of the IoT ecosystem with its end-users and their personal environments are used in addition to build a network of trust agents and blockchain nodes performing various trust activities described in the following sections.

B. GENERAL DESCRIPTION OF THE TRUST MODEL

To evaluate the trustworthiness in a completely decentralized IoT community the authors in [18]–[20] propose conceptionally a comprehensive trust model covering several aspects where end-users act as decentralized service providers. The proposed trust model covers aspects such as service functionality, service quality, end-user behavior, end-user task participation. Fig. 2 shows the trust evaluation layer model which are further described.

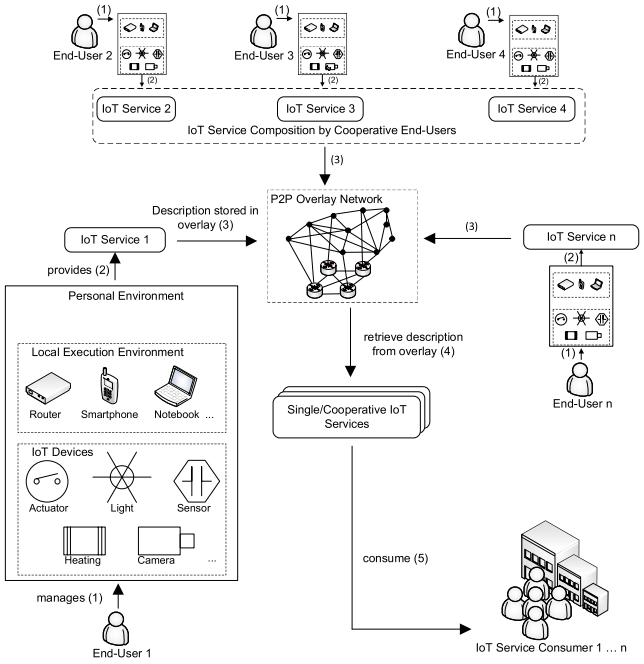


FIGURE 1. Decentralized IoT Ecosystem.

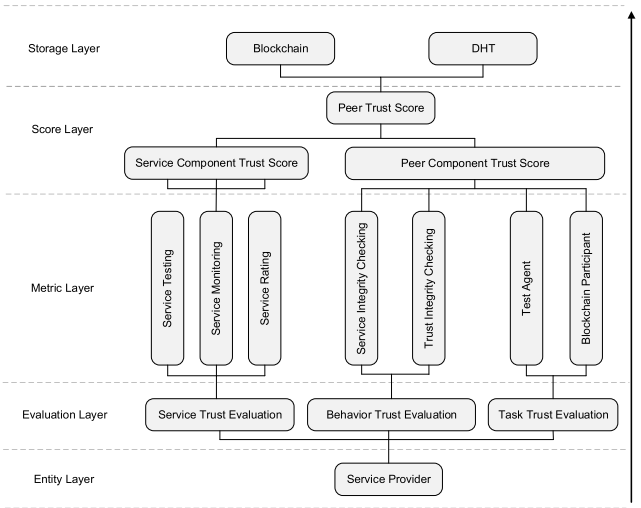


FIGURE 2. Trust evaluation layer model.

Entity Layer: Every end-user (peer) part of the IoT ecosystem has the possibility to evaluate the trustworthiness of other end-users acting as service providers.

Evaluation Layer: Three types of trust evaluations are proposed to be done: evaluation of the services provided by an end-user; evaluation of the behavior of an end-user; evaluation of the end-user participation in community tasks.

Metric Layer: The Service Trust Evaluation consists of several metrics including service testing, service monitoring, and service rating. The Behavior Trust Evaluation consists of testing the integrity of service or trust data. The Task Trust Evaluation consists of checking whether the end-user is participating in different community activities such as testing other peers or performing blockchain actions.

Score Layer: The results of the Service Trust Evaluation will create a component called Service Component Trust Score, which is combined with the component called Peer Component Trust Score (derived from behavior and task trust evaluation) to get the Peer Trust Score of an end-user.

Storage Layer: The computed trust scores are stored in the blockchain (to enable tamper-proof storage) and Distributed Hash Tables (DHT) (to enable fast lookup for information).

One key aspect of the holistic trust model is the possibility to evaluate the trustworthiness of new services or new end-users joining the IoT community. Several other trust models in the literature do not consider the initial trust score of new entities or assign default initial trust scores without validation or based on related information about entities. The proposed trust model in this research is integrating service and performance testing after service deployment in the trust evaluation process. The tests are done by other community members and the results are part of the initial trust score evaluation. This ensures to identify malfunctioning services from malicious or unexperienced end-users (acting as service providers) even in the beginning after services are published to others in the community.

Another important aspect of the holistic trust model is the way how trust data are managed. The increasing number of nodes joining and leaving the network and their possible malicious behavior by removing or changing trust data can harm the whole system and hide a clear view about the truth among good nodes. It has pointed out that blockchain with its cryptographic principles provides a first-class data integrity feature to store data securely in so-called distributed ledgers [7], [8]. Thus, the holistic trust model integrates blockchain for optimizing the storage system and to ensure tamper-proof trust data (introduced in [6]). Calculated trust scores and other related trust information are stored in the blockchain by including the information in transactions, which need to be validated using so-called consensus methods. To overcome several limitations of existing methods, the authors in [19] introduce a Trust-Consensus Protocol, which considers trust in all steps part of the block creation cycle such as the block leader selection, the block generation, and the block validation. The proposed consensus method is not only used for blockchain activities but also for other parts of the IoT eco- system such as service provisioning or peer admission/removal to the IoT community.

C. TRUST METRICS AND MATHEMATICAL MODELS

For each of the trust metrics mentioned in the previous subsection (and illustrated in Fig. 2), there are specific trust submetrics defined and used for the trust evaluation. Table 2 shows the different sub-metrics and their respective symbol used for the mathematical model.

In the following, the different trust metrics and their respectively mathematical model are described.

TABLE 2. Trust metrics and Sub-Metrics.

Trust Metric	Trust Sub-Metric	Symbol
Service Testing	Functional testing	S_{ft}
	Response time	S_{ptnrt}
	Service acceptance	S_{ptar}
Service Monitoring	Service uptime	S_{mtavt}
	Service online/offline actions	S_{mtava}
	Number of times a service is used	S_{mtacn}
	Ratio positive responses	S_{mtar}
Service Rating	Service satisfaction	S_{ratint}
Peer Task Participation	Participation in tasks	S_{tp}
Peer Integrity Checking	Service or Trust Information Integrity	S_{inch}

Service testing – here the service capabilities including service functionality and service performance are tested. The testing occurs for new and existing services and is performed by other end-users' part of the IoT community.

1. Functional testing – a service is assigned with a service description containing information about its functional behavior. Based on this information other end-users are able to automatically generate test cases and to perform functional tests concluding with pass or fail test cases. The functional testing results are expressed in percentage of successful test cases. Through performance feature scaling, a value from 0 – 1 is derived indicating that 0 is the worst value and 1 the best. The following equation is used for standard scaling purposes:

$$s = \frac{s_i - \min(s_i)}{\max(s_i) - \min(s_i)} \tag{1}$$

where: s is the normalized value; s_i non-normalized value (test result); $max\,(s_i)$ is the maximum value; $min\,(s_i)$ minimum value;
Thus, this equation can be transformed for deriving the score for functional testing:

$$S_{ft} = \frac{S_{tr} - \min(S_{tr})}{\max(S_{tr}) - \min(S_{tr})} \tag{2}$$

where: S_{ft} is normalized score regarding the functional behavior; S_{tr} is test result after functional testing; $max\,(S_{tr})$ is the maximum possible test score (equal to 100); $min\,(S_{tr})$ is the minimum possible test score (equal to 0).

2. Performance testing – same as for the functionality, some information about the service performance are assigned in the service description and are going to be tested by other end-users. An important aspect of performance testing is accessibility, which includes the response time (idea adapted from [53], [54]) in comparison to the maximal response time (defined in the service description of the service) and the service acceptance. For response time the following equation has been defined:

for $S_{ptrt} > \max(Resp_{time})$

$$S_{ptnrt} = 1 - \frac{S_{ptrt} - \max\left(Resp_{time}\right)}{\max\left(Resp_{time}\right)} \tag{3}$$

for $S_{ptrt} < \max(Resp_{time})$ then $S'_{ptrt} = 1$;
for $S_{ptrt} > 2\max(Resp_{time})$ then $S'_{ptrt} = 0$;
where: S_{ptnrt} is the normalized score regarding response time of the service; S_{ptrt} is the response time of the service; $\max(Resp_{time})$ is the maximal response time.
For the service acceptance the following equation has been defined:

$$S_{ptar} = \frac{Resp_{pos}}{Req} \tag{4}$$

where: S_{ptar} is the score regarding the service acceptance; $Resp_{pos}$ are the number of positive responses; Req is the number of requests.

Service monitoring – this is happening continuously during the lifetime of a service. The service monitoring is done by other end-users' part of the IoT community. Service monitoring includes some metrics from the performance

1. Availability – is the time a service is online from its starting point and/or the number of online/offline actions a service is doing (idea adapted from [55]). Following equation for service online/offline has been defined:

$$S_{mtavt} = \frac{t_{up}}{t_{up} + t_{down}} \tag{5}$$

where: S_{mtavt} is the score regarding the service uptime; t_{up} is the uptime; t_{down} is the downtime.
For the online/offline actions the following equation has been defined:

$$S_{mtava} = \frac{N_{oa}}{M_a} \tag{6}$$

where: S_{mtava} is the score regarding the online/offline actions; N_{oa} is the number of online actions; M_a are the monitoring actions.

2. Activity – consists of the number of times a service is used by others for a predefined period and the number of positive responses (idea adapted from [53], [54]) handled by the service. The following equation is about the number of times a service is used:
for $N_{sa} < N_{saaver}$

$$S_{mtacn} = \frac{\frac{N_{sa}}{t_{mon}}}{\frac{N_{saaver}}{t_{monav}}} \tag{7}$$

for $N_{sa} > N_{saaver}$ then $S_{mtacn} = 1$;
where: S_{mtacn} is the score regarding the usability of a service; N_{sa} is the number of service utilizations; N_{saaver} is the average number of service utilizations; t_{mon} is the monitoring time period of the service, t_{monav} is the average monitoring time period of services.

Moreover, this is the equation for number of positive responses handled by a service:

$$S_{mtar} = \frac{Resp_{pos}}{Req} \tag{8}$$

where: S_{mtar} is the score regarding the service acceptance; $Resp_{pos}$ are the number of positive responses; Req are the number of requests.

Service rating - other end-users have the possibility to rate a service based on their own experience. This can be done by expressing the service satisfaction S_{ratsat} (using 0 for not satisfied and 1 for satisfied. Another metric is the number of successful interactions (idea adapted from [54]) between a service provider and service consumer. The equation is:

$$S_{ratint} = \frac{I_{suc}}{I_{tot}} \tag{9}$$

where: S_{ratint} is the score regarding the service interactions; I_{suc} is the number of successful interactions; I_{tot} is the total number of interactions

Peer Task Participation – here the effort of end-users for participating in different community tasks is measured. In this context, the participation as a test agent for testing and evaluating other end-users and services is considered. Moreover, the participation in blockchain tasks is also part of this metric. In the following the equation for Peer Task Participation is shown:

$$S_{tp} = \frac{\frac{N_{tp}}{t_{mont}}}{\frac{N_{tpaver}}{t_{montav}}} \tag{10}$$

where: S_{tp} is the score for participation in tasks; N_{tp} is the number of tasks done; N_{tpaver} is the average number of average tasks done; t_{mont} is the monitoring time period of a task; t_{montav} is the average monitoring time period of tasks.

Peer Integrity Checking – considers checking the integrity of service and trust data by comparing information in the P2P overlay and the blockchain. Therefore, the following equation:

$$S_{inch} = \frac{M_{corr}}{C_{tot}} \tag{11}$$

where: S_{inch} is the score for service integrity; M_{corr} are the correct matches; C_{tot} is the total number of checks.

D. TRUST IN THE LOOP FOR TRUST OPTIMIZATION

The trustworthiness of the participants in the IoT community is continuously evaluated. The evaluation will pick out malicious nodes with a low trust score tending to exhibit malicious behavior. Previously, the authors in [20] proposed to punish untrustworthy peers being able to provide or use services and by banning them out the IoT community using smart contracts. Besides them, to increase the overall security and to benefit from local resources of every node, it is recommended to incentivize peers with a low trust score from the network to boost up their trust score by changing to cooperative and good behavior. Therefore, this publication proposes to use the benefits of the holistic trust model, the blockchain, the trust consensus protocol by integrating them in a control loop with feedback functionality. In the context of control loops, the authors in [23], [24] introduce a new concept called User in the Loop (UIL), where the user is part of a control loop and motivated to change the location in order to optimize the signal to interference noise ratio in wireless cellular networks. The basic idea here is to incentivize or motivate the user towards a specific behavior. Afterwards, the behavior is analyzed and based on that the end-user is accordingly informed.

This publication proposes to integrate the UIL concept to the trust paradigm, which is a completely different application field in comparison with the initial usage of this concept in [23], [24]. The proposed control loop is called Trust in the Loop (TIL) and is shown in Fig. 3. The control loop contains a target trust score which has to be achieved by the service provider and the service it is providing. To do so, the Trust Unit will look-up in the blockchain for the current trust score of the ser- vice provider or its service. The current trust score is compared with the target score and if it is below, the Trust Unit will set incentives (e.g. discounts for using other services or more responsibilities for community tasks to increase own trust score) for the service provider. These incentives coupled with relevant service information are sent to the service provider. The service provider then decides whether or not to provide a better service in order to get the benefits promised by the Trust Unit. The outcome of the revised service is the service behavior which will trigger the initiation of a new trust evaluation of the service provider and the service in a feedback loop. The TIL concept can also be applied to service providers or to other relevant tasks in the IoT community. Moreover, it can be used by a service consumer who wants to use a specific rare service (no other alternatives) which has currently a low trust score. The activities of the trust loop are realized completely autonomously through smart contracts. Smart contracts as self-executed codes stored in blockchains and enabling untrustworthy intermediations between entities are very powerful in order to automate processes in a fully decentralized network (originated in [21], [22]).

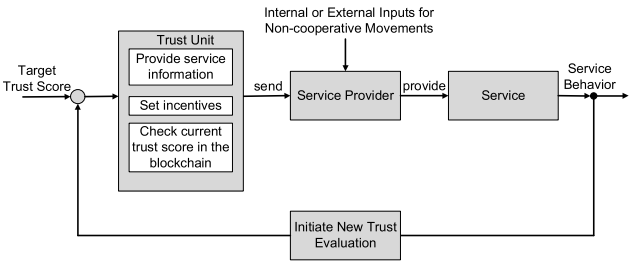


FIGURE 3. Trust in the loop.

IV. TRUST EVALUATION AND AGGREGATION IN DECENTRALIZED COMMUNITIES

A. TRUST EVALUATION AND INFORMATION STORAGE

The authors in [18]–[20] propose a completely decentralized trust evaluation system, where every end-user part of the

community can act as a trust agent by performing trust activities described in section II. As mentioned in [6] evaluated trust scores are stored in the blockchain to secure the integrity of the data. This publication describes the trust score storage in the blockchain more in detail and how trust is evaluated and aggregated.

First, every end-user evaluates the partial trust score of another service or peer by using one of the defined trust metrics in section III. Afterwards, the evaluated trust score is sent to the blockchain by including the trust information in a transaction. This transaction has initially an unconfirmed status and is waiting to be added to the blockchain. Over time, many transactions are part of the pool of unconfirmed transactions and are containing trust information about different peers and services. Other end-users can use this information to aggregate an overall trust score of the service or peer (by creating a list of transactions for a specific entity which has to be evaluated). Therefore, the collected trust scores are used to create an overall trust score using a dynamic weighting system (described in section V) for every trust metric part of the calculation. Thus, the current overall trust score of a peer or service is evaluated from a peer part of the IoT community, which is selected randomly based on its trust score as a block creator to create the new block (using the Trust-Consensus Protocol [19]). Other peers will receive the newly created block and will have the possibility to check if the block is created correctly. This means that the transactions included in the block are correct, only trusted transactions are considered, trusted block creator etc. The trust score evaluation can be done in predefined timeslots (time-driven) or when a specific number of transactions is reached (event-driven). In cases when a service consumer wants to know the current trust score of a service, a trust score request (using smart contracts) is needed to initiate the trust score evaluation (which triggers the trust evaluation cycle described above).

B. INITIAL TRUST SCORE FOR NEW IOT SERVICES

To evaluate the trustworthiness of new peers or new services provided to the IoT community it was proposed to evaluate the functional behavior and the performance of a service based on the information provided by the service provider [18]–[20]. It can be distinguished between new IoT services provided by a new service provider (peer) or new IoT service provided by an existing service provider (peer). For a new service provided by a new peer, as mentioned, the functional behavior and the performance of the service are considered. The weighting of the two sub-metrics is set based on their importance (further on argued). The functional behavior respectively the functionality of a service has the highest importance. That means if a service does not work the performance will not play a big role for the service consumer. However, if the service works well, then the performance can affect the satisfaction of the consumer. Thus, the weighting score for service testing is set as $\mu_{st} = 0.7$ and for performance testing $\mu_{st} = 0.3$. The reason why performance testing is considered in the weighting is that it could be that a service is partially working or e.g. 90% of the functionality is working correctly. The following equations show the calculation of the initial trust score for a new IoT service provided by a new peer:

$$T_{init}^{np} = \mu_{st} S_{st} + \mu_{pt} S_{pt} \tag{12}$$

where: T_{init}^{np} is the initial trust score of a new service provided by a new peer; S_{st} is the score for service testing; S_{pt} is the score for performance testing.

For new services provided by existing peers, the overall trust score of the peer is also considered in the trust evaluation. The weighting is here assigned as follow: $\mu_{st} = 0.6$ for service testing; $\mu_{st} = 0.2$ for performance testing; $\mu_{et} = 0.2$ for the existing trust score of the service provider. Thus, the following equation for trust evaluation can be presented:

$$T_{init}^{ep} = \mu_{st} S_{st} + \mu_{pt} S_{pt} + \mu_{et} P_{et} \tag{13}$$

where: T_{init}^{ep} is the initial trust score of a new service provided by an existing peer; P_{et} is the trust score of the existing peer.

C. TRUST AGGREGATION SCHEME WITH EFFICIENT WEIGHTING SYSTEM

The evaluation results of the different trust metrics defined in the previous section need to be aggregated to an overall trust score of the end-user (represented as a peer and acting as a service provider). As mentioned, the overall trust score consists of the scores derived from service testing, service monitoring, service rating, peer integrity checking and peer task evaluation. Thus, it is important to assign a weighting system for the different trust metrics as they have a different impact under different conditions on the overall trust score of a service or service provider. Therefore, this publication proposes to combine different aspects in order to present a dynamic weighting system which enables efficient trust aggregation and automatically weighting adjustment based on the current situation in the community.

In the following the steps for trust evaluation, trust weighting, and trust aggregation are described:

1. Every peer in the IoT community also behaves as a test agent performing test activities and trust activities. Moreover, every peer part of the blockchain is able to participate actively in blockchain activities.
2. Peers continuously act as test agents and perform the above-mentioned tests regarding the trust evaluation. The test results are sent as blockchain transactions to the blockchain in order to be stored tamper-proofed in the blockchain.
3. One peer is selected using the Trust-Consensus Protocol as the Block Creator (in Bitcoin called Miner) and starts collecting unconfirmed transactions from the transactions pool in order to form a block. In the collection/selection phase the block creator considers only transactions from peers with average or high trust score. Other transactions are not considered (sorted out) – this ensures that malicious or untrustworthy peers cannot

impact the trust management system and thus many attacks are mitigated.

4. Before forming the block, the block creator sorts the filtered transactions based on the trust metric category and starts some calculations. This includes the weighted average trust score for a specific trust sub-metric (for instance, the block creator collects three transactions consisting with information about the service testing score. Therefore, the average of these three values are calculated). Moreover, the block creator looks up for the trust score of the originator of the transaction in order to consider it also in the trust calculation. This process is done for all other trust sub-metrics. In the end, the block creator will have a list of parameters which will be considered for the next steps of the total trust score computation. The following equation shows the above-described process:

$$S_x^{w_r} = \frac{\sum_{i=1}^{n} T_{p_i} S_{X_i}}{\sum_{i=1}^{n} T_{p_i}} \tag{14}$$

where: $S_x^{w_r}$ is the weighted service trust score for a trust sub-metric; T_{p_i} is the trust score of the peer who has evaluated the service; S_{X_i} the trust score assigned by the peer for the specific trust sub-metric (see Table 1).

5. Another point which has to be considered in the preparation of the trust parameters is the number of tests which are done in a round for a specific trust sub-metric (it could be that service testing is done three times and service rating only one time). Therefore, the following equation is used:

$$S_{nt}^{w_u} = \frac{\sum n_{S_x} S_x}{\sum n_{S_x}} \tag{15}$$

where: $S_{nt}^{w_u}$ is the weighted service trust score for the service/peer metrics based on the trust score of each of the considered sub-metrics and their frequency; n_{S_x} is the number of inputs for a specific sub-metric; S_x is the score for the specific sub-metric (mentioned above).

6. The next step is to rank the different parameters from the worst to the best value. According to this ranking, the weighting to the parameters is assigned. This paper argues that parameters with a bad value should be weighted higher in order to motivate service providers in future rounds to provide better services and to participate actively and positively in community activities. The weighting is done adaptively, that means that every round (every new block and new calculation of the overall trust score) the ranking is done and according to that the weighting is adjusted. A future step could be to include also the trust score of the block creator in the trust evaluation process. Therefore, the following equations are used for ranking the trust parameters (are illustrated with the metric Service Testing):

$$S_{test}^{rk} = 1 - S_{test} \tag{16}$$

$$\alpha = \frac{S_{test}^{rk}}{S_{test}^{rk} + S_{mont}^{rk} + S_{rat}^{rk} + S_{inch}^{rk} + S_{tp}^{rk}} \tag{17}$$

where: $S_{test}^{rk} S_{mont}^{rk} S_{rat}^{rk} S_{inch,}^{rk} S_{tp}^{rk}$ are the ranking values for the metrics Service Testing S_{test}, Service Monitoring S_{mont}, Service Rating, Peer Integrity Che- cking, Peer Task Participation; α is the weighting parameter for the metric S_{test}.

Similar calculations are also done for the other weighting parameters: β (for the metric S_{mont}); γ (for the metric S_{rat}); δ(for the metric S_{inch}); ε(for the metric S_{tp}).

7. The overall current trust score of a peer is computed by considering all derived scores from the different trust metrics (and calculated in the previous steps) weighted with the corresponding weighting parameters derived in step 6. The following equation shows the calculation process:

$$T_{total}^{cur} = \alpha S_{test} + \beta S_{mont} + \gamma S_{rat} + \delta S_{inch} + \varepsilon S_{tp} \tag{18}$$

where: T_{total}^{cur} is the current total trust score of a peer; α, β, γ, δ, ε are the weighting coefficients for the different metrics.

8. To compute the overall trust score, the current one should also be combined with the old one. Therefore, both scores are weighted according to the average peer trust score of each block (last block and current block). The following equation expresses the overall trust score of a peer:

$$T_{total} = \frac{1}{n} \sum_{i=1}^{n} T_{p_i}^{old} \times T_{total}^{old} + \frac{1}{m} \sum_{i=1}^{m} T_{p_i}^{cur} \times T_{total}^{cur} \tag{19}$$

where: T_{total} is the overall trust score of a peer; $T_{p_i}^{old}$ is the average peer trust score of the last block; $T_{p_i}^{cur}$ is the average peer trust score of the current block; T_{total}^{old} is the previous trust score of a peer.

The presented steps for trust evaluation consider a hybrid dynamic (and adaptive) weighting including different weighting aspects in the overall system and enabling trust self-optimization in the whole community.

V. EVALUATION OF THE TRUST MODEL

The previous sections have introduced a comprehensive trust model with its metrics and calculation principles. The proposed novel trust model with its different characteristics, starting from the initial trust score considerations, the different trust metrics, the trustworthy consensus protocol, the trust aggregation concept, and the synergy of blockchain, smart contracts and trust, fulfils all the requirements defined in section 2 (under which other trust approaches are also assessed). This section shows the reliability and resiliency of the proposed trust evaluation system by performing different experiments as shown in the following.

A. EXPERIMENTAL SETTINGS

The evaluation of the presented trust evaluation system consists of different defined experiments and scenarios simulated

under the same general conditions. Ten to fifty transactions per block are conducted where each transaction consists of values regarding the different sub-metrics evaluated by different peers. Moreover, five to ten blockchain circles are executed consisting of five to ten blocks where each block consists of the overall computed trust score of the peer. Experiments comprising the following elements and scenarios are realized: Increasing malicious population (nodes providing false trust information); Impact and evolution of initial trust scores; Static vs. dynamic weighting; Bad-Mouthing Attack (malicious nodes providing bad recommendations to good nodes) [2]; Ballot-Stuffing Attack (malicious nodes providing good recommendations to bad nodes) [2]; Comparative analysis with other existing trust models. Moreover, the experiments include scenarios where all peers are trustworthy (trust score is above equal to 0.5) and scenarios where the percentage of malicious peers trying to manipulate the overall trust score of the evaluated peer sending false trust scores vary from 20% to 80%. Throughout the experiments, the initial trust score capability of the introduced trust model with other approaches providing only default values or no initial trust scores is compared. Moreover, the introduced dynamic weighting system is compared against other approaches with no or static weighting. To highlight the resiliency of the proposed trust model, a comparison with other simple trust models is done to identify the performance differences of both when being attacked by other nodes under increasing malicious population. Finally, a relative trust score is derived and used to assess the accuracy of the proposed trust model in comparison with existing ones in a comparative analysis.

B. EXPERIMENT 1: IMPACT OF INITIAL TRUST SCORE ON TRUST EVOLUTION

As evaluated in section 2, none of the existing trust approaches is providing a considerable solution for initial trust scores of new services. Most of them are assigning default values or considering only experience values for the start. This subsection shows the evolution of the trust score when using the proposed trust model and its initial trust score strategy in relation to existing approaches.

In this experiment, there is a service provider (peer) which has a good trust score (0.8) and provides five services with good performance. At a moment, five new services are added by the service provider and the evolution of its trust score is analyzed when considering the proposed trust approach and two other approaches (with default initial trust score of 0.5 and without initial trust score). Moreover, the performance of the new services is considered bad throughout their lifetime (trust score 0.2). It is also assumed that the existing services are slightly decreasing their trust performance (from 0.8 to 0.55) throughout the block cycles.

The outcome of the simulation (see Fig. 4) shows the evolution of the trust score when the peer is tending to move to a malicious node by providing bad services. The initial trust score consideration and evaluation using the proposed trust

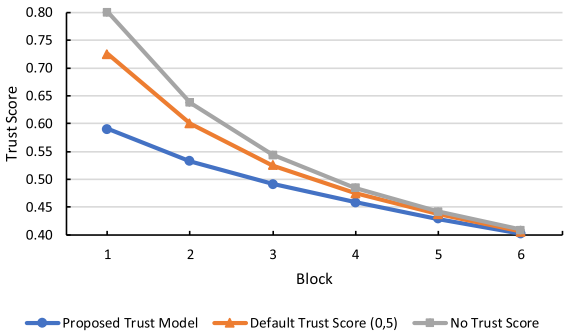


FIGURE 4. Trust evolution with new services (good to bad).

model enables quick identification of malicious or untrustworthy behavior in comparison to existing methods. This supports other peers acting as service consumers in their decisions whether or not to use services from the service provider. This provides better reaction times in mitigating bad nodes (with initial good scores) to participate in community tasks, such as in blockchain activities considering also the Trust-Consensus Protocol.

C. EXPERIMENT 2: STATIC VS. DYNAMIC WEIGHTING

The proposed trust model includes a dynamic weighting system combining different aspects to enable efficient trust aggregation and automatically weighting adjustment based on the current situation in the community. The aim of this experiment is to show the trust evolution when using the proposed dynamic weighting system in comparison with static and no weighting approaches.

In the first scenario, a service provider offers various good services where the number of low trust services (up to 60% of the services) is intentionally increased during different block cycles (eight). The proposed dynamic weighting will assign for each service based on the current situation a weight which will be adapted in future rounds of trust evaluation and aggregation. The static weighting will consider predefined weights for the services without including their current behavior in the evaluation. The proposed trust model motivates the peer to stay active in all steps.

The outcome of this experiment (see Fig. 5) shows that the changing behavior of the peers is detected faster using the proposed trust model with its dynamic weighting system. Using dynamic weighting, bad behavior is identified, and malicious peers are demotivated to keep up with the same activities as it leads to a lower trust score (downgrade) and less acceptance in the community. Moreover, when using static weighting, due to the fact that the trust weights are known, the service providers may neglect one or the other service.

Contrary to the first scenario, the second one considers the situation where a low trust service provider is providing bad services (also lower trust scores) and trying to increase its overall trust score during future block rounds in order to attack the system by seemingly providing some

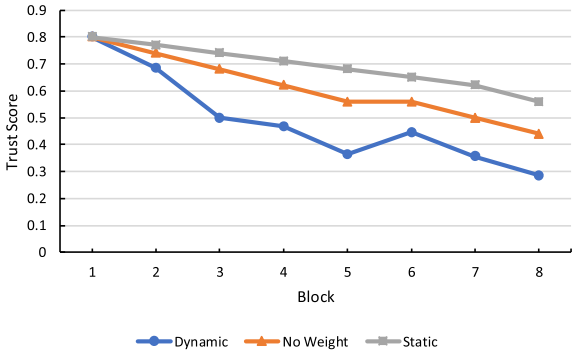


FIGURE 5. Trust evolution – behavior worsening.

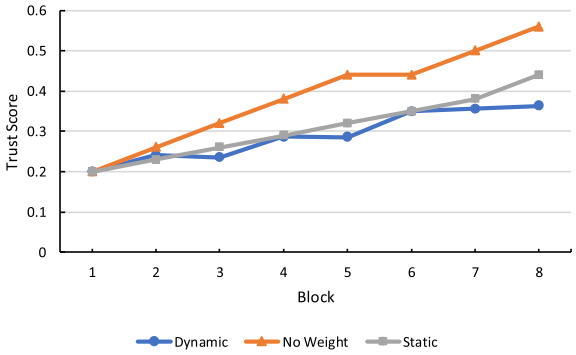


FIGURE 6. Trust evolution – behavior improving.

good services. Fig. 6 shows the outcome of the experiment, where it is illustrated that the trust evolution with dynamic is increased more slowly than with static or no weighting approaches. The bad service provider does not have the possibility to boost up its trust score in this way and is demotivated (considering also the first scenario) to behave passively or bad in the community.

Similar results are also conducted when applying this experiment to a service provider providing with just one service but changing the performance of individual characteristics of that service.

D. EXPERIMENT 3: PROPOSED TRUST MODEL VS. SIMPLE TRUST MODEL – BAD-MOUTHING ATTACK

This section evaluates the resiliency of the proposed trust model in comparison to a simple trust model (with basic average calculations) against malicious nodes in the network performing bad-mouthing attacks [2], where bad or malicious nodes provide bad recommendations for good nodes. The aim of this experiment is to compare the two models with each other by showing the differences in their performance and demonstrating the stability of the proposed model against attacks.

The attacks are run against one service which is provided by a service provider. The service and the service provider are considered trustful with good trust scores in the past. The percentage of the malicious nodes in the network is increased during the experiment. The malicious nodes are performing bad-mouthing attacks by trying to decrease the overall trust score of the service provider. The aim of the experiment is to identify the changes in the overall trust score of the peer during different block cycles and under different amount of bad-mouthing transactions. Moreover, the resiliency difference between the proposed trust model and a simple trust model is conducted.

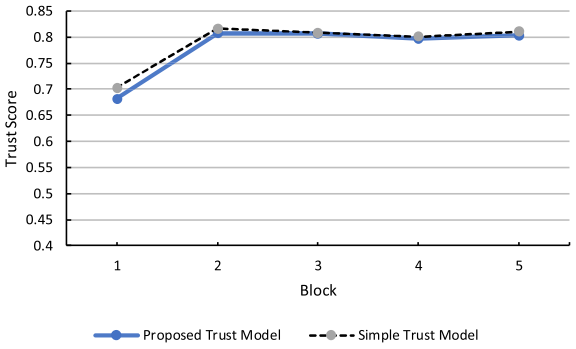


FIGURE 7. Trustworthy peers.

Fig. 7 shows the scenario where all peers participating in the trust evaluation are good (trust score 0.5 or higher) which send different trust scores for the evaluated service and service provider. The outcome of this scenario shows that using the simple model for trust score evaluation, the overall trust score of the service provider is slightly better than with the new proposed model. However, the result using the simple model does not reflect the detailed truth because it fails to include the trust score of all test agents performing the trust evaluation in the overall trust weighting.

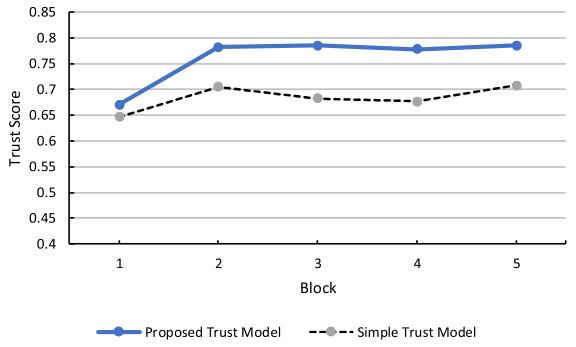


FIGURE 8. 20% Malicious peers.

Figs. 8-11 consider the existence of malicious nodes (with trust score 0.2) which sends transactions with low trust scores about the evaluated service and service provider. These figures show that with the increasing number of malicious nodes the resilience of the trust score evaluated decreases using the simple trust model. Thus, the difference between the trust scores evaluated using the simple trust model and the new proposed trust model increases with the increasing number of malicious nodes. The results also show that the trust score using the new proposed trust model stays stable with only

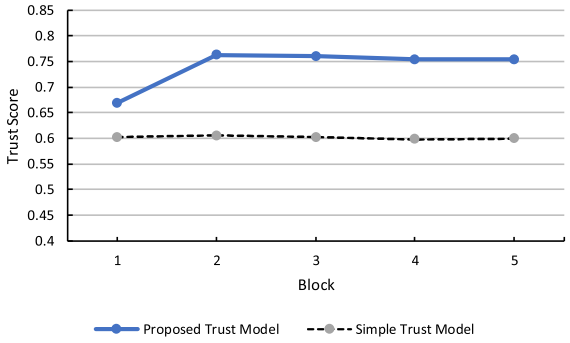


FIGURE 9. 40% Malicious peers.

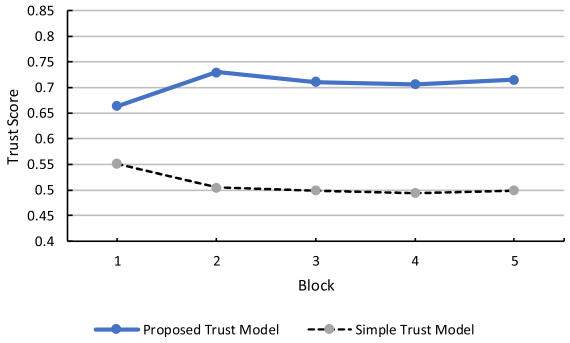


FIGURE 10. 60% Malicious peers.

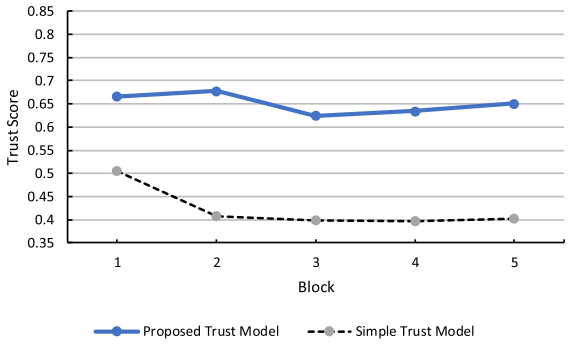


FIGURE 11. 80% Malicious peers.

a minor impact in contrast to the evaluations by malicious nodes.

Fig. 12 shows the trust evolution of the peer versus the increasing percentage of malicious nodes. The outcome shows that the proposed trust model provides good resiliency against attacks even if they increase to an 80% population. This can be argued by the fact that untrustworthy peers and services are ignored in the block building process and the proposed dynamic (adaptive) weighting system.

E. EXPERIMENT 4: PROPOSED TRUST MODEL VS. SIMPLE TRUST MODEL – BALLOT-STUFFING ATTACK

This section evaluates the resiliency of the proposed trust model in comparison to a simple trust model (with basic average calculations) against malicious nodes in the network

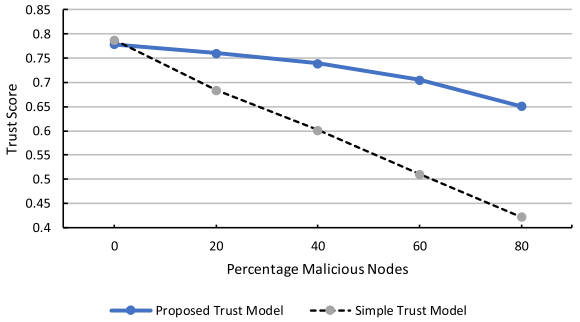


FIGURE 12. Trust Evolution in relation to malicious population.

performing ballot-stuffing attacks [2], where bad or malicious nodes provide good recommendations for bad nodes.

The attacks are run against one service which is provided by a service provider. The service and the service provider have a low trust score with bad trust scores in the past. The percentage of the malicious nodes in the network is increased during the experiment. The malicious nodes are performing ballot-stuff attacks by trying to increase the overall trust score of the service provider. The aim of the experiment is to identify the changes in the overall trust score of the peer during different block cycles and under different amount of transactions. Moreover, the resiliency difference between the proposed trust model and a simple trust model is conducted.

Under normal conditions without malicious peers in the network, the performance of the two models are almost the same (shown in Fig. 13) but the differences appear when starting the attacks. Figs. 14-17 show that by increasing the percentage of malicious nodes, which send good trust scores for a bad service, the proposed trust protocol stays resilient with only a slight impact from wrong trust evaluation scores. In contrast, the simple trust model totally crashes (in terms of successfully being attacked) by increasing the trust score up to 100% of its starting trust score (also shown in Fig. 18).

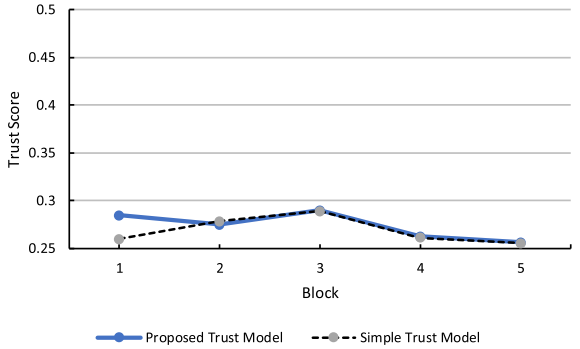


FIGURE 13. Trustworthy peers.

F. EXPERIMENT 5: COMPARATIVE ANALYSIS

This subsection presents a comparative analysis of the proposed trust model against other relevant trust approaches which are theoretically evaluated in section 2:

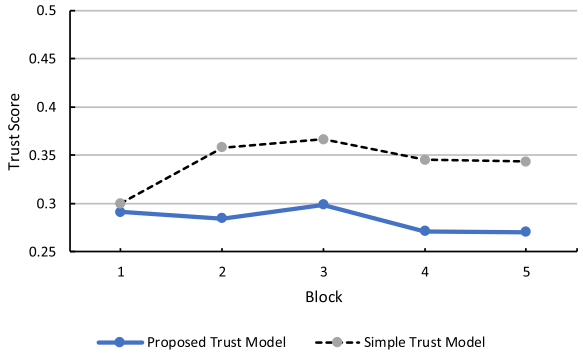


FIGURE 14. 20% Malicious peers.

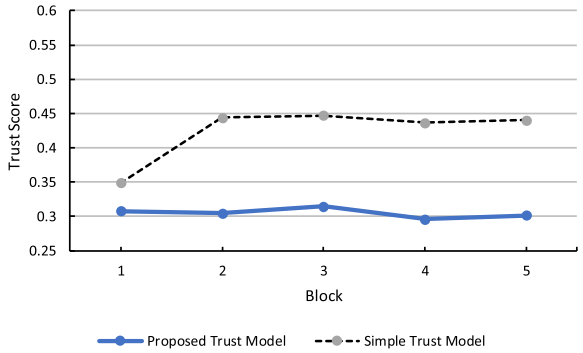


FIGURE 15. 40% Malicious peers.

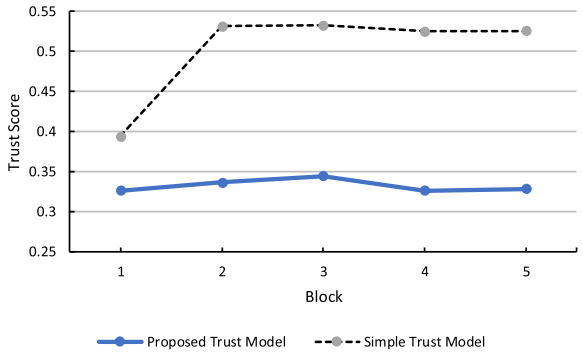


FIGURE 16. 60% Malicious peers.

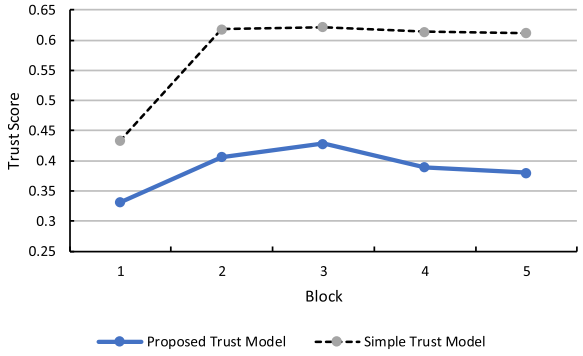


FIGURE 17. 80% Malicious peers.

BlockTIoT [11], HierSysT [14], TrustChain [13], SybRet [12], and TArChain [15]. The comparison focuses on the performance of the different protocols under different

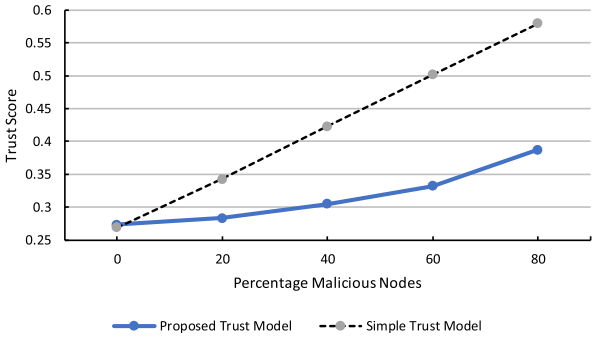


FIGURE 18. Trust evolution in relation to malicious population.

attacks and increasing population of malicious nodes. Initially, based on the trust average of all evaluated trust models the relative trust score is defined and used to assess the reliability of them under malicious conditions.

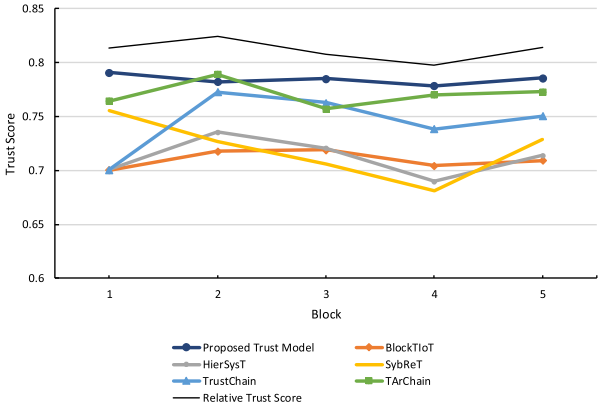


FIGURE 19. 20% Malicious peers.

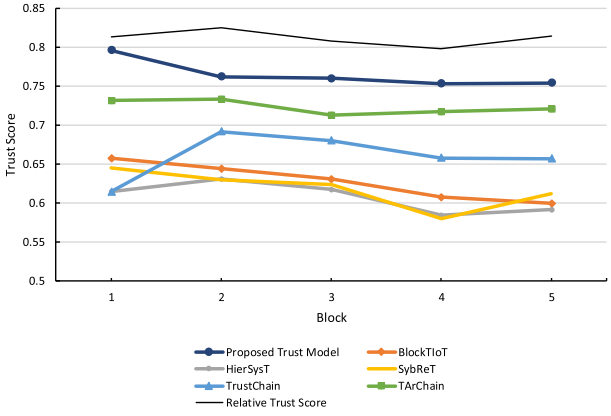


FIGURE 20. 40% Malicious peers.

Figs. 19-22 demonstrate the performance of the different trust models under the bad-mouthing attack for different block rounds and different malicious population. It can be seen that the proposed trust model stays quite stable and resilient throughout different scenarios. The increasing percentage of false trust information is ignored by the proposed

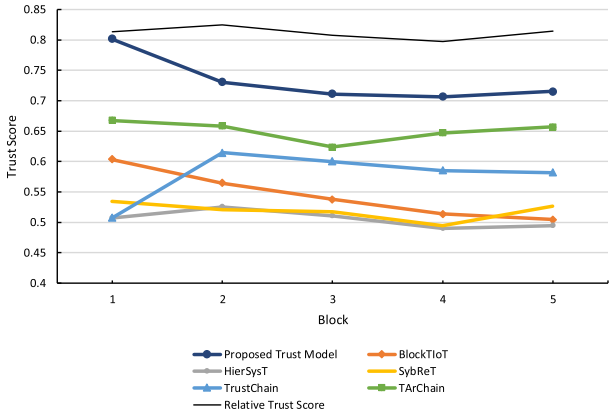


FIGURE 21. 60% Malicious peers.

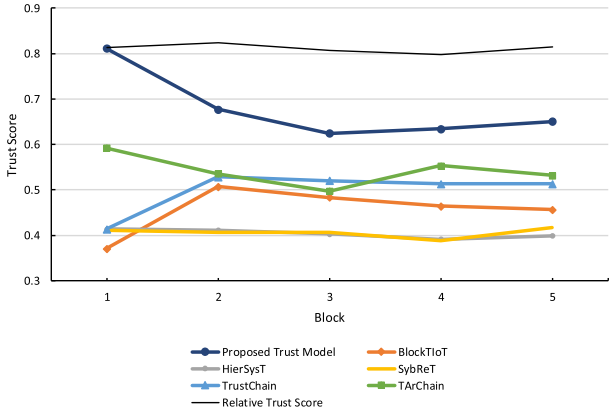


FIGURE 22. 80% Malicious peers.

trust model due to the fact that evaluation results from untrustworthy peers are completely ignored in the block building process in the IoT community. Moreover, the impact of the initial trust score enables a true start in the trust-building process providing overall several advantages besides existing approaches. Other approaches present limitations in terms of trust reliability because of uncomplete trust metric lists, susceptible weighting systems, and/or missing trust entity considerations. Fig. 23 confirms the trust resiliency of the proposed trust model in comparison to BlockTIoT [11], HierSysT [14], TrustChain [13], SybRet [12], and TArChain [15] under increasing malicious nodes population in the network. As a result, bad-mouthing attacks, where nodes try to downrate a good performing node, are almost mitigated by the proposed trust model.

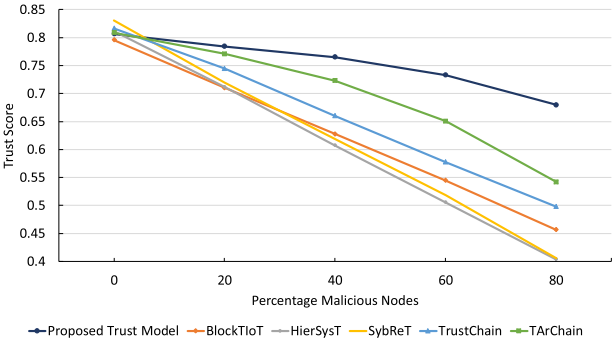


FIGURE 23. Trust evolution in relation to malicious population.

The results of the ballot-stuff attack performed against the different trust models are shown in the Figs. 24-27. Here the malicious nodes are trying to rate up one of their "friends" in order to harm the system. The figures illustrate

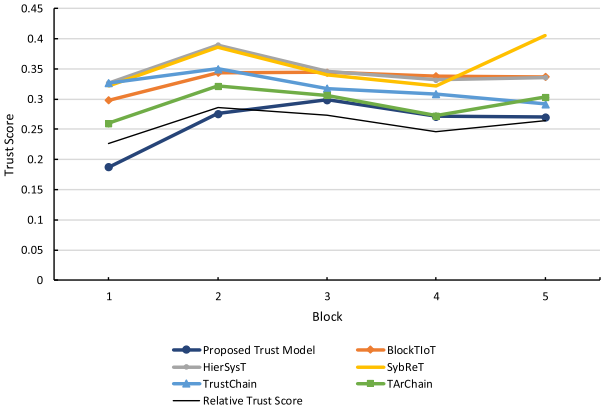


FIGURE 24. 20% Malicious peers.

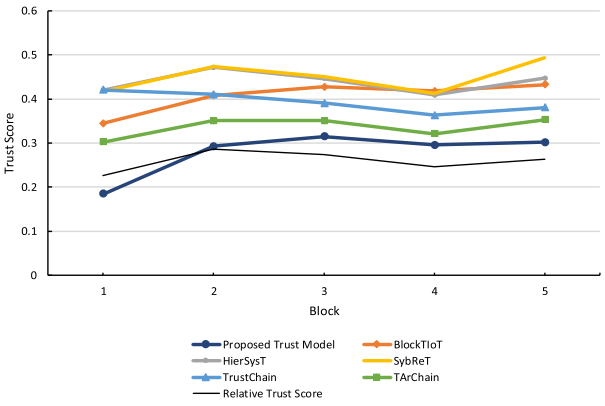


FIGURE 25. 40% Malicious peers.

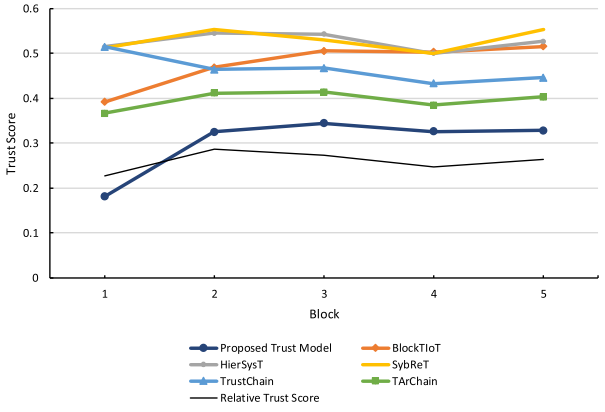


FIGURE 26. 60% Malicious peers.

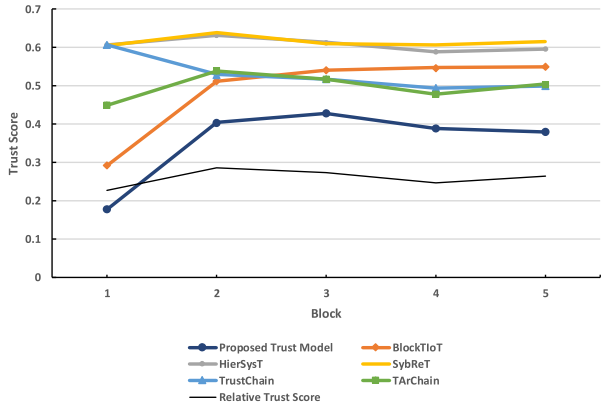


FIGURE 27. 80% Malicious peers.

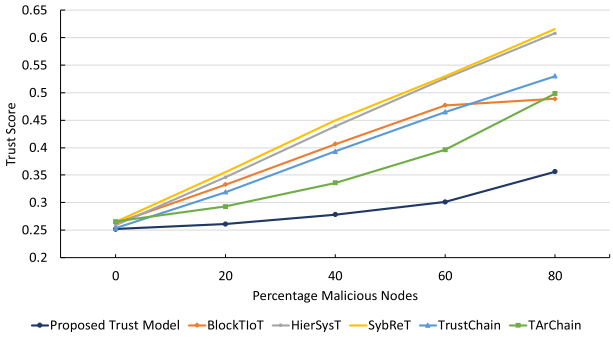


FIGURE 28. Trust evolution in relation to malicious population.

that the proposed trust model is only slightly impacted by this attack and the global view about the bad node will remain untrustworthy throughout the different block rounds. The trust evolution under increasing malicious population can be seen in Fig. 28 and demonstrates again the reliability and stability of the proposed trust model. Most of the existing trust models are quickly impacted by the attack, giving the malicious nodes the possibility to change the opinion in the community, which afterwards leads to further attacks.

The comparative analysis performed in this subsection demonstrates the high resiliency of the proposed trust model against different attacks (bad-mouthing and ballot-stuffing). The increasing percentage of malicious nodes in the network will also have a low impact on the performance of the proposed trust model. Moreover, the different experiments conducted in this section shows the advantages of the proposed trust model, such as the initial trust score evaluation or the dynamic weighting system. Next to them, the trust inclusiveness in all steps of the trust evaluation process and the blockchain activities ensures high reliability on the outcomes.

VI. CONCLUSION

In order to effectively counteract several security and trust issues present in decentralized IoT communities, this research proposes to use the powerful attributions derived from the synergy of blockchain and trust. Therefore, this paper first presents a comprehensive review of existing blockchain-based trust approaches and provides information about their suitability to decentralized IoT communities. Then, it introduces a holistic trust model which does not only cover the trust status of existing services or service providers but also considers the trustworthiness of new joining entities. Single point of failure issues are completely eliminated by a fully decentralized trust evaluation system. Furthermore, the community members are motivated to act in several community tasks through trust competitions. This research publication also provides detailed information on the trust metric parameters and presents their mathematical model used for trust evaluation. Moreover, it introduces a new trust aggregation scheme comprised of a dynamic weighting system in order to compute reliable trust scores of the participating entities in an IoT community. Through a previously introduced trust consensus protocol, the trust evaluation and aggregation steps are highly optimized in terms of trustworthiness and reliability. Only trustworthy peers are allowed to proceed, create and validate transactions/blocks used for the different trust processes. Additionally, this paper proposes to combine blockchain and trust with control loops to introduce a novel concept which optimizes the security of the ecosystem by incentivizing low-trust peers to improve their behavior in the community. Finally, the performance of the trust model is demonstrated, and different experiments are carried out. The experimental results show that the proposed trust approach outperforms in terms of resiliency and reliability in comparison with existing ones.

Future works will have a special focus on the control-loop concept and their possible integration in several aspects of the decentralized IoT ecosystem. The proposed blockchain-based trust model can serve as a good basis for further research on increasing the trustworthiness in IoT networks with the incorporation of blockchain. Moreover, it can be mapped onto other fields such as in VANETs, Flying Ad Hoc Networks (FANETs) or the Internet of Everything (IoE).

REFERENCES

[1] M. Steinheimer, U. Trick, W. Fuhrmann, B. Ghita, and G. Frick, "M2M application service provision: An autonomous and decentralised approach," *J. Commun.*, vol. 12, no. 9, pp. 489–498, 2017, doi: 10.12720/jcm.12.9.489-498.

[2] *Overview of Trust Provisioning in Information and Communication Technology Infrastructures and Services*, document ITU-T Y.3052, 2017.

[3] M. Gillani, A. Ullah, and H. A. Niaz, "Trust management schemes for secure routing in VANETs—A survey," in *Proc. 12th Int. Conf. Math., Actuarial Sci., Comput. Sci. Statist. (MACS)*, Nov. 2018, pp. 1–6, doi: 10.1109/MACS.2018.8628440.

[4] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 279–298, 2nd Quart., 2012, doi: 10.1109/SURV.2011.042711.00083.

[5] I. U. Din, M. Guizani, B.-S. Kim, S. Hassan, and M. K. Khan, "Trust management techniques for the Internet of Things: A survey," *IEEE Access*, vol. 7, pp. 29763–29787, 2019, doi: 10.1109/ACCESS.2018.2880838.

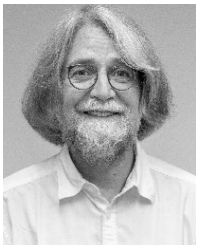
[6] B. Shala, P. Wacht, U. Trick, A. Lehmann, B. Shala, B. Ghita, and S. Shiaeles, "Ensuring trustworthiness for P2P-based M2M applications," in *Proc. Internet Technol. Appl. (ITA)*, Sep. 2017, pp. 58–63, doi: 10.1109/ITECHA.2017.8101911.

[7] *Blockchain-Based Data Exchange and Sharing for Supporting IoT and SC&C*, document ITU-T TS D3.6, 2019.

[8] *Blockchain-Based Data Management for Supporting IoT and SC&C*, document ITU-T TS D3.7, 2019.
[9] E. Bellini, Y. Iraqi, and E. Damiani, "Blockchain-based distributed trust and reputation management systems: A survey," *IEEE Access*, vol. 8, pp. 21127–21151, 2020, doi: 10.1109/access.2020.2969820.
[10] R. Di Pietro, X. Salleras, M. Signorini, and E. Waisbard, "A blockchain-based trust system for the Internet of Things," in *Proc. 23nd ACM Symp. Access Control Models Technol.*, Jun. 2018, pp. 77–83, doi: 10.1145/3205977.3205993.
[11] A. Lahbib, K. Toumi, A. Laouiti, A. Laube, and S. Martin, "Blockchain based trust management mechanism for IoT," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–8, doi: 10.1109/WCNC.2019.8885994.
[12] S. Asiri and A. Miri, "A sybil resistant IoT trust model using blockchains," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1017–1026, doi: 10.1109/Cybermatics_2018.2018.00190.
[13] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "TrustChain: Trust management in blockchain and IoT supported supply chains," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 184–193, doi: 10.1109/Blockchain.2019.00032.
[14] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "An efficient architecture for trust management in IoE based systems of systems," in *Proc. 13th Annu. Conf. Syst. Syst. Eng. (SoSE)*, Jun. 2018, pp. 138–143, doi: 10.1109/SYSOSE.2018.8428732.
[15] V. Dedeoglu, R. Jurdak, G. D. Putra, A. Dorri, and S. S. Kanhere, "A trust architecture for blockchain in IoT," in *Proc. ACM Int. Conf. Mobile Ubiquitous Syst., Comput., Netw. Services (MobiQuitous)*, 2019, pp. 190–199, doi: 10.1145/3360774.3360822.
[16] J. Ali, T. Ali, Y. Alsaawy, A. S. Khalid, and S. Musa, "Blockchain-based smart-IoT trust zone measurement architecture," in *Proc. Int. Conf. Omni-Layer Intell. Syst. (COINS)*, 2019, pp. 152–157, doi: 10.1145/3312614.3312646.
[17] M. Boussard, S. Papillon, P. Peloso, M. Signorini, and E. Waisbard, "STewARD: SDN and blockchain-based trust evaluation for automated risk management on IoT devices," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2019, pp. 841–846, doi: 10.1109/INFCOMW.2019.8845126.
[18] B. Shala, U. Trick, A. Lehmann, B. Shala, B. Ghita, and S. Shiaeles, "Trust-based composition of M2M application services," in *Proc. 10th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2018, pp. 250–255, doi: 10.1109/ICUFN.2018.8436992.
[19] B. Shala, U. Trick, A. Lehmann, B. Ghita, and S. Shiaeles, "Novel trust consensus protocol and blockchain-based trust evaluation system for M2M application services," *Internet Things*, vol. 7, Sep. 2019, Art. no. 100058, doi: 10.1016/j.iot.2019.100058.
[20] B. Shala, U. Trick, A. Lehmann, B. Ghita, and S. Shiaeles, "Blockchain-based trust communities for decentralized M2M application services," in *Advances on P2P, Parallel, Grid, Cloud and Internet Computing (PGCIC)* (Lecture Notes on Data Engineering and Communications Technologies), vol. 24, F. Xhafa, F. Y. Leu, M. Ficco, and C. T. Yang, Eds. Cham, Switzerland: Springer, 2018, doi: 10.1007/978-3-030-02607-3_6.
[21] V. Buterin, "A next generation smart contract & decentralized application platform," Ethereum, Zug, Switzerland, White Paper, 2013. [Online]. Available: https://ethereum.org/en/whitepaper/
[22] G. Wood, "A secure decentralised generalised transaction ledger," Ethereum, Zug, Switzerland, Yellow Paper, 2014. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf
[23] R. Schoenen, H. Yanikomeroglu, and B. Walke, "User in the loop: Mobility aware users substantially boost spectral efficiency of cellular OFDMA systems," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 488–490, May 2011, doi: 10.1109/LCOMM.2011.042511.102057.
[24] R. Schoenen and H. Yanikomeroglu, "Economics of user-in-the-loop demand control with differentiated QoS in cellular networks," in *Proc. IEEE 23rd Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2012, pp. 1131–1136, doi: 10.1109/PIMRC.2012.6362516.
[25] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019, doi: 10.1109/JIOT.2018.2836144.
[26] J. Gattermayer and P. Tvrdik, "Blockchain-based multi-level scoring system for P2P clusters," in *Proc. 46th Int. Conf. Parallel Process. Workshops (ICPPW)*, Bristol, U.K., Aug. 2017, pp. 301–308, doi: 10.1109/ICPPW.2017.50.
[27] F. Kandah, B. Huber, A. Skjellum, and A. Altarawneh, "A blockchain-based trust management approach for connected autonomous vehicles in smart cities," in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Las Vegas, NV, USA, Jan. 2019, pp. 544–549, doi: 10.1109/CCWC.2019.8666505.
[28] V. Strobel and M. Dorigo, "Blockchain technology for robot swarms: A shared knowledge and reputation management system for collective estimation," Institut de Recherches Interdisciplinaires et de Developpements en Intelligence Articielle, Univ. Libre de Bruxelles, Brussels, Belgium, Tech. Rep. TR/IRIDIA/2018-009, May 2018.
[29] Y. Alowayed, M. Canini, P. Marcos, M. Chiesa, and M. Barcellos, "Picking a partner: A fair blockchain based scoring protocol for autonomous systems," in *Proc. ACM Appl. Netw. Res. Workshop (ANRW)*. New York, NY, USA: Association for Computing Machinery, 2018, pp. 33–39, doi: 10.1145/3232755.3232785.
[30] S. Goka and H. Shigeno, "Distributed management system for trust and reward in mobile ad hoc networks," in *Proc. 15th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, Jan. 2018, pp. 1–6, doi: 10.1109/CCNC.2018.8319278.
[31] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.
[32] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019, doi: 10.1109/JIOT.2019.2920987.
[33] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," *IEEE Access*, vol. 7, pp. 147782–147795, 2019, doi: 10.1109/ACCESS.2019.2946373.
[34] F. Tang, S. Ma, Y. Xiang, and C. Lin, "An efficient authentication scheme for blockchain-based electronic health records," *IEEE Access*, vol. 7, pp. 41678–41689, 2019, doi: 10.1109/ACCESS.2019.2904300.
[35] A. Aderibole, A. Aljarwan, M. H. U. Rehman, H. H. Zeineldin, T. Mezher, K. Salah, E. Damiani, and D. Svetinovic, "Blockchain technology for smart grids: Decentralized NIST conceptual model," *IEEE Access*, vol. 8, pp. 43177–43190, 2020, doi: 10.1109/ACCESS.2020.2977149.
[36] A. S. Musleh, G. Yao, and S. M. Muyeen, "Blockchain applications in smart grid–review and frameworks," *IEEE Access*, vol. 7, pp. 86746–86757, 2019, doi: 10.1109/ACCESS.2019.2920682.
[37] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019, doi: 10.1109/ACCESS.2018.2890507.
[38] Y. He, H. Li, X. Cheng, Y. Liu, C. Yang, and L. Sun, "A blockchain based truthful incentive mechanism for distributed P2P applications," *IEEE Access*, vol. 6, pp. 27324–27335, 2018, doi: 10.1109/ACCESS.2018.2821705.
[39] H. Tan and I. Chung, "Secure authentication and key management with blockchain in VANETs," *IEEE Access*, vol. 8, pp. 2482–2498, 2020, doi: 10.1109/ACCESS.2019.2962387.
[40] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in VANETs," *IEEE Access*, vol. 7, pp. 117716–117726, 2019, doi: 10.1109/ACCESS.2019.2936575.
[41] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards data assurance and resilience in IoT using blockchain," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Baltimore, MD, USA, Oct. 2017, pp. 261–266, doi: 10.1109/MILCOM.2017.8170858.
[42] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Honolulu, HI, USA, Jun. 2017, pp. 468–475, doi: 10.1109/ICWS.2017.54.
[43] H. Wang and J. Zhang, "Blockchain based data integrity verification for large-scale IoT data," *IEEE Access*, vol. 7, pp. 164996–165006, 2019, doi: 10.1109/ACCESS.2019.2952635.
[44] I. Riabi, H. K. B. Ayed, and L. A. Saidane, "A survey on blockchain based access control for Internet of Things," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Tangier, Morocco, Jun. 2019, pp. 502–507, doi: 10.1109/IWCMC.2019.8766453.
[45] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019, doi: 10.1109/ACCESS.2019.2905846.
[46] H. Liu, D. Han, and D. Li, "Fabric-IoT: A blockchain-based access control system in IoT," *IEEE Access*, vol. 8, pp. 18207–18218, 2020, doi: 10.1109/ACCESS.2020.2968492.

[47] T. Alladi, V. Chamola, R. M. Parizi, and K.-K. R. Choo, "Blockchain applications for industry 4.0 and industrial IoT: A review," *IEEE Access*, vol. 7, pp. 176935–176951, 2019, doi: 10.1109/ACCESS.2019.2956748.
[48] T. M. Fernandez-Carames and P. Fraga-Lamas, "A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories," *IEEE Access*, vol. 7, pp. 45201–45218, 2019, doi: 10.1109/ACCESS.2019.2908780.
[49] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, "A scalable blockchain framework for secure transactions in IoT," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4650–4659, Jun. 2019, doi: 10.1109/JIOT.2018.2874095.
[50] S. Biswas, K. Sharif, F. Li, S. Maharjan, S. P. Mohanty, and Y. Wang, "PoBT: A lightweight consensus algorithm for scalable IoT business blockchain," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 2343–2355, Mar. 2020, doi: 10.1109/JIOT.2019.2958077.
[51] U. Majeed and C. S. Hong, "FLchain: Federated learning via MEC-enabled blockchain network," in *Proc. 20th Asia–Pacific Netw. Oper. Manage. Symp. (APNOMS)*, Matsue, Japan, Sep. 2019, pp. 1–4, doi: 10.23919/APNOMS.2019.8892848.
[52] I. Bashir, *Mastering Blockchain*. Birmingham, U.K.: Packt, 2018.
[53] S. Nakahira, S. Nakamura, T. Enokido, and M. Takizawa, "Trustworthiness in peer-to-peer systems," in *Proc. 18th Int. Conf. Netw.-Based Inf. Syst.*, Taipei, Taiwan, Sep. 2015, pp. 652–657, doi: 10.1109/NBiS.2015.97.
[54] Y. Ma and D. Wang, "A novel trust model for P2P networks," in *Proc. 12th Int. Conf. Natural Comput., Fuzzy Syst. Knowl. Discovery (ICNC-FSKD)*, Changsha, China, Aug. 2016, pp. 1969–1973, doi: 10.1109/FSKD.2016.7603482.
[55] *Security Requirements and Mechanisms of Peer-to-Peer-Based Telecommunication Networks*, document ITU-T X.1163, 2015.
[56] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, and Y. Zhang, "A blockchain-based nonrepudiation network computing service scheme for industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3632–3641, Jun. 2019, doi: 10.1109/TII.2019.2897133.
[57] Z. Zheng, S. Xie, H. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," *Future Gener. Comput. Syst.*, vol. 105, pp. 475–491, 2020, doi: 10.1016/j.future.2019.12.019.
[58] Y. Xu, G. Wang, J. Yang, J. Ren, Y. Zhang, and C. Zhang, "Towards secure network computing services for lightweight clients using blockchain," *Wireless Commun. Mobile Comput.*, pp. 1–12, 2018, doi: 10.1155/2018/2051693.

BESFORT SHALA received the B.Sc. and M.Sc. degrees in telecommunications from the Faculty of Electrical and Computer Engineering, University of Prishtina, Kosovo, in 2011 and 2015, respectively. He is currently pursuing the Ph.D. degree with the Centre for Security, Communications and Network Research, University of Plymouth, U.K. Since 2016, he has been a Research Associate with the Frankfurt University of Applied Sciences, Germany. His research interests include the broad area of M2M, the IoT, security, trust, and blockchain.



ULRICH TRICK received the Dipl.Ing. degree in electrical engineering-telecommunications and the Ph.D. degree from the University of Kaiserslautern, Germany, in 1983 and 1987, respectively. Since 2001, he has been a Professor of telecommunication networks with the Department for Computer Science and Engineering, Frankfurt University of Applied Sciences, Germany. His research interests include future networks, M2M, the IoT, WMN, virtualization, and 5G.

ARMIN LEHMANN received the Dipl.Ing. degree in information and communications technology from the Frankfurt University of Applied Sciences, Germany, in 2005, and the Ph.D. degree from Plymouth University, U.K., in 2014. Since 2016, he has been a Deputy Professor of programming in information technology at the Frankfurt University of Applied Sciences. His research interests include 5G, NFV, M2M, and the IoT.

BOGDAN GHITA received the Ph.D. degree from the University of Plymouth, U.K., in 2005. He is currently an Associate Professor with the University of Plymouth and leads the networking area within the Centre for Security, Communications, and Network research. His research interests include computer networking and security, with a focus on network security, performance modeling and optimization, and wireless/mobile networking. He has published over 150 articles, has graduated 20 Ph.D. students, and has been a principal investigator in a number of industry-led, national, and EU research projects in these areas. He was a TPC member for over 100 international conference events and a Reviewer of the IEEE Communications Letters, *Computer Communications*, and *Future Generation Computer Systems* journals.

STAVROS SHIAELES (Member, IEEE) received the B.Eng./M.Eng. degree in electrical and computer engineering and the Ph.D. degree in cybersecurity from the Democritus University of Thrace, Greece, in 2007 and 2013, respectively. He is currently a Senior Lecturer with the School of Computing and a member of the Cyber Security Research Group, University of Portsmouth. He holds an EC-Council Certified Ethical Hacker (CEH) Certificate, an EC-Council Advance Penetration Testing (CAST611) Certificate, an ISACA Cobit 5 Foundation Certificate, and a Cyberoam Certified Network and Security Professional (CCNSP) Certificate. He is an EC-Council Accredited Instructor and delivers training to professionals in U.K. and EU on cybersecurity. He has published more than 30 articles in international scientific journals, conferences, and books and has participated in EU-funded and national research and development projects. His research interests span the broad areas of cybersecurity, open-source intelligence, trust, blockchain, digital forensics, and machine learning applied in cybersecurity context. He is actively involved with professional bodies in U.K., Greece, and Cyprus and a Fellow of BCS and the Higher Education Academy. He has been a TPC member and a regular reviewer for a number of international journals and conferences.