electronics

Article

Blockchain-Based Trust and Reputation Management in SIoT

Sana Alam [1,2,*], Shehnila Zardari [3] and Jawwad Ahmed Shamsi [4]

[1] Department of Computer Science & Information Technology, NEDUET, Karachi 75270, Pakistan
[2] Department of Computer Engineering, SSUET, Karachi 75300, Pakistan
[3] Department of Software Engineering, NEDUET, Karachi 75270, Pakistan
[4] Department of Computer Science, FAST-National University of Computer and Emerging Sciences (NUCES), Karachi 75270, Pakistan
* Correspondence: sana.email43@gmail.com

Abstract: In the Social Internet of Things (SIoT), trust refers to the decision-making process used by the trustor (Service Requesters (SRs) or Service Consumers (SCs)) to decide whether or not to entrust the trustee (Service Providers (SPs)) with specific services. Trust is the key factor in SIoT domain. The designing of a two-way, two-stage parameterized feedback-based, service-driven, attacks-resistant trust and reputation system for SIoT accompanied by a penalty mechanism for dishonest SPs and SRs is our main contribution that mitigates the trust-related issues occurring during service provisioning and service acquisition amongst various entities (SPs or SRs) and enhances trust amongst them. Our proposed methodology examines a SP's local trust, global trust, and reputation by taking into account "Social Trust" and "Quality of Service (QoS)" factors". Two—Stage Parameterized feedback" is incorporated in our proposed strategy to better manage "intention" and "ability" of SRs and provides early identification of suspicious SRs. This feature compels SRs to act honestly and rate the corresponding SPs in a more accurate way. Our recommended paradigm sorts SPs into three SP status lists (White List, Grey List, and Black List) based on reputation values where each list has a threshold with respect to the maximum service fee that can be charged. SPs in White List charge the most per service. SPs in other lists have a lower selection probability. Every feedback updates the SP's trust and reputation value. Sorting SPs increases resistance against On Off Attack, Discriminatory Attack, Opportunistic Service Attack, and Selective Behavior Attacks. SPs must operate honestly and offer the complete scope of stated services since their reputation value relies on all their global trust values (Tglobal) for various services. Service requests may be accepted or denied by SPs. "Temporarily banned" SRs can only request unblocked services. SRs lose all privileges once on a "permanently banned" list. If local and global trust values differ by more than the threshold, the SR is banned. Our method also provides resistance against Bad Mouthing Attack, Ballot Stuffing Attack. Good Mouthing Attack/Self—Propagating Attack. Experiments indicate our trust and reputation management system recognizes and bans fraudulent SRs. "Dishonest SPs" are "blacklisted," which affects their reputation, trust, and service charges.

Keywords: trust; reputation; parameterized feedback; service-based; SIoT; blockchain; penalty

check for updates

Citation: Alam, S.; Zardari, S.; Shamsi, J.A. Blockchain-Based Trust and Reputation Management in SIoT. *Electronics* **2022**, *11*, 3871. https://doi.org/10.3390/electronics11233871

Academic Editor: Andrei Kelarev

Received: 3 October 2022
Accepted: 10 November 2022
Published: 23 November 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The Internet of Things (IoT), is a relatively new concept that refers to the ability of various electronic devices and sensors to interact with one another and improve our quality of life by exchanging data via the internet. The IoT makes use of internet-connected smart gadgets in order to come up with innovative solutions to a wide variety of problems and concerns that are affecting various economic, governmental, and public/private sectors all over the world. [1]. By gathering and processing copious amounts of data, IoT can assist in enhancing various processes so that they are more quantifiable and observable [2]. IoT has the potential to improve the quality of life in a variety of contexts, including healthcare, smart cities, the building sector, agriculture, water management, and the energy sector [2].

In this way, the IoT may be seen as a network whose primary goal is to include requestors' and providers' nodes that can make service requests and offers services. In addition, several nodes may work together to provide a unified service [3]. Many new ideas and contexts, such as "Social IoT" (SIoT), "Industrial IoT," and "IoT in the Healthcare Domain," have emerged as a direct consequence of the exponential growth of the IoT paradigm since its conception.

Due to IoT, heterogeneous devices may share data and work together to provide and receive services. However, trust issues between devices might arise from such cooperative engagement, calling for a decentralized, mobile, low-cost, low-latency, lightweight, and scalable trust management system. SIoT is the realization of "social networks" and the "internet of things [4]," defined by the heterogeneity of the software and hardware components and the range of hardware designs. Devices from different categories work together in SIoT to accomplish a shared goal [5]. Connectivity between "people", between "things," or between "people and things" are all included in the definition of "SIoT" [6]. SIoT allows for the fast discovery of geographically scattered heterogeneous items [7].

P2P networks and social ties between different systems that are autonomous are both parts of the SIoT. In these networks, nodes may give services as service providers (SPs) or seek and receive services as consumers or requesters (SRs or SCs). When objects or nodes in a network collaborate, they get more accurate results to their queries than would be possible if they worked alone [8,9]. Self-organization of things, via the sharing of computing resources, information, and services, is central to the concept of SIoT, which aims to decouple them from human control. Objects must choose their own relationship types with one another [9].

Depending on the context, a SIoT system may support either user-to-thing or thing-to-thing relationships. Inter-SIoT interaction and the application area are greatly impacted by relationship kinds [10]. Things develop relationships with one another after realizing they have a capacity for social interaction. Social connections between objects may be built using criteria such as entity or node specifications, activity patterns, installed applications, services provided, etc. [11,12]. In the SIoT, many types of social ties exist.

- The parent-object relationship [4,12] describes a connection between two products or nodes that come from the same manufacturer. The nodes that come from the same manufacturer tend to be rather similar.
- Co-location is a connection between things that share the same physical place [4,12]. Depending on their dimensions, objects might be in the same workplace or in the same city.
- Objects have a co-work connection when they work together toward a single purpose or application [4,12]. Both similar and dissimilar entities may be linked together.
- Ownership object relationship is Inherent among things with the same owner as a connection based on ownership. There's no need for similar entities [4].
- When two or more nodes come into touch with one another, whether on a regular or sporadic basis, for reasons that are wholly attributable to the connections between their owners, a social object relationship is formed [4,12]. It often emerges at the intersection of seemingly unrelated entities.

The "service-based" is an important concept and one of the building blocks of "social relationships" in SIoT. All the social networks/ social websites/ social apps revolve around the services they provide. One social network or social app serving as the service provider (SP) is regarded as worthy for one type of service but is rated below average for other types of services. Thus, service requesters or service consumers (SRs or SCs) tend to have "service-related trust". Therefore, to design a trust and reputation management framework in the SIoT domain special consideration must be given to the service-related trust. Hence, our suggested models give prime focus on the "service-based" concept for the trust and reputation management framework.

The idea of "Trust" has many applications outside of the IoT and SIoT, including the fields of psychology, economics, organizational management, sociology, networking,

and computing, to name just a few. Trust is viewed as an interdisciplinary quality whose definition varies depending on the context in which it is used [13,14]. In SIoT, trust is the process by which the trustor (SRs or SCs) determines whether or not to entrust the trustee (SPs) with certain responsibilities and how to best leverage the trustee's efforts to achieve the trustor's objectives. The trustor's confidence in the trustee's ability and willingness to carry out their duties is a key factor. Trustworthiness judgments are made by both the trustor and the trustee. Uncertainty in the environment, the consequences of actions, and the requirements of the task at hand all contribute to analyzing trustworthiness.

Much attention has recently been paid to the blockchain, both in academic circles and the business world. Distributing digital data is made possible by blockchain technology. As data is not kept in one central repository, it is simple to confirm all of the data. Blockchain technology is secure and reliable because it is not centralized and has no single point of failure.

The decentralized, shared, and immutable blockchain [15] can lead to a whole wave of SIoT security advancements in general and more specifically in the trust management sector. The blockchain is a distributed ledger [16] consisting of a sequence of blocks that, in the same way as a conventional public ledger would provide an entire list of transaction data [17]. The blockchain was first introduced for Bitcoin [18]. The breakthrough advancement in economic computing, known as Bitcoin, enables users to trade money online quickly, reliably, and at a minimal cost [18]. If we take the example of two parties wishing to trade digital currency, it is necessary for them to initiate a transaction before they may do so. As with other initiated transactions, it is bundled into a block. The chain of computers then incorporates the additional block into the resulting network. Network nodes (also known as "miners") use complex mathematical procedures to determine the legitimacy of a transaction's request for confirmation. This indicates that at least 51% of the computers engaged in the transaction have verified its correctness. Each block of legitimate transactions must be given a cryptographic hash, which includes a reference to the prior block in the chain. A record chain created using this method is incredibly difficult to forge. After the exchange of value has taken place, the transaction is finalized and declared successful [19].

Another Distributed Ledger Technology (DLT) is Tangle. Tangle can store transactions in the form of a directed acyclic graph. Two other transactions must be approved before a new one can be added to the Tangle. Unauthorized transactions are known as "tips." It is possible to implement a strategy that will randomly select tips from the pool of those tips that are available. "Genesis" refers to the very first transaction. Tangle is simple enough for everyday use. Microtransactions are feasible now because of how flexible this system is, making almost any kind of transaction low-cost and instantaneous. Tangle can be used for money transfers between bank accounts. In this way, time is not wasted during costly transfers. Since Tangle enables transactions between machines, it has close ties to the IoT sector. Several divergences can cause issues because it is unrealistic to share all transactions at once. The IOTA Reference Implementation (IRI) is the foundation upon which Tangle operates; it is a Java-based application that establishes connections between the Node's user and their immediate network peers. Decentralization is facilitated through the operation of a Node within the Tangle, and no third-party node is required to gain access to the ledger [19].

In an effort to enhance the efficiency and dependability of blockchain systems, the Linux Foundation launched the Hyperledger project in December 2015 as an open-source alternative. The Hyperledger project, which aims to facilitate blockchain development, currently hosts five distinct frameworks: (i) Burrow, (ii) Fabric, (iii) Indy, (iv) Iroha, (v) Sawtooth. (i) Burrow: As a multi-chain universe, Burrow is pre-defined by its applications. (ii) Fabric: In order to build a secure, permissioned blockchain environment, developers can use Hyperledger Fabric, which runs on the Linux operating system. (iii) Indy: Identification and identity verification are requirements for joining or taking part in any organization or institute. The distributed ledger allows each institution to simply share a common identity

by keeping a digital identity. With this philosophy, Hyperledger Indy was created. (iv) Iroha: The code for the IROHA project was made available for download by Soramitsu, a Fintech startup in Japan. The Linux Foundation hosted this project as part of the Hyperledger initiative. IROHA and other blockchains are distinguished primarily by the fact that each member is not permitted to preserve the entire data history in IROHA. Only users who have been authenticated and given authorization can query the data. (v) Sawtooth: The Hyperledger Sawtooth architecture is a distributed ledger or blockchain that aims to establish a business firm by placing all relevant parties on the blockchain and keeping track of them [20].

A distributed ledger platform for storing and managing financial agreements is called Corda. It is tailored for use with financial organizations [20].

Ethereum is a decentralized open-source platform for decentralized networks that supports blockchain technology [21]. Beyond the original cryptocurrency, it expanded the uses of blockchain technology [22]. On Ethereum, programmers can create smart contracts—codes that manage digital money (ether)—and execute smart contracts. "Smart contract" is a unique account that stores information and computer code that may perform a variety of predefined tasks [23]. There is a need for many organizations to use blockchain capabilities, such as timestamping and tamper-proofing, for which the private blockchain is frequently required because transactions need typically to be kept private. Both public and private blockchains can use Ethereum. The vast majority of voluntary nodes run the public Ethereum network, and miners are responsible for creating blocks. As a result, they reach a consensus via a system called Proof-of-Work (PoW), which is comparable to Bitcoin. Another consensus mechanism created for the public Ethereum network is called Proof-of-Stake (PoS), which enables miners with more cryptocurrency to mine blocks more quickly as compared to those with less cryptocurrency. Private Ethereum is made to enable a small number of users to access a shared blockchain [21].

Our proposed trust and reputation management system can play a vital role in IoT-based social applications seeking to help users by providing cooperative solutions to improve their lifestyle, healthcare, and economic problems. In fact, societal applications like analyzing air and water quality, reducing energy use, utilizing electric vehicles for smart transportation, promoting shared mobility, and locating COVID-19 patients have drawn a number of researchers to create new technologies using cutting-edge technologies like IoT cloud/edge computing. Additionally, policymakers and businesses have encouraged researchers and product creators to provide socio-economic solutions through the use of more recent technology, such as blockchain [24]. In all the above-mentioned applications trust management is the key issue. Hence, our trust and reputation management system provides a basis for resolving trust-related issues pertaining to the SRs and SPs.

One of the most helpful uses of blockchain is the ability to track goods along the whole supply chain and food industries. The benefits of blockchain technology have drawn researchers to explore how it may be applied in the supply chain. This technology can improve the supply chain, manage and monitor risk mitigation measures, and even help avoid security breaches [18]. Therefore, our proposed trust and reputation management system provides benefits to mitigate trust-related issues in the supply chains also.

In this light, and with respect to the various advantages offered by the blockchain we use blockchain as the backbone of our proposed trust and reputation management framework. We have used Ethereum blockchain as it offers both public and private blockchains. Moreover, Ethereum's adaptable and flexible features make it possible to create any kind of blockchain application, which is a major benefit [23]. The smart contracts that serve as the key elements of blockchain [25,26] are designed to provide various features of our trust and reputation management framework deployed in the private Ethereum blockchain.

In a nutshell, our contributions to the proposed trust and reputation management system in SIoT domain are listed as follows:

(i) The entities (SRs or SPs) communicate with each other to acquire or provide services. Once SRs acquire the desired service, the next step is to rate the SPs accordingly in the

form of feedback. However, the feedback rating of SPs based on a single cumulative value has drawbacks. Firstly, such feedback does not justify the criteria on which SP is rated. Secondly, SRs that are "ill-intended" or "dishonest" can deliberately provide a poor rating as feedback to the SP despite SP providing a good service. Thirdly, "amateur" SRs lack the correct decision-making ability with respect to giving feedback to the corresponding SP. In view of the above issues, we introduce the concept of using "two-stage parameterized feedback". Firstly, it enhances the "ability" of SRs to be in a better judgment position about the service they acquire. It provides ease of judgment to the amateur SRs or even opens new "dimensions of criteria" for the experienced SRs to correctly rate the SP based on the service they (SRs) have acquired. Second, those SRs who are more interested in eventually becoming SPs for the same service might improve the service they are going to offer in the future from the perspectives of "Social Trust" and "Quality of Service (QoS)" factors. This also leads to a good analysis of the "intention" aspect of SRs. The "two-stage parameterized feedback" acts as a first step in the identification of the suspicious SRs since based on the "two-stage parameterized feedback", the Local Trust Values (Tlocal) are calculated. The input to "two-stage parameterized feedback" is taken in two stages "pre-service avail" and "post-service avail". These "pre-service avail" and "post-service avail" lead to the calculation of Tlocal. The "pre-service avail" value aids in determining the "intention" of SRs because SRs assess several parameters according to their perceived relevance in relation to the service they are about to acquire. The "post-service avail" value forces SRs to rate the parameters correctly in accordance with the service being supplied by the associated SPs after they have acquired the service. This Tlocal leads to the calculation of the Global Trust Values (Tglobal). Tlocal and Tglobal values' differences aid in the detection of "suspicious" or "dishonest" SRs. A particular dishonest SR is first added to the "Suspicious List" and then, depending on the criteria, is added to the "Banned List" if there is any noticeable difference (based on the criteria) in the values of Tlocal and Tglobal (where Tlocal values are based on the "two-stage parameterized feedback" provided by that SR and Tglobal values are calculated from the Tlocal values) for a specific service with respect to a specific SP.

(ii) The trust and reputation management models that are suggested so far in the SIoT domain evaluate SPs' trustworthiness values but consider SRs as trustworthy entities. Hence, these trust and reputation models paved the concept of "blind trust" in SRs. To overcome this drawback, we have proposed "two-way trust and reputation management" by providing a mechanism to track the performance of SPs as well as SRs. This proposed model signifies the fact that the "breach of trust" and "concept of malevolent entities" is not only limited to the SPs but also encompass SRs. Our model negates the theory of "blind trust" on SRs by keeping a continuous watch on SRs as well. The check and balance phenomena on a regular basis led to the incorporation of a "regular check and penalty mechanism" for SRs besides SPs in our suggested framework.

(iii) Our model focuses on the "service-based" criteria for the deployment of a trust and reputation management framework. The "service-based" concept is the key factor of "social relationships" in SIoT. SPs (any social networks or social apps) are regarded as reliable for certain types of services, but not for other types of services that they provide. Therefore, the trust and reputation evaluation of SPs should be "service-based" or "service-specific". Also, because of this contribution, SRs can acquire services from one SP that has a high-quality rating in a given area and acquire services from another SP that has a higher-quality rating in a different area.

(iv) So far, the "idea of fee charge" has been overlooked in the trust and reputation management system. It's crucial to understand this idea as SPs mostly offer their services because they can make money from doing so. Therefore, our suggested trust and reputation management system includes this idea to ensure that SPs are providing services in an ethical manner. In addition, the "regular check and penalty

mechanism" that we propose uses the "fee charge concept" that causes monetary loss to the dishonest SP, thus forcing the SPs to act in an honest way.

(v) The "regular check and penalty mechanism for SPs" provides a check and balance system for SPs. SPs are sorted into various SP status lists reflecting their reputation values based on the services they provide. Each list has a maximum threshold for the "fee charge". The SPs belonging to a specific list can only charge up to the maximum allowable value for that particular list. These lists are categorized as "White List, Grey List, and Black List" based on the criteria discussed further in the paper. SPs in the "White List" have the privilege to charge the most for a certain service. Moreover, SPs on "Grey List" and "Black List" have fewer chances to be selected for providing services.

(vi) To restrict SRs to act in an honest way, the "regular check and penalty mechanism for SRs" is implemented that causes the malevolent SRs to be sorted into the "Suspicious List"", "Temporarily Banned", and "Permanently Banned" lists as per criteria further discussed in our paper. The distinguishing feature between the "Temporarily Banned" and "Permanently Banned" is that the former allows the SR to place requests for services for which that particular SR is not banned whereas the latter imposes a ban on SR from requesting any kind of service. Thus, if an SR is Permanently Banned then that SR is prohibited from requesting all services whereas Temporarily Banned SRs can request other services for which they are not banned.

(vii) Our suggested mechanism for managing trust and reputation gives SP the option of accepting or declining the service request. In addition, our approach to managing trust and reputation helps SR choose SPs that best suit their needs. To elaborate, if an SR is concerned with keeping costs down, they may select an SP from the "Grey List" rather than the "White List".

(viii) Our proposed strategy causes the reputation value to be based on all the service-specific global trust values of SPs. As a result, it forces SPs to provide all services honestly rather than offering some services in an honest way and others in a dishonest way.

(ix) The "regular check and penalty mechanism" incorporated in our strategy provides resistance against various trust-specific attacks in SIoT domain such as Ballot Stuffing Attack (BSA), Bad Mouthing Attack (BMA), Self-Propagating Attack/Good Mouthing Attack (SPA/GMA), Opportunistic Service Attack (OSA), Discriminatory Attack (DA), Selective Behavior Attack (SBA), and On Off Attack (OOA).

2. Literature Review

Trust is one of the key factors whenever there is communication between entities (SRs or SPs) in SIoT domain. Hence, the development of the trust management framework is given prime importance in SIoT domain.

A significant amount of work has been done using blockchain for the trust management framework in IoT but the incorporation of blockchain for the trust management aspect of SIoT requires attention. Table 1 presents the prominent studies that use technologies other than blockchain for the designing of trust management strategies in SIoT domain whereas Table 2 presents the studies which have based their proposed trust management models on blockchain technology. A recent comprehensive survey [14] is provided by the authors on the trust management aspect of SIoT. This survey [14] represents that only 3 studies use blockchain for implementing the trust management framework in SIoT. Moreover, authors of the scholarly work [14] also identify blockchain as the future direction for the designing of trust and reputation management framework. Hence, blockchain is the emerging paradigm with respect to the trust and reputation management aspect in SIoT domain.

Table 1. Prominent studies using technologies other than the blockchain to design trust management models in SIoT.

Ref.	Summary of the Insights for Prominent Studies Using Technologies Other than the Blockchain to Design Trust Management Models in SIoT
[27]	A framework for managing trust is presented with regard to node behavior during the launch of BMA. A Bayes Model along with the Weighted Sum are used to calculate expected and estimated trust, whereas overall trust is the result of the two. The trust calculation makes use of prior and anticipated behavior to combat malicious attacks.
[28]	A trust model based on the adaptive method is provided to enhance security against malevolent nodes. Node configuration that changes dynamically provides resistance against destructive attacks. The stability of the network is sacrificed for trust.
[29]	Offers a paradigm for trust focused on knowledge and reputation (according to the object and its ownership). This study explores trust between humans and between humans and things. Knowledge regarding people-to-people is based on the community of interest, cooperation, honesty, and experience, whereas human-to-object knowledge is based on entities and services.
[30]	REK is proposed. Reputation and experience are used for calculating trust. Experience is calculated using interaction frequency, whether an interaction is cooperative, uncooperative, or neutral, and relationship status. Based on these variables, experience grows, shrinks, or decays. The authors draw the conclusion that while trust is challenging to build, it deteriorates more quickly. For reputation, the model uses Google Page Rank. The methodology for evaluating trust makes use of human cognition.
[31]	A trust system focused on credit and reputation was put forward. Credit establishes a node's ability to communicate, whereas reputation determines a node's reliability and identifies malicious nodes. Penalties are provided in this architecture for identifying and restricting hostile nodes.
[32]	Presents a hybrid Trust and reputation architecture for SIoT (TRM-SIoT). According to the research work, social contacts establish reputation whereas personal interactions determine trust. Malicious activity includes offering and recommending fraudulent services. Two trust values are computed provided that SP's and SC's communication regarding a service exceeds a threshold. One reveals long-term contentment, while the other highlights current patterns.
[33]	A trust model exhibiting subjective characteristics is suggested. The ability to manage trust is crucial, as are benevolence and integrity. Ability tests the trustee's (SP's) capability for a work, Benevolence gauges the trustee's cooperation, and Integrity gauges the trustee's reputation. A modified, weighted page-rank algorithm is suggested in the literature to assess the reputation. Utilizing mobile crowd-sensing (MCS), the trust model is assessed.
[34]	Compares page rank to the recommendation methodology. Graphs that are weighted and directed display object relationships. An object's outbound links serve as an indicator of its quality relationships. PR rankings are based on external connections. The most trustworthy items in this model are given rank values, while the others are given zero.
[35]	The architecture described consists of objects with various capabilities, a server in charge of user compatibility and authentication for each "thing," and a trust management system that evaluates trust values and performs trust calculations based on feedback and context.
[36]	Unreliable nodes are promptly identified and isolated using the suggested trust management technique. The method prevents object-oriented attacks.
[37]	ML (Machine Learning) algorithm-based trust management approach is proposed. This research finds attacks connected to trust and separates malicious nodes.
[38]	A model for the administration of both direct and indirect trust is put forward. In this study, a "DTrustInfer" technique is presented, where the authenticator is the node having the highest centrality score. In order to verify node messages, the authenticator creates and transmits secret codes.
[39]	Uses homomorphic encryption to safeguard an object's privacy. A self-enforcing privacy-preserving method is presented in this paper. The study assesses the trustworthiness of the owner and the object. Participant privacy is protected via trust assessment. Feedback from various entities should be weighted and kept confidential. Object ratings are shown on the bulletin board
[40]	Provides a framework for managing trust based on discriminating SIoT node behavior. To assign trust providers to the entities, the study uses DHT (distributed hash table). For the indices they cover, trust providers store entity trust values
[41]	To identify reliable nodes, the study uses a bipartite network, matrix factorization, and Hellinger distance. According to SC and SP, SIoT is depicted as a bipartite graph. Between SRs and SPs, a social structure is created by the Hellinger distance. Matrix factorization is used to find reliable SP.
[42]	The research uses trustor-suggester similarity to establish trust in SIoT devices on the basis of a user's interest preference.
[43]	The study puts forward the centralized and decentralized models of trust. Pre-trusted objects use a distributed hash table in the centralized approach to facilitate SP's trust queries. The proposed paradigm isolates malicious nodes at the expense of an increase in network traffic brought on by feedback exchange.

Table 1. *Cont.*

Ref.	Summary of the Insights for Prominent Studies Using Technologies Other than the Blockchain to Design Trust Management Models in SIoT
[44]	According to the study, SP trust should be based on sociability, intimacy, service evaluations, and transaction value. A trust predictability model for OOA is suggested in this paper and is based on a node's previous actions.
[45]	Proposes a trust model that employs ML (Machine Learning) and DL (Deep Learning) to provide resistance against attacks. According to this study, users can be classified as genuine, maliciously endorsing, or maliciously delivering services.
[46]	Suggests a strategy for managing subjective trust based on direct and indirect interaction. Consideration of friends' perspectives and experiences is indirect engagement.
[47]	In order to assess and forecast trust levels, the study provides a "community of interest" trust management technique. The basis for node communication is shared interests. The suggested method includes member updates, administrator election, trust value initialization, and community creation.
[48]	According to the paradigm put forward, a time-driven approach is employed for trust updates while an artificial neural network technique is used for trust aggregation.
[49]	Using K-means clustering, a trust aggregation technique is suggested to differentiate between trustworthy and untrustworthy interactions. A trust prediction system is utilized to comprehend how specific features affect the total trust score.
[50]	Focused on the similarity factor existing amongst various nodes in terms of friendship, co-work, and community of interest, the study proposes a trust model. Direct trust and indirect trust are combined in the suggested trust paradigm. When there isn't any direct prior experience, recommendations are taken into consideration
[51]	Soft set theory was used to propose a weighted trust scheme.
[52]	Considering the friendliness factor, the work introduces the F-TRM, a trust and relationship management method for dependable service supply in SIoT. This study suggests employing an updated friendship directory (UFD) along with a dynamic friendship supervision technique (DFS).
[53]	Uses context to calculate SIoT trust. In order to calculate node-owner trust, social science and psychology are used. Similarity and familiarity are indicators of trust. Similarity trust employs the community of interest and centrality. Recommendations and direct trust are the main factors in familiarity trust. Fuzzy logic and a kernel-based nonlinear multivariate grey prediction model are used to calculate familiarity trust.
[54]	Considering the idea of "fission" computing, the work suggests a trust and privacy method for SIoT. The paper suggests a plan for eliminating the need for centralized servers by developing a scalable and distributed strategy that uses end-user devices as mini-edge servers.
[55]	Deep learning is used in the trust management system for the isolation of compromised nodes and the identification of attacks linked to trust.
[56]	Using a multiplicative attribute graph (MAG) provides a trust management technique for SIoT. Each entity has a relationship with a set of attributes. The connection probability between two nodes represents trust in this research work with the entire trust between various nodes being determined using MAG.
[57]	A cloud-based calculation-based trust management strategy is suggested. In general, direct and indirect trust scores form the foundation of trust.
[58]	An innovative approach to evaluating node trustworthiness and determining the most trustworthy SP is put forth. To speed up the trust calculation process and find the most dependable service provider, SPs are selected based on contextual data from recommendations and QoS.
[59]	The work provides a reliable crowdsourcing strategy in the SIoT field by fusing the concepts of the social cloud and sensing nodes derived from the social awareness process.
[60]	A trust management methodology (ConTrust) focusing on context is presented for choosing a reliable SP and assigning tasks in SIoT. A SIoT trust model is created by combining social networks with trust theory. This paper also offers methods for incorporating resilience against attacks on trust in SIoT.

Table 2. Blockchain-based Trust Management in SIoT.

Ref.	Summary for the Insight into the Studies That Propose Blockchain-Based Trust Management in SIoT
[61]	The study proposes a blockchain-based trust management model. In this research, reputation is calculated using information entropy. The work uses smart contracts to measure trust.
[62]	A trust management strategy using blockchain technology is presented. Limiting the interaction overload leads to the proposal of a simple trust management mechanism. Node privacy-preserving features are discussed. The social connection is calculated using three different methods: ownership-based similarity, owner-friendship-based similarity, and device-based similarity.
[63]	With blockchain technology at its core, proposes a trust management paradigm tailored to SIoT. The research offers a flexible and adaptable trust calculation process, which can be used to improve node dependability in terms of trustworthiness computation. The blockchain is used to store and retrieve information related to trust.

Table 1 reveals that none of the cited research actually uses the two-way trust and reputation management approach. In addition, the "regular check and penalty mechanism" that is a part of our research is missing from the aforementioned studies. Neither of the aforementioned research work incorporates the important idea of a fee charge for service. These studies also lack the concept of "two-stage parameterized feedback," which greatly improves the reliability factor and lays the groundwork for the early detection of malicious SRs. In addition, since the reputation value is derived from global trust values that are unique to each service, it forces SPs to deliver all services in an ethical manner. The proposed trust management paradigm in Table 1 does not account for reputation values of this type. The major drawback of various suggested trust management strategies in Table 1 is the absence of an immutable, tamper-free, and auditable trust management system which is possible through the use of blockchain technology.

However, an analysis of the studies in Table 2, indicates that trust management is not evaluated from the service point of view in these studies. Trust management based on service provisioning is an important aspect as one SP is trusted for one kind of service but not for the other kind of service. The penalty mechanism is also not included in the studies. Feedback is calculated as a whole which is not suitable as parameters need to be mentioned while calculating the feedback to make the feedback more transparent and auditable at the same time the introduction of "two-stage parameterized feedback" in our strategy also enhances SR's ability and leads to the early detection of malevolent SRs. There is no concept of fee charges while providing a service. Moreover, a two-way trust management system to maintain the check and balance for both the SPs and SRs is required to maintain transparency and auditability of the system. However, the aforementioned research studies have not implemented the trust management aspects from the SRs' viewpoint. Reputation value calculation on the basis of all service-specific global trust values for SPs is also not part of the studies presented in Table 2.

Hence, in light of the above literature survey, it can be stated that there is a need for the development of a bidirectional, two-stage parameterized feedback-based, service-driven, attack-resistant trust and reputation system for SIoT, complete with a penalty and constant check mechanism for dishonest SPs and SRs, which together reduce trust-related issues that arise during service provisioning and service acquisition between different entities.

3. Proposed Trust and Reputation Framework

A general representation of our proposed model is shown in Figure 1. The features of our proposed trust and reputation management system are: (i) Two-Stage Parameterized feedback—The values are input in two stages "pre-service avail" and "post-service avail". (ii) Service-Based Trust Value Computation—This leads to the computation of Tlocal values that are based on "Two-Stage Parameterized Feedback" and Tglobal values that are based on the Tlocal values. (iii) Service-Based Reputation Value Calculation—The Reputation Values of SPs are calculated. (iv) SP Status List—Based on the SP reputation values, the SPs are categorized into 3 different Status Lists (White List, Grey List, and Black List). (v) Penalty Mechanism—Our proposed trust and reputation management system incorporates penalty mechanisms for SPs in the form of "Grey List" and "Black List" and for SRs in the form of "Temporarily Banned" and "Permanently Banned" lists. (vi) There is a maximum threshold value of fee for each SP Status List up to which the fee can be charged by SPs presented in the corresponding lists. (vii) SRs can select SPs to acquire a certain service from the list of available SPs for that service. (viii) SRs that are the part of "Permanently Banned" list cannot request any service. However, those SRs that are the part of "Temporarily Banned" list cannot request the service for which they are banned. (ix) Attacks addressed are BMA, BSA, SPA/ GMA, DA, OOA, OSA, and SBA.

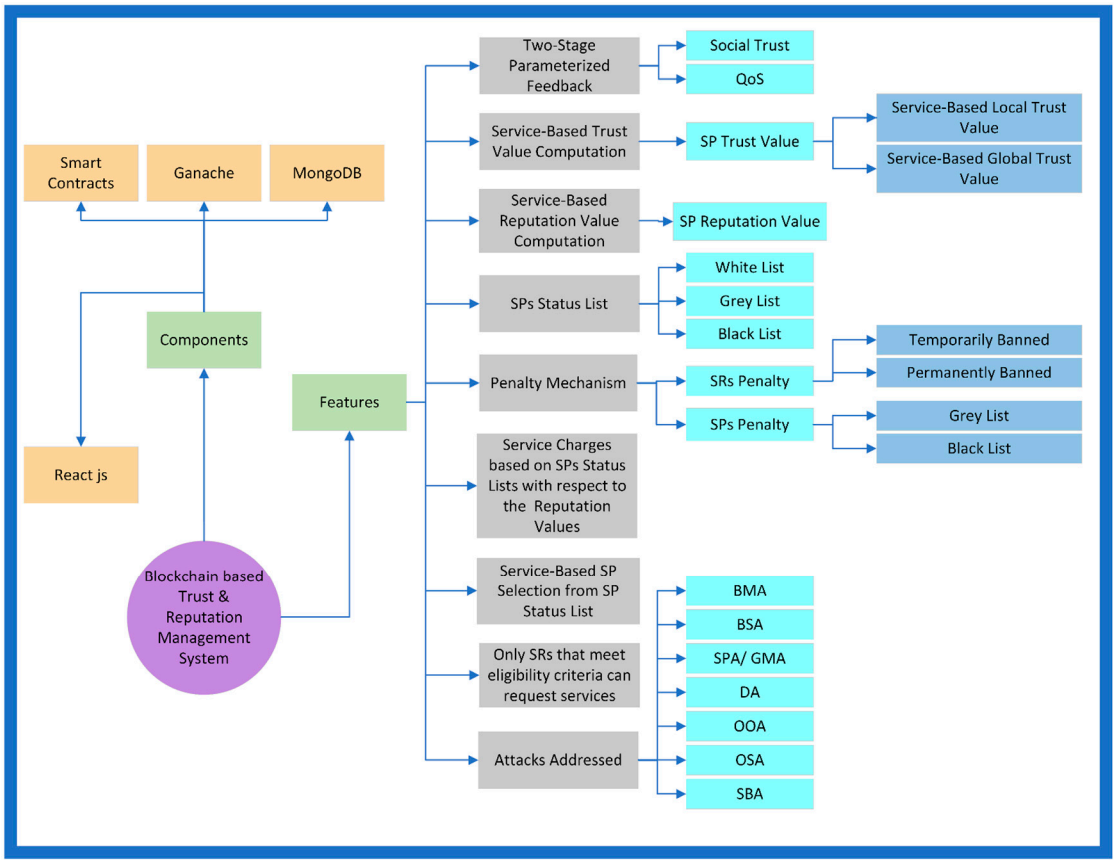

Figure 1. General representation of our Trust and Reputation Management Framework.

The first phase of our trust management is the registration of SP for providing different services. A single SP can provide multiple various services therefore, services corresponding to different SPs are registered. All the SPs are stored in the Registered List in accordance with the services that they provide. Algorithm A1 (please refer to Appendix A) depicts the entire process for the SP registry. Whenever the SP intends to register itself for providing service or services, the account is first checked for any previous registration. If the SP is already registered, then the concerned SP is informed accordingly. However, the new SPs register themselves with any number of services they are able to provide. The new SPs are automatically placed in the "BLACKLIST" "Black List" with a default reputation value of 0.2. The minimum threshold value for an SP to be in the "Black List" is 0.1 so to keep the new SPs on the safe side a value of 0.2 is assigned. The maximum "fee charge" for the SPs occupying "Black List" is 20 USD per service.

The next phase comprises requesting the already registered services. SRs can request multiple services at the same time. When the service request is generated, SR status is checked to ensure that the requested service is coming from a valid SR. Upon acceptance of the service request, SRs avail the requested services.

A complete process for requesting service is represented in Algorithm A2 (please refer to Appendix A). Whenever SR places a request for acquiring one or more than one service, a validity check is performed on the status of SR. This validity check is a part of the "regular check and penalty mechanism for SR". This validity check ensures that SR is allowed to request that service/ services. An SR can avail of up to any number of services if found to be absent from the list of "Temporarily Banned" and "Permanently Banned". In case, the validity check fails, the request is not forwarded to the SP, and SR is informed accordingly. The failed service request comes under the umbrella of the banned scenario. Temporarily Banned still gives chance to the SR to request some other service after informing SR accordingly. But if the SR occupies a place in the list of "Permanently

Banned", then that specific SR is forbidden from requesting any kind of service. However, the successful service request is followed by the service acceptance or service rejection as shown in Algorithm A3 (please refer to Appendix A). Algorithm A3 states the steps for providing services to SRs. Algorithms A2 and A3 are interconnected since the successful service request by SR can only be fulfilled if followed by the service acceptance from the selected SP. SP has the right to either accept or reject the service. SR is notified about the acceptance or rejection of service accordingly by the SP. All the requests are forwarded to SP in Algorithm A3 only if the SR passes the validity check as shown in Algorithm A2.

The third phase which corresponds to the "Trust Computation" process, handles feedback provided by SRs for each of the availed services. In our research study, the prime focus is given to the "intention" and "ability" of the Service Requesters (SRs) to provide correct feedback to the Service Providers (SPs). These "two-stage parameterized feedbacks" form the basis of calculating local trust, global trust, and reputation values. To facilitate the SRs in providing correct feedback, the 5 parameters encompassing QoS and Social Trust are defined named Availability (Av), Accuracy (A), Cruciality (Cr), Responsiveness (R), and Cooperation (C). The inputs to these parameters are taken in two stages. The first stage ("pre-service avail") reflects the weightage (0–1) in terms of the importance of these parameters for SRs with respect to a particular service. Therefore, the "intention" of SRs was revealed by pre-evaluation ("pre-service avail"), revealing which criteria are more relevant to SRs and which are less significant to SRs in relation to a certain service. The importance of each of the aforementioned five factors is represented by the initial values chosen for them. Additionally, these weights show the significance of the 5 characteristics from SR's perspective with regard to a certain service. The second stage ("post-service avail") represents the rating of 5 parameters based on the actual experience of SR after the service is availed. Thus, pre-evaluation ("pre-service avail") and post-evaluation ("post-service avail") are responsible for the calculation of local trust based on the "two-stage parameterized feedback" in the form of informed decisions. The "two-stage parameterized feedback" on the one hand provides SRs with the "ability" to decide the importance of various features in the service they are about to acquire and on the other hand once the service is acquired, rate the SPs accordingly based on these parameters.

Trust values are based on the services provided by the SPs rather than on the SPs as a whole. Therefore, it is important to differentiate amongst various services provided by the SPs. The trust is decomposed into two parts: Local Trust and Global Trust. Local Trust Values (Tlocal) are calculated as a weighted sum from "two-stage parameterized feedback" given for each availed service by SRs. These values after being normalized to ensure that they lie in the range 0–1, proceed to the "Trust Aggregation" phase for Global Trust Values (Tglobal) calculation. The global view of the rating for a service is provided through Tglobal. Tglobal is the summation of the current Tlocal and the past Tlocal values. Tglobal includes a decay factor (as represented by "h" in Algorithm A4 (please refer to Appendix A)) for older Tlocal values as compared to the newer ones to give more weightage to the recent Tlocal values. Once the Tglobal values are calculated, these values are normalized to keep the calculated values in the allowable range of 0–1. Reputation values are calculated on the basis of Tglobal values for all services provided by that specific SP. The reputation value is a measure to bound SP to provide all services in a satisfactory way.

Trust and reputation update in our trust management framework is event-driven. At each feedback, the value of trust and reputation is updated, and based on the "regular check and penalty mechanism", the SPs are assigned to the corresponding status list (White List, Grey List, and Black List).

Figure 2 represents the categorization of the "regular check and penalty mechanism" for SRs and SPs. When implementing the mechanism, the "suspicious SR" can be banned temporarily or permanently based upon certain criteria as shown in Algorithm A6 (please refer to Appendix A). For SPs, the penalty causes the SPs to be placed in either "Grey List" or "Black List" whereas the "White List" is the privileged list in accordance with the criteria represented in Algorithm A5 (please refer to Appendix A).

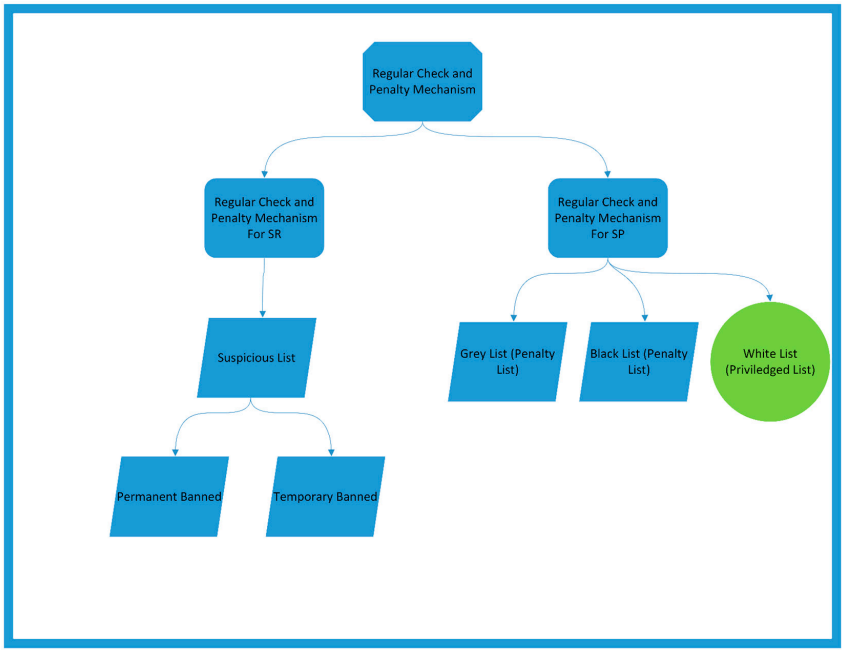

Figure 2. Regular Check and Penalty Mechanism.

The proposed "regular check and penalty mechanism" provides resiliency against the aforementioned attacks. A brief representation of the "regular check and penalty mechanism for SPs and SRs" is shown in Figure 2. Since the Tlocal, Tglobal, and reputation values are updated regularly based on the feedback, therefore the terminology "regular check" is used. To incorporate the "regular check and penalty mechanism for SPs" in our proposed trust and reputation management framework, the SPs are placed in 3 different status lists (White List, Grey List, and Black List) in accordance with the reputation values as shown in Algorithm A5. In every list, an upper limit is imposed on the maximum fee that can be charged for the services. The maximum thresholds of fee charges by SPs per service are 20 USD for "Black List", 50 USD for "Grey List", and 100 USD for "White List". To regulate the SPs to provide all the services in a satisfactory manner, the reputation value is based on all services provided by SP. This distribution of SPs in the aforementioned 3 status lists helps in providing resiliency against SBA, OSA, DA, and OOA. Tglobal and reputation values help the SRs to decide about the selection of the SP. Moreover, every SP can provide a specific service to a maximum count, therefore SPs can't receive requests for a specific service beyond the maximum count for each service, therefore providing resiliency against DDoS. The ranges of the reputation values and maximum fee charge for each list are selected to provide a stern penalty to dishonest SPs while keeping a constant check on them.

Two penalty lists are created to implement the "regular check and penalty mechanism for SR," obliging the SRs to rate truthfully and resisting SPA/GMA, BMA, and BSA. The regular check mechanism is incorporated as Tlocal, Tglobal, and reputation values are calculated after every feedback. Because the rating provided by the fraudulent SR is either too high or too low, creating a discrepancy of $\geq$0.3 between Tlocal and Tglobal for either 2 times or 3 times, the SR is "Temporarily Banned" from requesting a certain service. According to "Permanently Banned," the SR is prevented from making any service requests if the gap between Tlocal and Tglobal $\geq$ 0.3 for more than three occasions. The procedure used to verify SR's authenticity is represented by Algorithm A6. We carefully crafted the criteria for both the Banned Lists and the Suspicious List to ensure that dishonest SRs are severely punished and regularly monitored.

The "regular check and penalty mechanism" are implemented with a view to dealing with many of the trust-related attacks in SIoT. The attacks that are dealt with in our suggested model fall into two major categories named as:

(i) Collaborative Attacks
(ii) Individual Attacks

Collaborative Attacks: Entities (SCs) collaborate to attack an SP in collaborative attacks. Collaborative attacks have two classifications:

- Bad Mouthing Attack: After obtaining acceptable service, the SC purposefully gives unfavorable comments. In this attack, a number of SCs group together to pick on a certain SP and provide unfavorable feedback. As a result, attackers with low ratings improve their reputation by giving unfavorable feedback to nodes with a strong reputation. Attacking nodes get an increase in reputation ratings as a consequence [12]. BMA is prevented in our proposed model by implementing the "regular check and penalty mechanism for SR". To combat BMA, a regular check on the difference between Tlocal and Tglobal is beneficial. If Tglobal–Tlocal $\geq$ 0.3, then the SR responsible for that Tlocal would be placed in the "Suspicious List" which further leads to SR being Temporarily or Permanently Banned.
- Ballot Stuffing Attack: Several malicious nodes work together to boost the reputation of another fraudulent node by consistently giving that node favorable feedback. Thus, it increases the likelihood that the adversary will be chosen as a potential SP. There is often no common ownership between the target nodes and the attackers [12]. Instead, various nodes (attackers) work together to offer each other positive feedback in order to raise the rating of nodes with a poor reputation. BSA is not successful in our suggested framework since the reputation value does not depend upon just one service but upon all the services provided by that particular SP. Moreover, any difference between the Tlocal and Tglobal resulting in the value $\geq$ 0.3 i.e., if the condition Tlocal–Tglobal $\geq$ 0.3, then this causes the fraudulent SRs that are responsible for making the condition valid, to be placed in the list of either "Temporarily Banned" or "Permanently Banned".

Individual node attacks include those listed below, which include:

- Self-Promotion Attack/Good Mouthing Attack: The entity presents itself as one of the most reliable SP by offering positive recommendations about itself [12]. In this case, the attacker controls many SC nodes, all of which give an SP a high rating. In other words, attackers own the SP and SC. Our suggested approach eliminates the possibility of SPA/ GMA by the use of a "regular check and penalty mechanism for SR." Regularly comparing local and global values (Tlocal minus Tglobal) is useful for preventing SPA/GMA. If Tlocal–Tglobal is more than or equal to 0.3, the SR responsible for that Tlocal will be added to the "SUSPICIOUS LIST," which might lead to a suspension, either temporarily or permanently by later on adding them into the "Temporarily Banned List" or "Permanently Banned List" if the criteria satisfy.
- On-Off Attack: A node (SP) attempts to keep up a steady reputation by alternating between providing good and poor services. The node (SP) begins providing quality service when it determines that its reputation is likely to fall below a certain level [12].
- Opportunistic Service Attack: SPs use their high trust value to be chosen, but they work with other malevolent entities/nodes to attack the chosen node [12,64].
- Selective Behavior Attack: An SP performs well for some services and poorly for others. For instance, an SP performs well when resource usage is low and poorly when it is not [12].
- Discriminatory Attack: Regardless of the reputation of the other node, the attacker nodes deliver an attack on the targeted nodes that don't have strong social ties with them [64].

Our suggested framework provides resiliency against the attacks (OOA, OSA, SBA, and DA) by implementing the "regular check and penalty mechanism for SP". The continuous monitoring and placement of SPs in the "Grey List" and "Black List" in accordance with the reputation values force the SPs to provide good and satisfactory service all the time for all the services they offer. Moreover, SPs who are placed in the "Grey List" and

"Black List" also suffer a financial setback as every list has a maximum threshold for fee charges. SPs present in the aforementioned 2 lists also has fewer chances to be selected as the potential SP for a specific service. These drawbacks compel the SPs to behave in an appropriate way every time for every service thus, providing resiliency against the OOA, OSA, SBA, and DA.

Attacks that aren't normally related to SIoT networks can nonetheless do more harm to the targeted SIoT networks if they're launched from outside the network. These can be characterized as "Extrinsic Attacks," such as Storage Attacks, Sybil, Distributed DoS, and Message Spoofing and Denial of Service (DoS) attacks.

A flowchart representing the complete flow of our trust and reputation management framework is presented in Figure 3a,b. In Figure 3a,b, "2" is used as a "Page Connector".

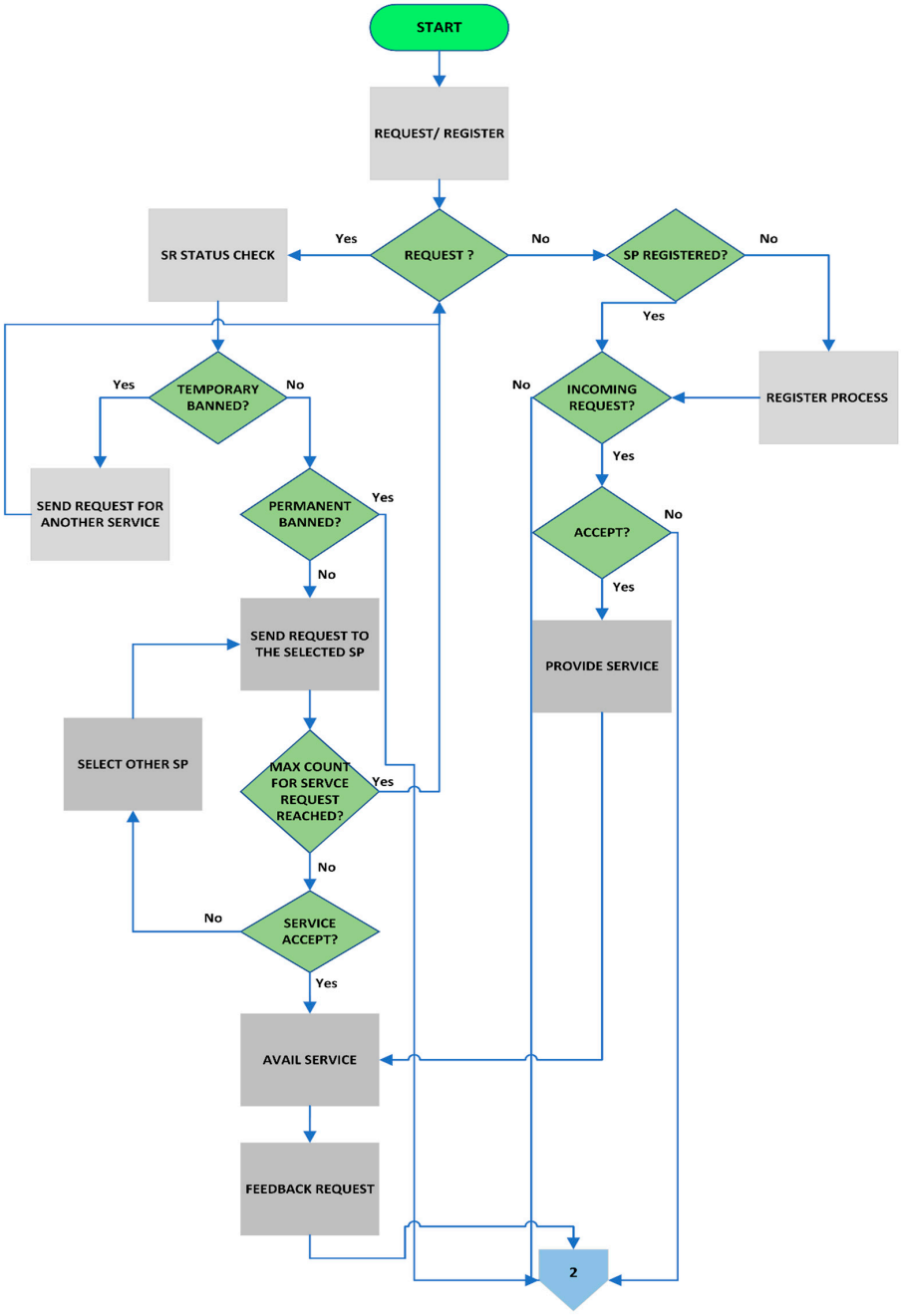

Figure 3. *Cont.*

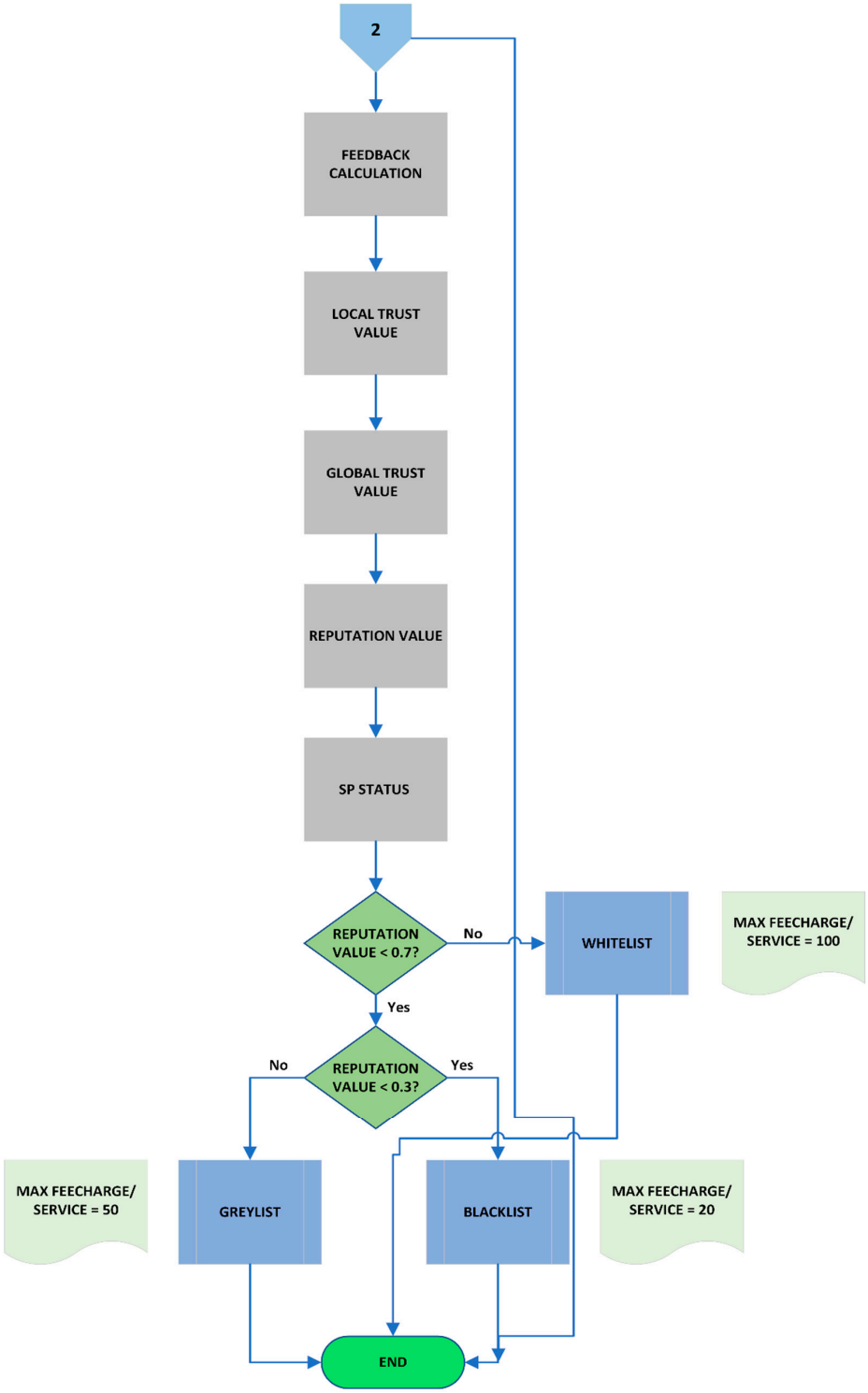

Figure 3. Flow Chart for Our Trust and Reputation Management Framework.

4. Results and Discussion

We have implemented the "Ethereum Private Blockchain" on "Ganache" to verify our trust management model. We have selected Ethereum since Ethereum offers the designing of various types of blockchain applications in an easy-to-use way. The Node Package Manager (NPM), which is included with Node.js, is the first dependency that needs to be set up. Ethereum enables programmers to create "smart contracts," which are pieces of code that are executed in response to predefined events. In turn, the Ethereum web3.js

API processes these events. A smart contract is a piece of blockchain-based, autonomous software. These are quite similar to the standard commercial contracts that are used when two parties agree on a code of conduct for their dealings with one another. When the predetermined conditions are satisfied, the smart contracts will automatically carry out their intended actions. By removing the need for a trusted third party or central authority, smart contracts may facilitate the execution of agreements and transactions between parties that may not otherwise be able to do so securely or reliably. Solidity is a programming language used to create smart contracts. In this method, the smart contracts are tested in Truffle Framework before being deployed to the blockchain. The Truffle framework makes it easier to create, test, and launch distributed programs. Truffles have an ecology that includes Ganache. It's useful for developing Ethereum since it offers a private blockchain. It's similar to an Ethereum client in that respect. It can be used to put the truffle-based decentralized app through its tests. In the process of building a decentralized system, it may be utilized to implement contracts. The Ethereum address and private key for each Ganache account are completely unique. The framework also makes it easier to test blockchain and smart contracts. The database in our proposed framework is developed on MongoDB which stores the data from the blockchain in the form of events and is connected to the front end developed on React js to display different charts.

The test cases use to validate our proposed trust and reputation management framework are represented by different SPs (SP1, SP2, SP3, and SP4) addresses. The first two test cases represented as SP1 and SP2 are demonstrated below where the total number of cumulative feedbacks for 10 SPs is 1000 where "malicious feedback" and "dishonest SPs and dishonest SRs" is given consideration. For SP3 the cumulative feedback for 10 SPs is 2500 and for SP4 the cumulative feedback for 10 SPs is 800. SP3 and SP4 represent the case of "honest SPs and honest SRs". The number of feedbacks generated for each SP is different. The focus of these test cases is to validate our proposed trust and reputation management framework in various scenarios. The reputation charts represent the values of different SPs based on the Tglobal (global trust values) associated with each SP with respect to all the services they have offered. Since every SP has offered a different number of services therefore the cumulative feedback generated for every SP is different. The reputation chart for SP1 is shown in Figure 4 whose address is 0x5913e2250B528FB976fb238C6a61b4E078af9954 with the number of feedbacks generated for this SP1 is 97 and SP2 (Figure 5) whose address is 0x1Ac2CbA8318299A45d47A0fF1B94A692B9C1b444 and the number of feedbacks generated for SP2 is 77. SP3 (Figure 6) address is 0xf75Eba840D946821247659C879E9562153dB8275 with 235 feedbacks generated. SP4 (Figure 7) whose address is 0xfDbB93D91076617F B6a4a786383872A1e992Dc45 with a total number of feedbacks is cumulated 69. The addresses of SPs are shown in the dropdown box of the SP status chart depicting the switching between 3 different lists. In Figures 4–7, the x-axes represent the number of feedbacks shown as (# of feedbacks) and the y-axes represent reputation values in the range 0–1.

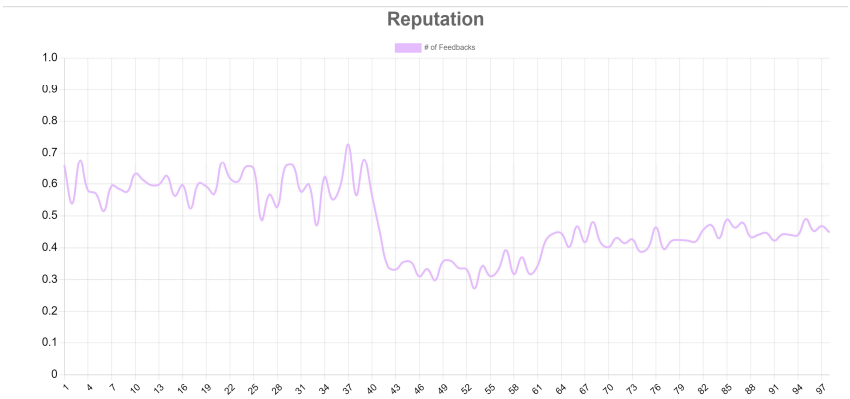

Figure 4. Reputation Chart for SP1.

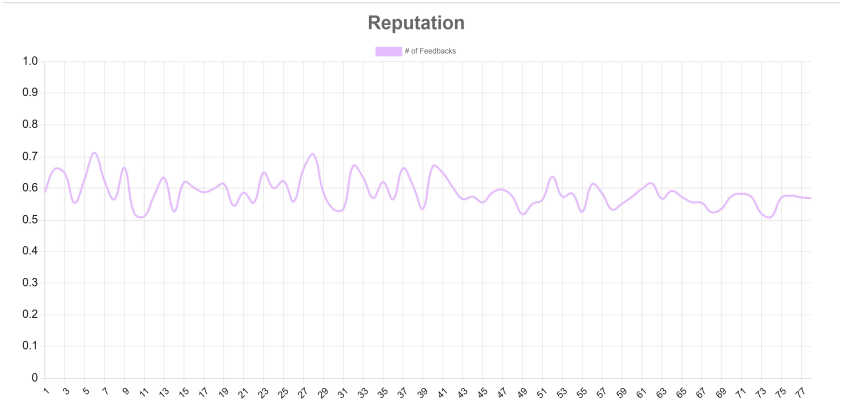

Figure 5. Reputation Chart for SP2.

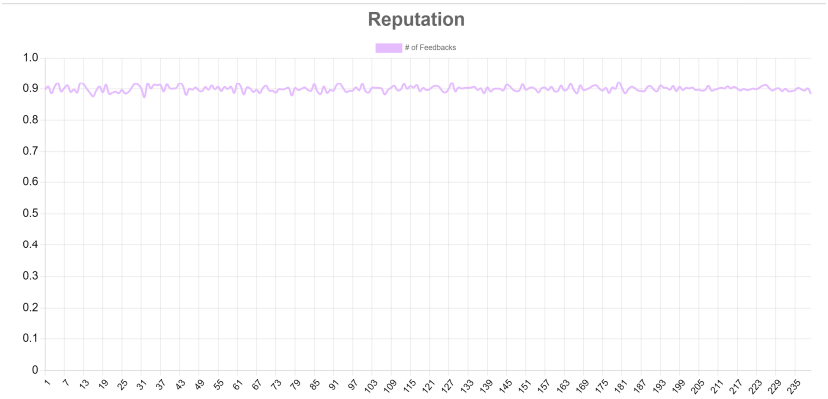

Figure 6. Reputation Chart for SP3.

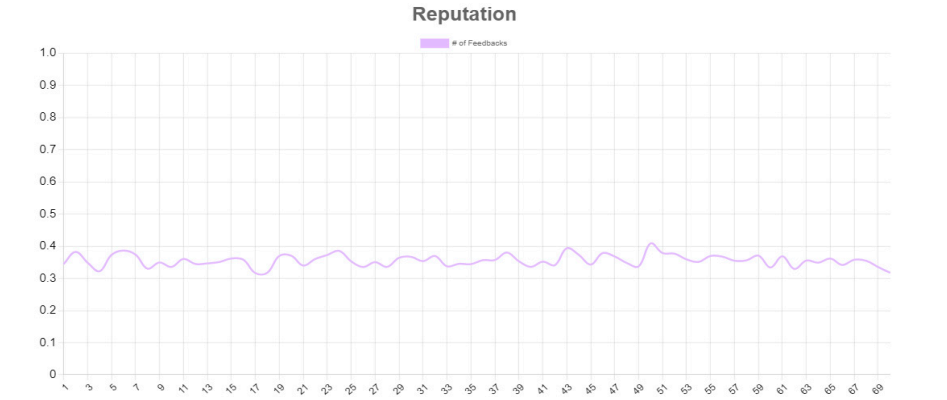

Figure 7. Reputation Chart for SP4.

The reputation charts for SP1 and SP2 (Figures 4 and 5) show the variation in the reputation because "malicious feedback" and "dishonest SRs and dishonest SPS" are considered in these cases thus representing malevolent SRs and SPs. The tables (Tables 3 and 4) represented below show the reputation values where the switching of SPs (SP1 and SP2) amongst 3 different lists (White List, Grey List, and Black List) takes place thus depicting the current status of SP. These switching amongst lists reflect the fact that SPs (SP1 and SP2) are unable to provide satisfactory services thus based upon the reputation values, the SPs (SP1 and SP2) statuses are reflected. These switching amongst the status takes place on the basis of the specified range for a particular status value. The ranges are depicted in Algorithm A5. The SP1 and SP2 statuses are represented in Tables 3 and 4 respectively. However, Figures 4 and 5 also depict the fact that the dishonest SPs are forced to act

honestly else their reputation values won't converge. Since SP3 and SP4 reflect the case of "honest SRs and SPs" therefore, the switching amongst the lists takes place only once. SP3 switches to White List for the reputation value of 0.8974. SP4 switches to Grey List for a reputation value of 0.345 from the initial default value of 0.2 for the Black List.

Table 3. Reputation Values representing variation in SP1 status.

Status	Number of Feedback	Reputation Values
Grey	1	0.659
White	37	0.727
Grey	38	0.565
Black	48	0.298
Grey	49	0.357
Black	53	0.273
Grey	54	0.343

Table 4. Reputation Values representing variation in SP2 status.

Status	Number of Feedback	Reputation Values
Grey	1	0.586
White	6	0.714
Grey	8	0.565
White	28	0.708
Grey	29	0.587

It is to be noted that the change in SPs status is a continuous process as the updates in the trust and reputation values are event-driven. The updates take place after every interaction (Feedback). This feature provides resiliency against the attacks OSA, DA, SBA, and OOA. The SP when fails to main a satisfactory reputation is listed in either Grey List or Black List. These lists are considered the "penalty lists", especially the Black List. SPs present in the aforementioned 2 lists has fewer chances to be selected to provide a specific service by the corresponding SR. Moreover, the fee that can be charged by SPs presented in these 2 lists for each service is much less than the fee that can be charged for the SPs present in the White List. The maximum fee that can be charged by the SP in the Grey List is half the maximum fees that can be charged by the SPs that are present in the White List. For the SPs present in the Black List, the bar to charge maximum fees is even lower as the SPs present in the Black List can only charge 20% of the maximum fees that can be charged by the SPs in the White List. Therefore, to occupy a place in the White List, a constant good reputation value is to be maintained thus restricting the SPs to act honestly. Hence, dishonest SPs who either perform good service for some time before proceeding to provide below-par services or would perform below-par service once they are selected or provide certain good services and certain below-par services fail to maintain their position in White List and are eliminated from it. Hence, it prevents SPs to launch attacks (OSA, DA, OOA, and SBA) and forces them to act honestly else they would not only have fewer chances to get selected but also suffer a financial setback by only being able to demand 20% or 50% (depending upon the list) of the maximum fee charge as compared to the ones present in the White List. Moreover, constant monitoring is going on as the status of SP is updated after every feedback for the specific service so a good reputation value must be maintained on a regular basis. Since reputation values are the average of Tglobal for all services provided by a specific SP, therefore every offered service must be provided in an honest way. SP1 and SP2 represent the test cases for "malicious feedback" and "dishonest SPs and dishonest SRs" whereas SP3 and SP4 represent the test cases for "honest SPs and honest SRs". In accordance with Table 3, SP1 is switched to Grey List 4 times, to White List 1 time, and to Black List 3 times (by default all the SPs are initially in Black List as the default value of the reputation of SP = 0.2). This switching amongst SP status is shown in Figure 8 for SP1. In accordance with Table 4, SP2 is switched to Grey List 3 times, to White List 2 times, and to Black List 1 time (by default all the SPs are initially in Black List as the default

value of the reputation of SP = 0.2). This switching amongst SP status is shown in Figure 9 for SP2. SP3 switches one time from Black List to White List for one feedback and then continues to remain in the White List as represented in Figure 10 whereas SP4 switches to Grey List from Black List for 1 feedback and then remains in the Grey List as represented in Figure 11. The frequent variation as shown in Figures 8 and 9 not only helps to identify the malevolent SPs. However, mostly the SPs tend to act honestly in our trust and reputation management framework due to the financial setbacks in case of dishonesty thus, providing resiliency against the OSA, DA, OOA, and SBA. Figures 4 and 5 also depict the fact that the dishonest SPs are forced to act honestly else their reputation values won't converge.

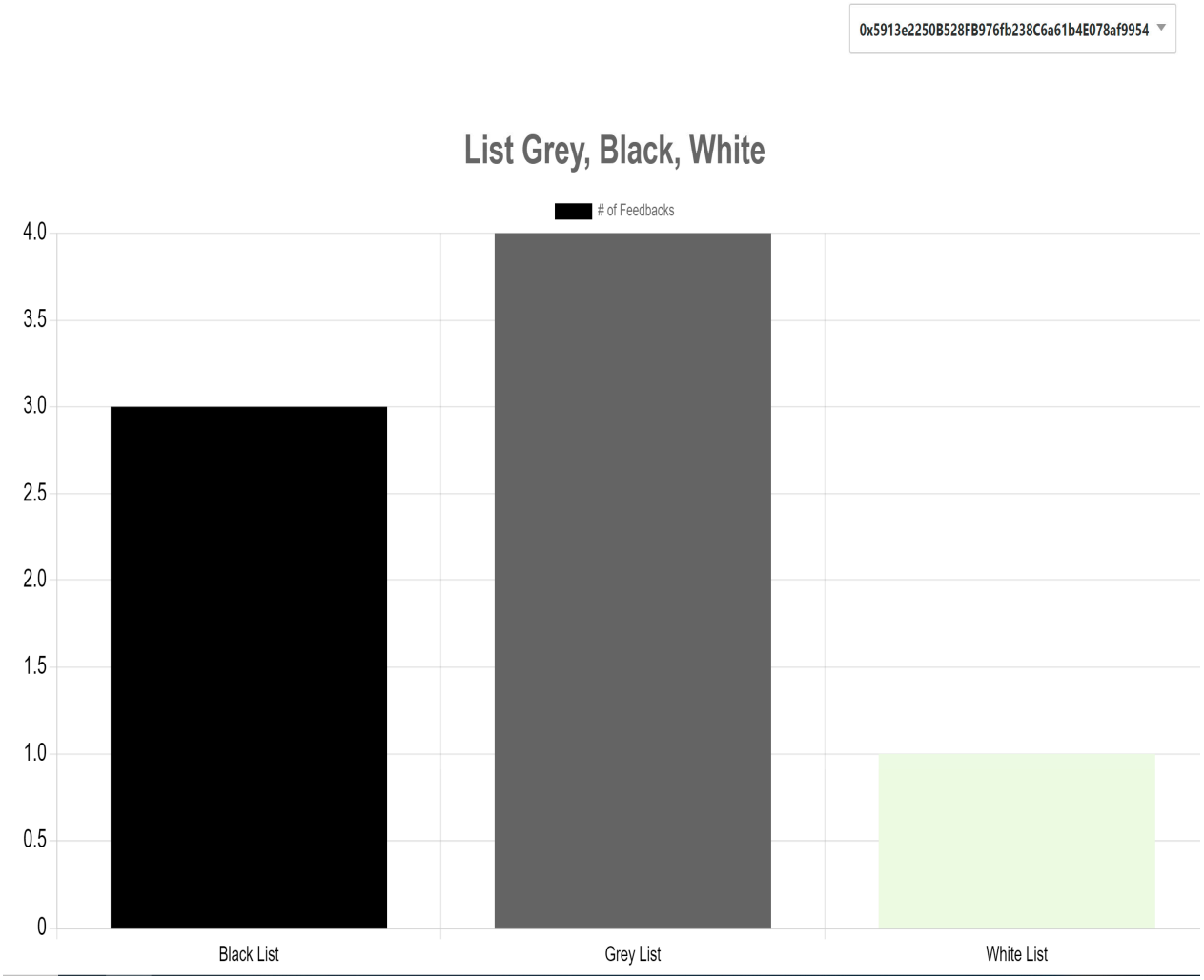

Figure 8. Variation in SP status based on the Reputation Values for SP1.

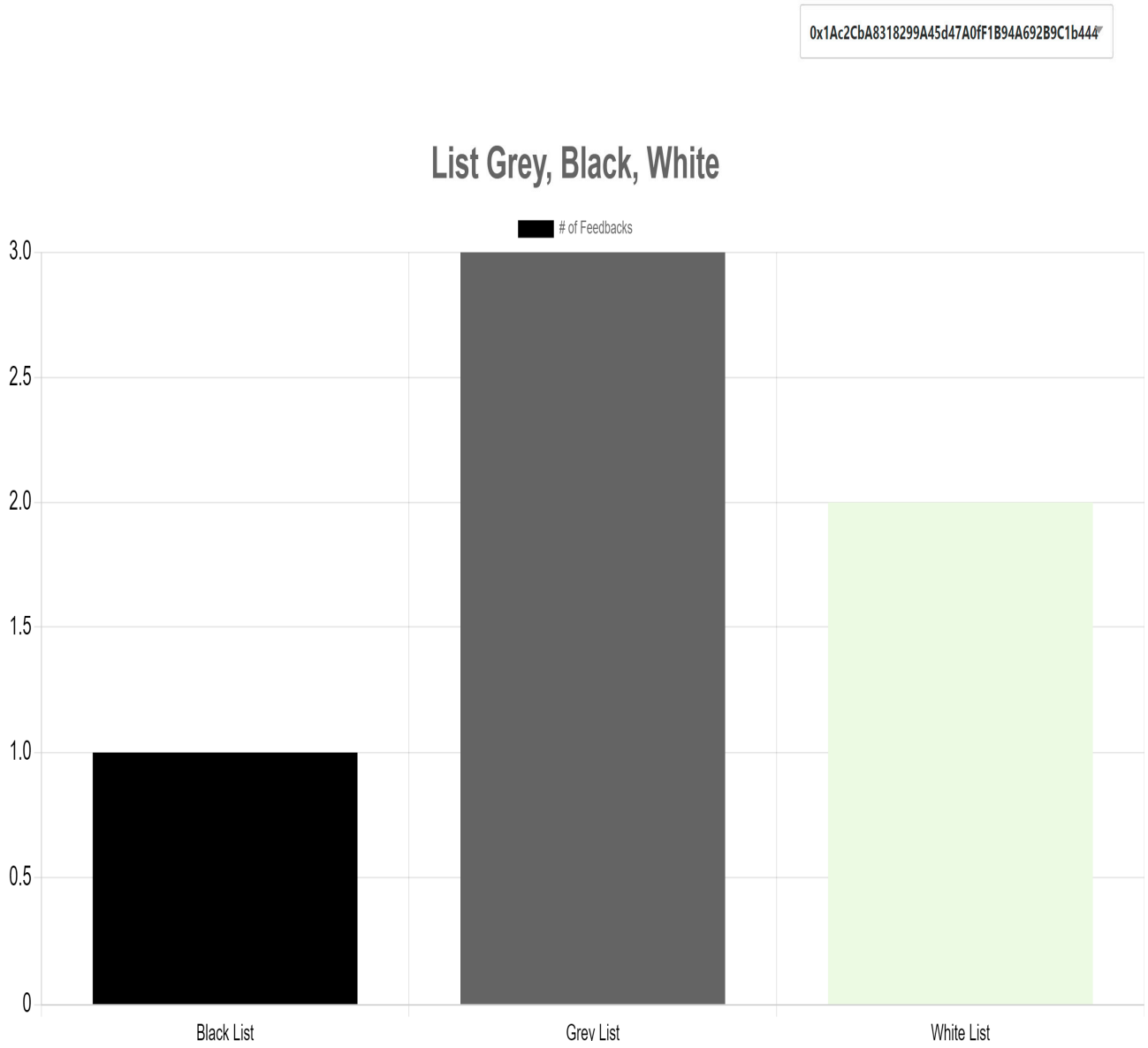

Figure 9. Variation in SP status based on the Reputation Values for SP2.

Figure 10. Variation in SP status based on the Reputation Values for SP3.

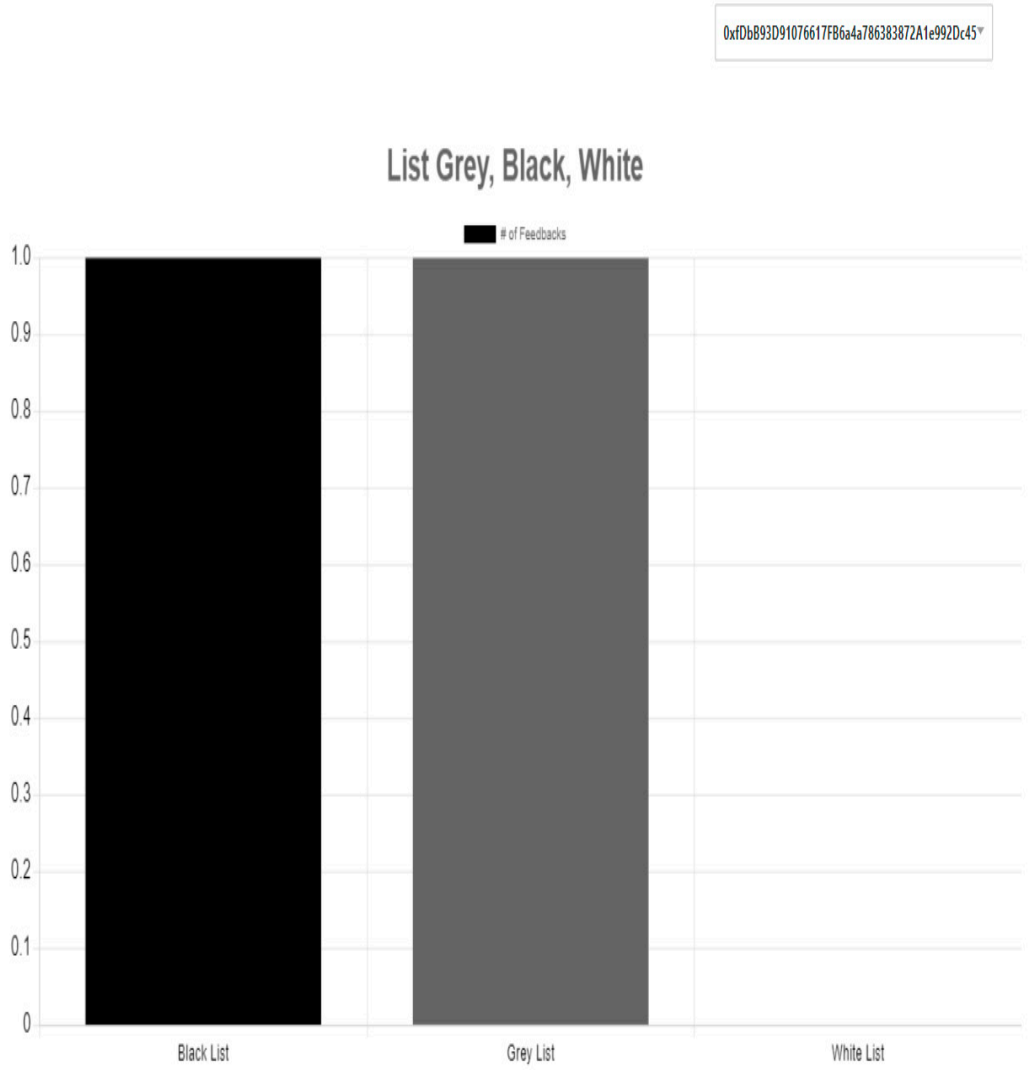

Figure 11. Variation in SP status based on the Reputation Values for SP4.

It is assumed that 5 services are provided by SPs. However, the number of times these 5 services are provided is different for each SP. These services are represented as S1, S2, S3, S4, and S5 for visibility and clear representation. The variation in the feedback values for SP1 (Figure 12) and SP2 (Figure 13) represents "dishonest SRs and dishonest SPs" and "malicious feedbacks". SP3 (Figure 14) and SP4 (Figure 15) Tglobal values are for the scenario of "honest SRs and honest SPs" where SRs don't provide "malicious feedback" and SPs also act honestly. The Tglobal chart is the representation of the fact that for different services, SP has different Tglobal. Thus, our trust and reputation management framework reflects the fact that Tglobal values are service-based values. In case of the "malicious feedback", the variation in the calculated Tglobal values is high but despite the variation, the reputation values of SP stabilize thus validating our proposed trust and reputation management framework. For Figures 12–15, the Global Trust Values (Tglobal) are represented in the range of 0–1 along y-axes and the number of feedbacks is represented along x-axes.

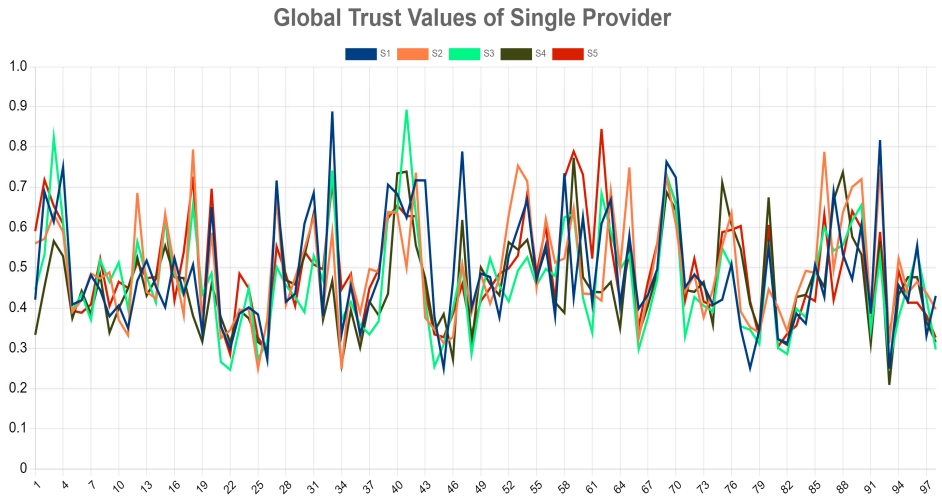

Figure 12. Global Trust Values (Tglobal) for 5 different services provided by SP1.

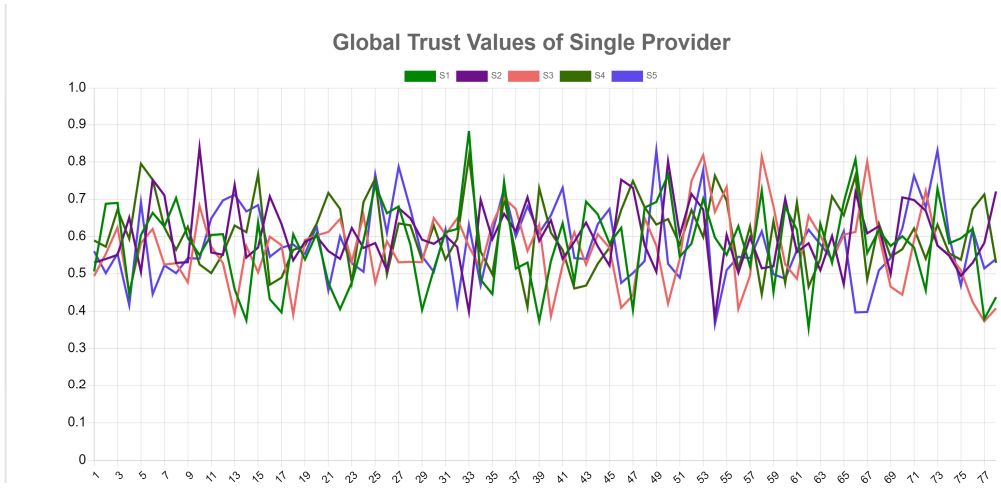

Figure 13. Global Trust Values (Tglobal) for 5 different services provided by SP2.

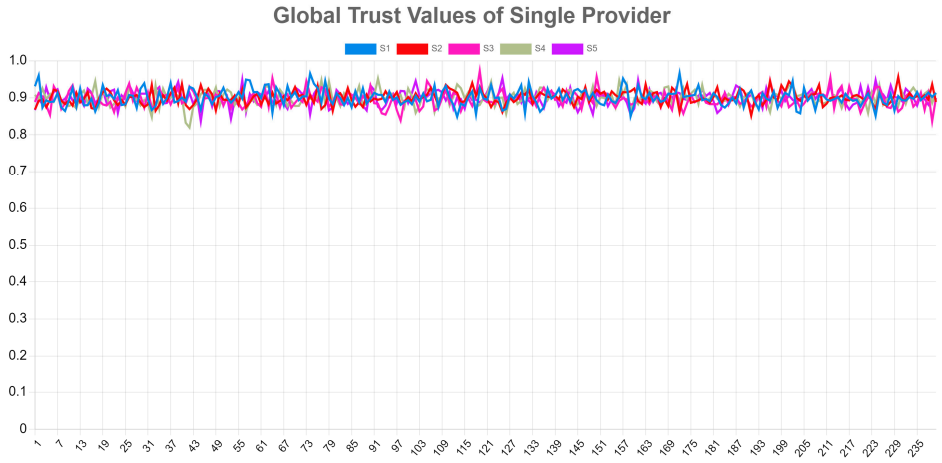

Figure 14. Global Trust Values (Tglobal) for 5 different services provided by SP3.

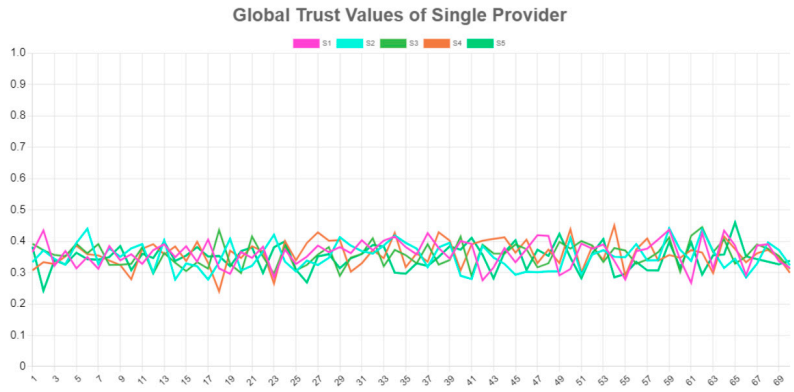

Figure 15. Global Trust Values (Tglobal) for 5 different services provided by SP4.

It is assumed that 5 services are provided by SP. However, the number of times these 5 services are provided is varied for each SP. These services are represented as S1, S2, S3, S4, and S5. The frequent variation in the global trust values (Tglobal) is due to "malicious feedback" and "dishonest SP and dishonest SR" as shown in Figures 12 and 13. Figures 16 and 17 provide a banned list of SRs generated for a cumulative 1000 feedbacks for SP1 and SP2. Since SP3 and SP4 are the cases representing "honest SRs and honest SPs", therefore there is no banned list for SP3 and SP4. Before being banned, SRs are first placed in the Suspicious List only if the difference between Tlocal and Tglobal ≥ 0.3. This provides resiliency against BMA, BSA, and GMA/ SPA. All those malevolent SRs which provide feedback for a particular service with respect to a particular SP for which Tglobal–Tlocal ≥ 0.3, thus launching BMA or BSA by giving that particular SP significantly low feedback which results in low Tlocal value as compared to the already associated Tglobal value to that SP for the particular service availed are under surveillance by placing them in the Suspicious List. Similarly, Tlocal–Tglobal ≥ 0.3 shows that SR launches SPA/GMA by giving SP significant higher feedback thus resulting in a significant rise in Tlocal associated with that particular SP for the particular service availed as compared to the already associated Tglobal with that particular SP for the particular service. Hence such SRs are placed on the Suspicious List to be monitored regularly. For each suspicious activity performed by SR, the SR is placed on the Suspicious List. If SR performs suspicious activities for >1 time but <3 times, then it means SR is in the Suspicious List for 2 times or 3 times reflecting the fact that that particular SR/ SRs are Temporarily Banned. The SR occupies a place in the Permanently Banned list if the SR is on the Suspicious List more than 3 times. The entire banning process is two-fold. Firstly, it offers regular check mechanisms for each SRs and secondly, it effectively identifies those fraudulent SRs who launches SPA/GMA, BMA, and BSA. Moreover, the SRs are given chances by not banning them at the first significant high or low feedback. The chances are given up to 3 times before being banned permanently. These chances are provided in view of the context that SRs might be unable to judge properly. Therefore, a Temporarily Banned SR can't request the service for which it is banned but can request other services. However, if the assignment of inappropriate feedback by SR happens on more than 3 occasions then it means that SR is fraudulent and is deliberately giving inappropriate values in the form of feedback to the SP with respect to a particular service, so SR is banned permanently. Permanently Banned SRs can never request any service. Figures 16 and 17 show that SR whose address is 0xeD1B8C335A1F0A9ffB6810c49225aA413b07E31C is Banned Permanently as it is banned for services S2, S3, S4, and S5. Similarly, SR whose address is 0x1e4Ae1f19098507F0024c671F8919120bE556148 is Banned Permanently as it is banned for S1, S2, S3, S4, and S5. All the other SRs which are present in the list are Temporarily Banned thus preventing them from requesting those service/services for which they are Temporarily Banned. However, the Temporarily Banned SRs can request other services for which they are not banned.

SR's Address	Services
0x846963A390FD6FeB873Be9f9a575c39841Bb1519	S4
0xa68DA73F48eDaD7dCFa73f859Bff8f3a1c7c26bE	S5
0x8f37a62b78A0cDda1ACb1DDb9D1e0C076A0c14A4	S1
0x8f37a62b78A0cDda1ACb1DDb9D1e0C076A0c14A4	S4
0x4706ACFD32739D3Ebc9503f6dCc7D17FBf1b929B	S3
0x4706ACFD32739D3Ebc9503f6dCc7D17FBf1b929B	S1
0x4706ACFD32739D3Ebc9503f6dCc7D17FBf1b929B	S2
0x4B5FC7D412efd9e013197eEC5039eC03248D436F	S2
0x4B5FC7D412efd9e013197eEC5039eC03248D436F	S5
0x4B5FC7D412efd9e013197eEC5039eC03248D436F	S4
0xeD1B8C335A1F0A9ffB6810c49225aA413b07E31C	S3
0xeD1B8C335A1F0A9ffB6810c49225aA413b07E31C	S4
0xeD1B8C335A1F0A9ffB6810c49225aA413b07E31C	S2
0xeD1B8C335A1F0A9ffB6810c49225aA413b07E31C	S5
0x7292bA5648213bc5775fcA0128f6097a5D5f1a41	S3
0x1e4Ae1f19098507F0024c671F8919120bE556148	S1
0x1e4Ae1f19098507F0024c671F8919120bE556148	S2
0x1e4Ae1f19098507F0024c671F8919120bE556148	S3
0x1e4Ae1f19098507F0024c671F8919120bE556148	S4
0x1e4Ae1f19098507F0024c671F8919120bE556148	S5
0x95399C173133B8df3823B44A795615c6B915A077	S5
0x7EA5FE167e5b45E99b3e985fD64de46b2841e66B	S1

Figure 16. Banned List for Malicious SRs.

0x4706ACFD32739D3Ebc9503f6dCc7D17FBf1b929B	S2
0x4B5FC7D412efd9e013197eEC5039eC03248D436F	S2
0x4B5FC7D412efd9e013197eEC5039eC03248D436F	S5
0x4B5FC7D412efd9e013197eEC5039eC03248D436F	S4
0xeD1B8C335A1F0A9ffB6810c49225aA413b07E31C	S3
0xeD1B8C335A1F0A9ffB6810c49225aA413b07E31C	S4
0xeD1B8C335A1F0A9ffB6810c49225aA413b07E31C	S2
0xeD1B8C335A1F0A9ffB6810c49225aA413b07E31C	S5
0x7292bA5648213bc5775fcA0128f6097a5D5f1a41	S3
0x1e4Ae1f19098507F0024c671F8919120bE556148	S1
0x1e4Ae1f19098507F0024c671F8919120bE556148	S2
0x1e4Ae1f19098507F0024c671F8919120bE556148	S3
0x1e4Ae1f19098507F0024c671F8919120bE556148	S4
0x1e4Ae1f19098507F0024c671F8919120bE556148	S5
0x95399C173133B8df3823B44A795615c6B915A077	S5
0x7EA5FE167e5b45E99b3e985fD64de46b2841e66B	S1
0x5c93eE534b5FE06e4Bf642756b26A4d1b2BbEed6	S1
0x326Ff026Df40D81Fa9b4e1bF07B8f902359c4865	S5
0xF1b9D3fC6E239B26Bd7e78739dAD584686FeC33c	S1
0xF1b9D3fC6E239B26Bd7e78739dAD584686FeC33c	S2
0xF1b9D3fC6E239B26Bd7e78739dAD584686FeC33c	S4
0x26c2067513664904352d88c7a41467F9Da703079	S3
0x26c2067513664904352d88c7a41467F9Da703079	S4
0x26c2067513664904352d88c7a41467F9Da703079	S1
0xF7b622648A8634B00A601447086137Ed66D3b05	S4
0x73c8253CfSdD114BB9ce94D107b267259b5A3041	S3
0x73c8253CfSdD114BB9ce94D107b267259b5A3041	S4
0xea994ECc5f5DB3e04eC6eF301e1B5F6ec7C98a65	S5
0xc855A7c0Afe14B9249f0411e3A1F9177F1dD8d4F	S4
0xf7415909e20EDDB59Dc70DABfD3c3106601c8C33	S4

Figure 17. Banned List for Malicious SRs.

5. Limitation and Future Work

Our study does not include mechanisms to combat whitewash attack. Our future plans involve enhancing our proposed trust and reputation management framework to protect against whitewash and other forms of external attacks. Moreover, the merging of Machine Learning and Blockchain to design a more efficient trust and reputation management system is also included in our future work.

6. Conclusions

To summarize, we have designed a trust and reputation management model that is completely centered on the provision of services in the domain of the Social Internet of Things (SIoT) with trust evaluations for both SPs (service providers) and SRs (service receivers). To obtain or offer services, the entities (SRs or SPs) connect with one another in SIoT domain. After receiving the requested service, SRs must rate the SPs in the form of feedback. However, there are disadvantages to basing SP feedback ratings on a single cumulative value. First of all, this feedback does not give insight into the criteria by which SP is evaluated. Second, SRs that are "ill-intended" or "dishonest" may purposefully give the SP a low rating even when the SP has provided good service. Thirdly, "amateur" SRs are unable to make the best choices while providing feedback to the relevant SP. We offer the idea of employing "two-stage parameterized feedback" in light of the aforementioned problems. First, it improves SRs' "capacity" to make better decisions about the services they receive. It makes judging simpler for novice SRs or even opens up new "dimensions of the criterion" for experienced SRs to accurately score the SP in accordance with the service they (SRs) have obtained. Second, those SRs who are keener on eventually taking over

as SPs for the same service may enhance it from the perspectives of "Social Trust" and "Quality of Service (QoS)" in the future. The "intention" component of SRs can also be well-analyzed as a result of this. Since the Local Trust Values (Tlocal) are derived from the "two-stage parameterized feedback," it serves as the initial step in the identification of suspicious SRs. " Pre-service avail" and "post-service avail" serve as the two levels of input for "two-stage parameterized feedback." Tlocal is determined by this "pre-service avail" and "post-service avail." Because SRs evaluate many factors based on their perceived significance in relation to the service they are about to acquire, the "pre-service avail" value assists in determining the "intention" of SRs. The "post-service avail" value compels SRs to evaluate the parameters correctly in light of the service provided by the linked SPs after they have used the service. The Global Trust Values (Tglobal) are determined on the basis of Tlocal values. The difference between Tlocal and Tglobal values helps to identify "suspicious" or "dishonest" SRs. If there is any noticeable difference (based on the criteria) in the values of Tlocal and Tglobal for a particular service with respect to a particular SP, that SR is first added to the "Suspicious List" and then, depending on the criteria, is added to the "Banned List."

The trustworthiness values of SPs are evaluated by the trust and reputation management models proposed so far in the SIoT area, while SRs are regarded as trustworthy entities. As a result, the concept of "blind trust" on SRs is paved by these trust and reputation models. We have suggested a "two-way trust and reputation management" to get over this problem by giving a way to monitor both SP and SR performance. The "breach of trust" and "idea of hostile nodes" are not just confined to SPs, but also include SRs, according to the suggested paradigm. Due to the constant monitoring of SRs, our model refutes the premise of "blind trust" in SRs. The frequent check and balancing phenomena prompted the addition of a "regular check and penalty mechanism" for SR in addition to SP in our proposed architecture.

The "service-based" requirements for the implementation of a framework for trust and reputation management are the emphasis of our proposed model. The foundational element of "social relationships" in SIoT is the "service-based" idea. For some types of services, SPs are regarded as trustworthy, but not for others. As a result, the evaluation of SPs' trust and reputation should be "service-based" or "service-specific". Additionally, SRs can utilize service from one SP that has a high-quality rating in one area while obtaining services from another SP that has a greater quality rating in a different area.

The trust and reputation management systems that have been proposed so far have not yet taken into consideration the "concept of fee charge." It's important to comprehend this concept as SPs typically provide their services in order to earn money. Therefore, to guarantee that SPs are offering services in an ethical manner, this concept is included in our proposed trust and reputation management system. The "regular check and penalty system" that we suggest also makes use of the "fee charge idea," which results in financial loss for the dishonest SP. Hence, forcing the SPs to act in an honest way.

A system of checks and balances is provided for SPs by the "regular check and penalty mechanism for SPs." Based on the services they offer; SPs are arranged into distinct SP status categories that reflect the values associated with their reputations. There is a top limit for the "fee charge" on each list. Only the maximum amount permitted for that specific list may be charged by providers who are members of that list. Based on the criteria stated in more detail in the paper, these lists are divided into "White List, Grey List, and Black List" categories.

The "regular check and penalty system for SRs" is implemented to limit SRs' ability to behave dishonestly. This mechanism enables the malicious SRs to be sorted into the "Suspicious List," "Temporarily Banned List," and "Permanently Banned List" according to criteria further explained in our work. The "Temporarily Banned List" and the "Permanently Banned List" differ in that the former permits the SR to request services for which they are not specifically banned, but the latter prohibits the SR from requesting any services. As a result, if an SR is Temporarily Banned, they can request other services for which they

are not banned, however Permanently Banned SRs are forbidden from seeking any services. The gap between the local trust and the global trust to be greater than the threshold value serves as the basis for SRs to be transferred from the "Suspicious List" to the "Banned List" (temporarily banned or permanently banned).

Our proposed approach makes use of SPs' aggregate global trust values across all of their individual services to determine their reputation score. As a result, it mandates that SPs be truthful in their provision of all services.

In the SIoT domain, our proposed "regular check and penalty mechanism" offers resistance to a variety of trust-related attacks, including the Ballot Stuffing Attack (BSA), Bad Mouthing Attack (BMA), Self-Propagating Attack/Good Mouthing Attack (SPA/GMA), Opportunistic Service Attack (OSA), Discriminatory Attack (DA), Selective Behavior Attack (SBA), and On Off Attack (OOA). Experiments have shown that "dishonest service requesters" are successfully placed in a suspicious list followed by either a permanently or temporarily banned list as per criteria. In a similar manner, "dishonest service providers" are subject to penalties, such as being placed on "Grey List" and "Black List," which lowers both their reputation and their global trust values (Tglobal) along with the threshold on the maximum fee they can charge per service and the chances of being selected by service requesters to provide services.

Author Contributions: Conceptualization, S.A. and S.Z.; methodology, S.A.; software, S.A.; validation, S.A. and S.Z.; formal analysis, S.A.; investigation, S.A.; resources, S.A.; data curation, S.A. and S.Z.; writing—original draft preparation, S.A.; writing—review and editing, S.A., S.Z. and J.A.S.; visualization, S.A.; supervision, S.Z. and J.A.S.; project administration, S.A. and S.Z.; funding acquisition, S.A. and S.Z. All authors have read and agreed to the published version of the manuscript.

Funding: The paper is entirely self-funded by Ms. Sana Alam.

Data Availability Statement: Any data is provided on request to the corresponding author at the email id: sanaalam@ssuet.edu.pk; sana.email43@gmail.com.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Algorithm A1 Algorithm for Registering Service Provider/Providers

Input: Register

```
Procedure Register
    check for SP in the Registered List
        if SP in Registered List == True
            Msg ("Account already registered")
        end if
            exit
        else if SP in Registered List == False
            register for Service/Services
                input: Service/Services (S1, S2, S3 . . . )
                    repeat
                        input: Maximum number of SRs to which a service is
                            provided, Charge for each service
                        add SP in Registered List (List of SPs for each
                            Specific Service)
                        assign Reputation = 0.2
                        Msg ("Service successfully registered")
                    exit
            end else if
        exit
```

Output: Registration of SP/SPs

Algorithm A2 Algorithm for Requesting Service/Services

Input: Request

```
1.  Procedure Request
2.  check for SR in the Banned List
3.      if SR in Banned List == True
4.          check for Banned Status
5.            if Permanently Banned == True
6.              Msg ("You cannot request the service")
7.            end if
8.          exit
9.            else
10.             request for Service/Services
11.               input: Service/Services (S1, S2, S3 . . . )
12.                 repeat
13.                   check SR status for requested service
14.                     if SR in Temporarily Banned List == True
15.                       Msg ("You can't request this service because banned
16.                           list")
17.                     end if
18.                 exit
19.                     else if SR in Temporarily Banned List == False
20.                       select SP from the Registered List
21.                         send Service Request to the selected SP
22.                           if Service Accept == True
23.                             Msg ("Accepted the request")
24.                               input: Av, A, R, Cr, C in the range (0–1)
25.                                 assign Av→ a, A→ b, R→ c, Cr→ d, C→ e
26.                                 avail service
27.                           end if
28.                         exit
29.                           else if Service Reject == True
30.                             Msg ("Provider cannot provide a service,
31.                           Please input another provider address:")
32.                             select other SP from the list
33.                             repeat steps 19–21 till Service Accept ==
34.                                   True Or Maxcount For Service
35.                                   Request == True
36.                               Msg ("You can't request service because
37.                                   exceed Maxcount!")
38.                         end else if
39.                       end else if
40.         exit
41.     end if
42.     exit
```

Output: Service/Services Availed/Not Availed

Algorithm A3 Algorithm for Providing Service/Services

Input: Service/ Services Request

```
Procedure Service Provide
    repeat for each service
        if Service Accept == True
            provide service
        end if
        exit
        else if Service Reject == True
            Msg ("Provider cannot provide a service, Please input another
                provider address:")
        end else if
        exit
```

Output: Service Provided/ Service Rejected

Algorithm A4 Algorithm for Calculating Local Trust, Global Trust, and Reputation Values

Input: Av, A, R, Cr, C

```
Procedure Local Trust/ Global Trust (Based on Each Service)
    repeat for Service Accept == True
        input: Av, A, R, Cr, C in the range (0–1)
            // service pre-avail stage
        assign Av→ a, A→ b, R→ c, Cr→ d, C→ e
        avail service
    exit
        repeat for each service after availing service
            select provide feedback
                input: Av, Av, R, Cr, C in the range (0–1)
                    // service post-avail stage
                calculate Tlocal (t) = (a*Av) + (b*A) + (c*R) + (d*Cr)
                                        + (e*C)
                normalize Tlocal (t)
                calculate Tglobal (t) = Tlocal (t) + (∑ (Tlocal) (t - 1)) *
                        h (decay factor)
                // where h = 1 – 1/√k
                // K = Total number of a particular service (for e.g.,
            S1) by a particular service
                // provider (SP1) i.e., Tglobal (t) for S1 by SP1=
        // Tlocal (t) for S1 by SP1 + (Tlocal)(t-1) for S1 by SP1)*(h)).
                normalize Tglobal (t)
        exit
    Procedure Reputation (Based on Each SP)
        calculate reputation = Σ_{i=1}^{n} Tglobal (t)/n
        // where n = Total no. of different services provided by a specific SP
        exit
```

Output: Local Trust, Global Trust, Reputation

Algorithm A5 Represents SP status (as per 3 different lists)

Input: Reputation Value

Procedure Service Provider Status
  repeat for each SP
    if reputation > 0.1 AND $\leq$ 0.3
      add in Black List AND maximum fee charge == 20
    else if reputation > 0.3 AND $\leq$ 0.7
      add in Grey List AND maximum fee charge == 50
    else if reputation > 0.7 AND $\leq$ 1
      add in White List AND maximum fee charge == 100
    end if
  exit

Output: Sorting of SPs in White List, Grey List, And Black List

Algorithm A6 Represents the validity mechanism of SR

Input: Tlocal, Tglobal

Procedure Service Requester Status
  check for SR in the Suspicious List
    repeat for each SR
      if difference of Tglobal and Tlocal $\geq$ 0.3
        add SR to the Suspicious List
      end if
  check for SR in the Temporarily Banned List
    repeat for each SR
      if (the number of times (SR in Suspicious List) == 2 OR (the number of times (SR in Suspicious List) == 3))
        add SR to Temporarily Banned List
      end if
    check for SR in Permanently Banned List
      repeat for each SR
        if (the number of times (SR in Suspicious List)) >3
          add SR to Permanently Banned List
        end if
Output: Placing SRs in Suspicious List, Temporarily Banned, Permanently Banned List Or SRs Are Not Banned at all

References

1. Kumar, S.; Tiwari, P.; Zymbler, M. Internet of Things is a revolutionary approach for future technology enhancement: A review. *J. Big Data* **2019**, *6*, 111. [CrossRef]
2. Hossein Motlagh, N.; Mohammadrezaei, M.; Hunt, J.; Zakeri, B. Internet of Things (IoT) and the energy sector. *Energies* **2020**, *13*, 494. [CrossRef]
3. Kouicem, D.E.; Imine, Y.; Bouabdallah, A.; Lakhlef, H. A decentralized blockchain-based trust management protocol for the internet of things. *IEEE Trans. Dependable Secur. Comput.* **2020**, *19*, 1292–1306. [CrossRef]
4. Atzori, L.; Iera, A.; Morabito, G.; Nitti, M. The social internet of things (SIoT)–when social networks meet the internet of things: Concept, architecture and network characterization. *Comput. Netw.* **2012**, *56*, 3594–3608. [CrossRef]
5. Afzal, B.; Umair, M.; Shah, G.A.; Ahmed, E. Enabling IoT platforms for social IoT applications: Vision, feature mapping, and challenges. *Future Gener. Comput. Syst.* **2019**, *92*, 718–731. [CrossRef]
6. Lakshmanaprabu, S.K.; Shankar, K.; Khanna, A.; Gupta, D.; Rodrigues, J.J.; Pinheiro, P.R.; De Albuquerque, V.H.C. Effective features to classify big data using social internet of things. *IEEE Access* **2018**, *6*, 24196–24204. [CrossRef]
7. Lin, Z.; Dong, L. Clarifying trust in social internet of things. *IEEE Trans. Knowl. Data Eng.* **2017**, *30*, 234–248. [CrossRef]
8. Tripathy, B.K.; Dutta, D.; Tazivazvino, C. On the research and development of social internet of things. In *Internet of Things (IoT) in 5G Mobile Technologies*; Springer: Cham, Switzerland; Manhattan, NY, USA, 2016; pp. 153–173.
9. Malekshahi Rad, M.; Rahmani, A.M.; Sahafi, A.; Nasih Qader, N. Social Internet of Things: Vision, challenges, and trends. *Hum. Cent. Comput. Inf. Sci.* **2020**, *10*, 52. [CrossRef]
10. Shahab, S.; Agarwal, P.; Mufti, T.; Obaid, A.J. SIoT (Social Internet of Things): A Review. In *ICT Analysis and Applications*; Springer: Singapore, 2022; pp. 289–297.

11. Atzori, L.; Iera, A.; Morabito, G. Social Internet of Things: Turning Smart Objects into Social Objects to Boost the IoT. *Newsletter*. 2015. Available online: https://iot.ieee.org/newsletter/november-2014/social-internet-of-things-turning-smart-objects-into-social-objects-to-boost-the-iot.html (accessed on 1 November 2022).
12. Chahal, R.K.; Kumar, N.; Batra, S. Trust management in social Internet of Things: A taxonomy, open issues, and challenges. *Comput. Commun.* **2020**, *150*, 13–46. [CrossRef]
13. Cho, J.H.; Chan, K.; Adali, S. A survey on trust modeling. *ACM Comput. Surv.* **2015**, *48*, 1–40. [CrossRef]
14. Alam, S.; Zardari, S.; Noor, S.; Ahmed, S.; Mouratidis, H. Trust Management in Social Internet of Things (SIoT): A Survey. *IEEE Access* **2022**, *10*, 108924–108954. [CrossRef]
15. Pourghebleh, B.; Wakil, K.; Navimipour, N.J. A comprehensive study on the trust management techniques in the Internet of Things. *IEEE Internet Things J.* **2019**, *6*, 9326–9337. [CrossRef]
16. Górski, T. Towards Continuous Deployment for Blockchain. *Appl. Sci.* **2021**, *11*, 11745. [CrossRef]
17. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
18. Khan, P.W.; Byun, Y.C.; Park, N. IoT-blockchain enabled optimized provenance system for food industry 4.0 using advanced deep learning. *Sensors* **2020**, *20*, 2990. [CrossRef]
19. Suciu, G.; Nădrag, C.; Istrate, C.; Vulpe, A.; Ditu, M.C.; Subea, O. Comparative analysis of distributed ledger technologies. In Proceedings of the 2018 Global Wireless Summit (GWS), Chiang Rai, Thailand, 25–28 November 2018; IEEE: Piscataway, NJ, USA; pp. 370–373.
20. Saraf, C.; Sabadra, S. Blockchain platforms: A compendium. In Proceedings of the 2018 IEEE International Conference on Innovative Research and Development (ICIRD), Bangkok, Thailand, 11–12 May 2018; IEEE: Piscataway, NJ, USA; pp. 1–6.
21. Toyoda, K.; Machi, K.; Ohtake, Y.; Zhang, A.N. Function-level bottleneck analysis of private proof-of-authority ethereum blockchain. *IEEE Access* **2020**, *8*, 141611–141621. [CrossRef]
22. Yi, X.; Yang, X.; Kelarev, A.; Lam, K.Y.; Tari, Z. Bitcoin, Ethereum, Smart Contracts and Blockchain Types. In *Blockchain Foundations and Applications*; Springer: Cham, Swizerland; Manhattan, NY, USA, 2022. [CrossRef]
23. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for secure ehrs sharing of mobile cloud based e-health systems. *IEEE Access* **2019**, *7*, 66792–66806. [CrossRef]
24. Benedict, S. Serverless blockchain-enabled architecture for iot societal applications. *IEEE Trans. Comput. Soc. Syst.* **2020**, *7*, 1146–1158. [CrossRef]
25. Górski, T. Continuous Delivery of Blockchain Distributed Applications. *Sensors* **2021**, *22*, 128. [CrossRef]
26. Górski, T. Reconfigurable Smart Contracts for Renewable Energy Exchange with Re-Use of Verification Rules. *Appl. Sci.* **2022**, *12*, 5339. [CrossRef]
27. Meena Kowshalya, A.; Valarmathi, M.L. Trust management for reliable decision making among social objects in the Social Internet of Things. *IET Netw.* **2017**, *6*, 75–80. [CrossRef]
28. Chen, R.; Bao, F.; Guo, J. Trust-based service management for social internet of things systems. *IEEE Trans. Dependable Secur. Comput.* **2015**, *13*, 684–696. [CrossRef]
29. Truong, N.B.; Um, T.W.; Lee, G.M. A reputation and knowledge based trust service platform for trustworthy social internet of things. In Proceedings of the 19th Innovations in Clouds, Internet and Networks (ICIN), Paris, France, 1–3 March 2016; pp. 104–111.
30. Truong, N.B.; Um, T.W.; Zhou, B.; Lee, G.M. From personal experience to global reputation for trust evaluation in the social internet of things. In Proceedings of the GLOBECOM 2017-2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; IEEE: Piscataway, NJ, USA; pp. 1–7.
31. Xiao, H.; Sidhu, N.; Christianson, B. Guarantor and reputation based trust model for social internet of things. In Proceedings of the 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, Croatia, 24–28 August 2015; IEEE: Piscataway, NJ, USA; pp. 600–605.
32. Kokoris-Kogias, E.; Voutyras, O.; Varvarigou, T. TRM-SIoT: A scalable hybrid trust & reputation model for the social internet of things. In Proceedings of the 2016 IEEE 21st international conference on emerging technologies and factory automation (ETFA), Berlin/Heidelberg, Germany, 6–9 September 2016; IEEE: Piscataway, NJ, USA; pp. 1–9.
33. Truong, N.B.; Lee, H.; Askwith, B.; Lee, G.M. Toward a trust evaluation mechanism in the social internet of things. *Sensors* **2017**, *17*, 1346. [CrossRef] [PubMed]
34. Jayasinghe, U.; Truong, N.B.; Lee, G.M.; Um, T.W. RpR: A trust computation model for social internet of things. In Proceedings of the 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), Toulouse, France, 18–21 July 2016; IEEE: Piscataway, NJ, USA; pp. 930–937.
35. Abderrahim, O.B.; Elhedhili, M.H.; Saidane, L. CTMS-SIOT: A context-based trust management system for the social Internet of Things. In Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017; IEEE: Piscataway, NJ, USA; pp. 1903–1908.
36. Kowshalya, A.M.; Valarmathi, M.L. Trust management in the social internet of things. *Wirel. Pers. Commun.* **2017**, *96*, 2681–2691. [CrossRef]

37. Marche, C.; Nitti, M. Trust-related attacks and their detection: A trust management model for the social IoT. *IEEE Trans. Netw. Serv. Manag.* **2020**, *18*, 3297–3308. [CrossRef]
38. Meena Kowshalya, A.; Valarmathi, M.L. Dynamic trust management for secure communications in social internet of things (SIoT). *Sādhanā* **2018**, *43*, 136. [CrossRef]
39. Azad, M.A.; Bag, S.; Hao, F.; Shalaginov, A. Decentralized self-enforcing trust management system for social Internet of Things. *IEEE Internet Things J.* **2020**, *7*, 2690–2703. [CrossRef]
40. Jafarian, B.; Yazdani, N.; Haghighi, M.S. Discrimination-aware trust management for social internet of things. *Comput. Netw.* **2020**, *178*, 107254. [CrossRef]
41. Aalibagi, S.; Mahyar, H.; Movaghar, A.; Stanley, H.E. A matrix factorization model for hellinger-based trust management in social internet of things. *IEEE Trans. Dependable Secur. Comput.* **2021**, *19*, 2274–2285. [CrossRef]
42. Talbi, S.; Bouabdallah, A. Interest-based trust management scheme for social internet of things. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *11*, 1129–1140. [CrossRef]
43. Nitti, M.; Girau, R.; Atzori, L. Trustworthiness management in the social internet of things. *IEEE Trans. Knowl. Data Eng.* **2013**, *26*, 1253–1266. [CrossRef]
44. Ekbatanifard, G.; Yousefi, O. A novel trust management model in the social internet of things. *J. Adv. Comput. Eng. Technol.* **2019**, *5*, 57–70.
45. Abdelghani, W.; Amous, I.; Zayani, C.A.; Sèdes, F.; Roman-Jimenez, G. Dynamic and scalable multi-level trust management model for Social Internet of Things. *J. Supercomput.* **2022**, *78*, 8137–8193. [CrossRef]
46. Nitti, M.; Girau, R.; Atzori, L.; Iera, A.; Morabito, G. A subjective model for trustworthiness evaluation in the social internet of things. In Proceedings of the 2012 IEEE 23rd international symposium on personal, indoor and mobile radio communications-(PIMRC), Sydney, NSW, Australia, 9–12 September 2012; IEEE: Piscataway, NJ, USA; pp. 18–23.
47. Abderrahim, O.B.; Elhdhili, M.H.; Saidane, L. TMCoI-SIOT: A trust management system based on communities of interest for the social Internet of Things. In Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017; IEEE: Piscataway, NJ, USA; pp. 747–752.
48. Babar, S.; Mahalle, P. Trust management approach for detection of malicious devices in siot. *Teh. Glas.* **2021**, *15*, 43–50.
49. Sagar, S.; Mahmood, A.; Sheng, Q.Z.; Zhang, W.E. Trust computational heuristic for social Internet of Things: A machine learning-based approach. In Proceedings of the ICC 2020-2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; IEEE: Piscataway, NJ, USA; pp. 1–6.
50. Sagar, S.; Mahmood, A.; Kumar, J.; Sheng, Q.Z. A time-aware similarity-based trust computational model for social internet of things. In Proceedings of the GLOBECOM 2020-2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; IEEE: Piscataway, NJ, USA; pp. 1–6.
51. Rehman, A.U.; Jiang, A.; Rehman, A.; Paul, A. Weighted based trustworthiness ranking in social internet of things by using soft set theory. In Proceedings of the 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 6–9 December 2019; IEEE: Piscataway, NJ, USA; pp. 1644–1648.
52. Rajendran, S.; Jebakumar, R. Friendliness Based Trustworthy Relationship Management (F-TRM) in Social Internet of Things. *Wirel. Pers. Commun.* **2022**, *123*, 2625–2647. [CrossRef]
53. Xia, H.; Xiao, F.; Zhang, S.S.; Hu, C.Q.; Cheng, X.Z. Trustworthiness inference framework in the social Internet of Things: A context-aware approach. In Proceedings of the IEEE INFOCOM 2019-IEEE Conference on Computer Communications, Paris, France, 29 April 2019–2 May 2019; IEEE: Piscataway, NJ, USA; pp. 838–846.
54. Sharma, V.; You, I.; Jayakody, D.N.K.; Atiquzzaman, M. Cooperative trust relaying and privacy preservation via edge-crowdsourcing in social Internet of Things. *Future Gener. Comput. Syst.* **2019**, *92*, 758–776. [CrossRef]
55. Masmoudi, M.; Abdelghani, W.; Amous, I.; Sèdes, F. Deep learning for trust-related attacks detection in social internet of things. In Proceedings of the International Conference on e-Business Engineering, Shanghai, China, 11–13 October 2019; Springer: Cham, Swizerland; Manhattan, NY, USA; pp. 389–404.
56. Premarathne, U.S. MAG-SIoT: A multiplicative attributes graph model based trust computation method for social Internet of Things. In Proceedings of the 2017 IEEE International Conference on Industrial and Information Systems (ICIIS), Peradeniya, Sri Lanka, 15–16 December 2017; IEEE: Piscataway, NJ, USA; pp. 1–6.
57. Ali-Eldin, A.M. A Cloud-Based Trust Computing Model for the Social Internet of Things. In Proceedings of the 2021 International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC), Cairo, Egypt, 26–27 May 2021; IEEE: Piscataway, NJ, USA; pp. 161–165.
58. Abidi, R.; Azzouna, N.B. Self-adaptive trust management model for social IoT services. In Proceedings of the 2021 International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 31 October 2021–2 November 2021; IEEE: Piscataway, NJ, USA; pp. 1–7.
59. Wang, K.; Qi, X.; Shu, L.; Deng, D.J.; Rodrigues, J.J. Toward trustworthy crowdsourcing in the social internet of things. *IEEE Wirel. Commun.* **2016**, *23*, 30–36. [CrossRef]
60. Latif, R. ConTrust: A Novel Context-Dependent Trust Management Model in Social Internet of Things. *IEEE Access* **2022**, *10*, 46526–46537. [CrossRef]
61. Amiri-Zarandi, M.; Dara, R.A. Blockchain-based trust management in social internet of things. In Proceedings of the 2020 IEEE International Conference on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence

and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Calgary, AB, Canada, 17–22 August 2020; IEEE: Piscataway, NJ, USA; pp. 49–54.
62. Amiri-Zarandi, M.; Dara, R.A.; Fraser, E. LBTM: A lightweight blockchain-based trust management system for social internet of things. *J. Supercomput.* **2022**, *78*, 8302–8320. [CrossRef]
63. Wei, L.; Wu, J.; Long, C. Enhancing trust management via blockchain in Social Internet of Things. In Proceedings of the 2020 Chinese Automation Congress (CAC), Shanghai, China, 6–8 November 2020; IEEE: Piscataway, NJ, USA; pp. 159–164.
64. Khan, W.Z.; Hakak, S.; Khan, M.K. Trust management in social internet of things: Architectures, recent advancements, and future challenges. *IEEE Internet Things J.* **2020**, *8*, 7768–7788. [CrossRef]