mathematics

MDPI

Article

Advancing the Social Internet of Things (SIoT): Challenges, Innovations, and Future Perspectives

Mehdi Hosseinzadeh [1,*], Venus Mohammadi [2], Jan Lansky [3,*] and Vladimir Nulicek [3]

[1] Pattern Recognition and Machine Learning Lab, Gachon University, 1342 Seongnamdaero, Sujeonggu, Seongnam 13120, Republic of Korea
[2] Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran 1477893855, Iran; venus.mohammadi@srbiau.ac.ir
[3] Department of Computer Science and Mathematics, Faculty of Economic Studies, University of Finance and Administration, 10100 Prague, Czech Republic; 6425@mail.vsfs.cz
* Correspondence: mehdi@gachon.ac.kr (M.H.); lansky@mail.vsfs.cz (J.L.)

Abstract: This study conducts an in-depth review of the Social Internet of Things (SIoT), a significant advancement from the conventional Internet of Things (IoT) via the integration of socialization principles akin to human interactions. We explore the architecture, trust management, relationship dynamics, and other crucial aspects of SIoT, with a particular focus on the relatively neglected areas of fault tolerance, cloud–fog computing, and clustering. Our systematic literature analysis, spanning research from 2011 to April 2023, uncovers critical gaps and establishes a detailed taxonomy of emerging SIoT themes. This paper not only sheds light on the current state of SIoT research but also charts a course for future exploration and development in this burgeoning field.

Keywords: social networks; Internet of Things (IoT); Social Internet of Things (SIoT); fault tolerance; cloud–fog computing; clustering; resilience and fault tolerance in SIoT

MSC: 68M10

Citation: Hosseinzadeh, M.; Mohammadi, V.; Lansky, J.; Nulicek, V. Advancing the Social Internet of Things (SIoT): Challenges, Innovations, and Future Perspectives. *Mathematics* **2024**, *12*, 715. https://doi.org/10.3390/math12050715

Academic Editor: Daniel-Ioan Curiac

Received: 25 January 2024
Revised: 23 February 2024
Accepted: 26 February 2024
Published: 28 February 2024



Copyright: © 2024 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) encompasses a global, dynamic infrastructure characterized by self-configuration and interoperable communications among physical devices or virtual entities, each with unique identification [1]. These "things" actively engage in social processes and continually evolve within heterogeneous communities based on shared interests, needs, and the advantages of social relationships. However, the decentralized transactions among "smart objects" over the Internet, such as queries or state transformations, bring about notable concerns regarding security and privacy. Consequently, a transformative architecture is imperative to address these challenges within the IoT landscape. Integrating social aspects into the IoT framework has given rise to the concept of Social Internet of Things (SIoT) [2,3].

The primary objective of SIoT lies in fostering social relationships within the IoT paradigm, aiming to facilitate robust knowledge discovery, instill trust, and bolster the scalability and navigability of communications. The integration of social structures into IoT draws inspiration from Fiske's theory [4], which delineates four foundational social models observed within human communities: communal sharing, equality matching, authority ranking, and market pricing. These interaction principles are succinctly summarized in Table 1.

Table 1. Principles of Fiske's relational models' theory.

Relational Model	Description
Communal sharing (CS)	- Corporate equity and membership emerge against any distinction. Individuals in the group share their abilities and meet their needs. - The object's behaviors that are not individually relevant but have a collective relationship. Objects that have this property are associated with the whole group.
Equality matching (EM)	- Justice-seeking relationships are characterized by symmetrical transaction and exchange. - Equality matching represents all forms of information exchange between objects that act equally, requesting/providing information among themselves to provide IoT services to users while maintaining their individuality.
Authority ranking (AR)	- Each individual is characterized by the degree of authority and power that reflects precedence, hierarchical social dimensions, status, rank, command, and deference, which are often asymmetric traits. - Examples include tag and tag reader in RFID, as well as primary and secondary in Bluetooth.
Market pricing (MP)	- Built on the proportionality of value, the interactions of individuals originated according to the balanced scale of the weights. - Work for mutual benefit. As long as it is involved, and it is worth carrying out.

SIoT mirrors human behavior by strategizing selective direct or indirect friendships (such as Friend of a Friend—FoAF) to enhance the quality-of-service composition. The original concept of the socialism of objects was introduced by Holmquist et al. [5] in 2001. Figure 1 visually portrays the evolution of SIoT from the Pre-Internet era (human-to-human intelligence) [6]. Initially, social progress witnessed the integration of human-like traits into intelligent alien entities, progressing further by amalgamating collaborative human and object cognitive data [7].

By harnessing the benefits of both social presence and intelligent decision making [8], SIoT has emerged as a pervasive domain comprising billions of interconnected objects. These objects interface either human-to-thing or thing-to-thing for deductive operations, operating without direct human intervention [9,10]. Consequently, SIoT has evolved into a highly promising area of research [11]. The flourishing of SIoTs via socialization in IoT devices, mirroring human behaviors, aims to achieve the following advantages:

- Objects gradually establish social connections to ensure dependable application and resource interactions, offering reliability and scalability while relieving individuals from direct intervention.
- Advancing the SIoT paradigm involves implementing a social scheme within IoT communities, as proposed by [12].
- This approach enhances trust among object relationships by managing transactions between interconnected "friend" devices, as indicated by [13].
- Via monitoring implicit correlations and patterns among objects, it enables the prediction of object behavior and potential threats, aiding in identifying potential attackers [14].

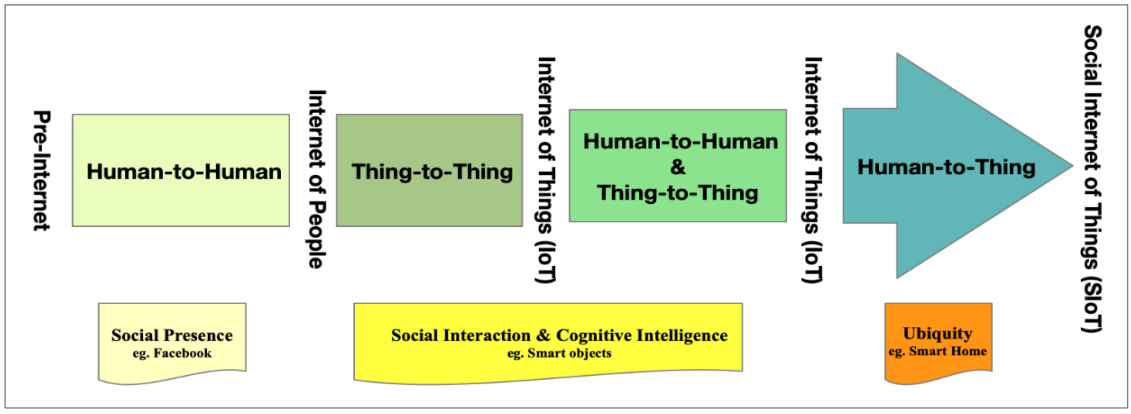


Figure 1. Evolution of SIoT.

In recent years, we have observed a proliferation of comprehensive reviews exploring diverse aspects of trust management within the SIoT paradigm, as evidenced by notable studies such as [15–18]. However, certain surveys, like Imran et al.'s [19], concentrated solely on the reliability of data dissemination in SIoT concerning security and privacy. Moreover, other notable contributions, like the commentary on features in SIoT by authors in [20], expounded on functional protocols and frameworks. In a similar vein, [21] enumerated emerging research and technologies in SIoT, culminating in a proposed design pattern.

Furthermore, Atzori et al. [22] conducted a statistical analysis examining social hierarchies, relationships, and mobility within SIoT entities, subsequently proposing a preliminary framework for ubiquitous computing in this domain. Despite the absence of a comprehensive convergence on all issues within SIoT to date, the prevailing focus in publications has been on security, privacy, and trust [22]. Additionally, some educational resources, like [23] and [24], have delved into areas covering architecture and its components, social connections, trust administration, and navigational aspects.

One of the less explored facets within SIoT pertains to the application of big data techniques for database collection and management. The significance of this issue becomes evident when users rely on self-establishment for accurate content and data installation within SIoT. Saura et al. [25] conducted a literature review focused on privacy within SIoT, examining five key areas: (i) data collection and privacy, (ii) security, (iii) threats, (iv) performance requirements, and (v) big data processing and analytics. Similarly, Amin et al. [26] conducted a comprehensive review across six pivotal areas of SIoT, encompassing service composition, navigability, framework design and its components, relationships, and trust. They offered an extensive analysis of SIoT's integration with big data and cloud computing technologies. However, we contend that certain emerging research contexts, such as cloud and fog computing, along with fault tolerance, remain relatively unexplored in prior works.

So far, our observation indicates a lack of comprehensive exploration into generic SIoT reference architecture and pivotal challenges. Most existing reviews have overlooked the interconnected facets of SIoT, neglecting crucial elements like platform dynamics, network navigability, scalability, clustering, cloud/fog computing, and fault tolerance. To bridge this gap, we propose a comprehensive survey encompassing these aspects of SIoT. Our paper's key contributions can be summarized as follows:

- In-depth exploration: we dissect unconventional SIoT patterns, offering fresh perspectives on its evolution and operational dynamics, which were previously underexplored.
- Holistic framework: by detailing nine core aspects of SIoT, our work provides a scaffold for future research, bridging gaps in architecture, trust management, and more.

- Focused analysis: our targeted evaluation of fault tolerance, cloud–fog computing, and clustering fills critical research voids, setting a new direction for SIoT studies.
- Statistical insights: via comparative analysis, we unveil trends and advancements, offering a quantifiable measure of progress in SIoT research.
- Strategic outlook: we identify pressing challenges and propose innovative solutions, guiding both academics and practitioners toward impactful future contributions.

The subsequent sections of this paper unfold as follows: Section 2 delves into methodologies and outlines the criteria employed for paper selection. Section 3 offers an exploration of various papers to unveil key aspects and a comprehensive taxonomy within SIoT. Section 4 delves into open discussions surrounding SIoT, shedding light on pertinent topics. Section 5 scrutinizes the challenges and potential directions, providing a thorough analysis. Finally, Section 6 draws conclusions that encapsulate the findings and contributions put forth in this paper.

2. Methodology

While the concept of SIoT has been present in academic literature for some time, certain interconnections within its domains remain relatively limited. Addressing this void, a systematic literature review has been undertaken to comprehensively elucidate the essence, originality, challenges, and emergent themes of SIoT, encompassing both theoretical and empirical dimensions. This meticulous approach aims to aggregate knowledge regarding novel subjects (e.g., [27,28]). In pursuit of this objective, researchers leverage past authoritative contributions to devise a theoretical conceptualization of the research landscape, proposing theoretical assertions for future exploration. Within the purview of scientific review, hypotheses are tested, and subsequent analyses seek statistical relationships among pertinent variables or constructs within models [29].

Our investigation unfolded as follows: Initially, we conducted an analysis of the theoretical underpinnings of concepts, selecting the most pertinent scientific literature within this domain [30]. This process involved prioritizing research questions and defining criteria to filter results based on relevance. Subsequently, we delved into articles published between 2011 and April 2023 across prominent International Science Indexing publications, excluding irrelevant descriptions to elucidate the fundamental structure of SIoT [31]. Our search spanned six international digital databases, namely ScienceDirect, IEEE Xplore, Springer, ACM, Wiley, and MDPI, as detailed in Table 2 with corresponding online URL addresses.

To retrieve the most relevant articles, our search phrase combined consistent terms with correlated elements [32]. Specifically, our search strings included "Social Internet of Things," "Social IoT," and "SIoT" coupled with related terms like "trust," "relationship," "architecture," "service discovery," "cloud/fog computing," and "Fault Tolerance." These searches employed logical AND combinations between consistent terms and logical OR between correlated elements or their synonyms.

Our paper selection process commenced with an initial assessment of titles, keywords, and abstracts to exclude studies not aligned with the research topic. Subsequently, we conducted an extensive analysis, emphasizing applications, to pinpoint articles suitable for inclusion. Lastly, our filtration process rigorously applied specific criteria to exclude irrelevant articles, considering parameters such as publication between 2011 and April 2023, relevance to SIoT or IoT, high-quality analytical approaches focused on key domains, accessibility to full-text content, use of the English language, publication in ISI indexed journals, and the presentation of a survey or systematic literature review that examined SIoT analytically and statistically.

Figure 2 illustrates the distribution of SIoT articles across various publishers from 2011 to April 2023. Notably, the absence of articles from Wiley in this dataset reflects the specific focus and selection criteria of our review, which prioritized sources with a direct

emphasis on SIoT research. This exclusion does not diminish the value of potential contributions from Wiley but highlights the scope and direction of our systematic literature review.

Table 2. Involved electronic databases.

Online Library	URL Address
ScienceDirect	www.sciencedirect.com (accessed on 22 February 2024)
IEEE Xplore	www.ieeexplorer.ieee.org (accessed on 22 February 2024)
Springer	www.links.springer.com (accessed on 22 February 2024)
ACM	www.dl.acm.org (accessed on 22 February 2024)
Wiley	www.onlinelibrary.wiley.com (accessed on 22 February 2024)
MDPI	www.mdpi.com (accessed on 22 February 2024)

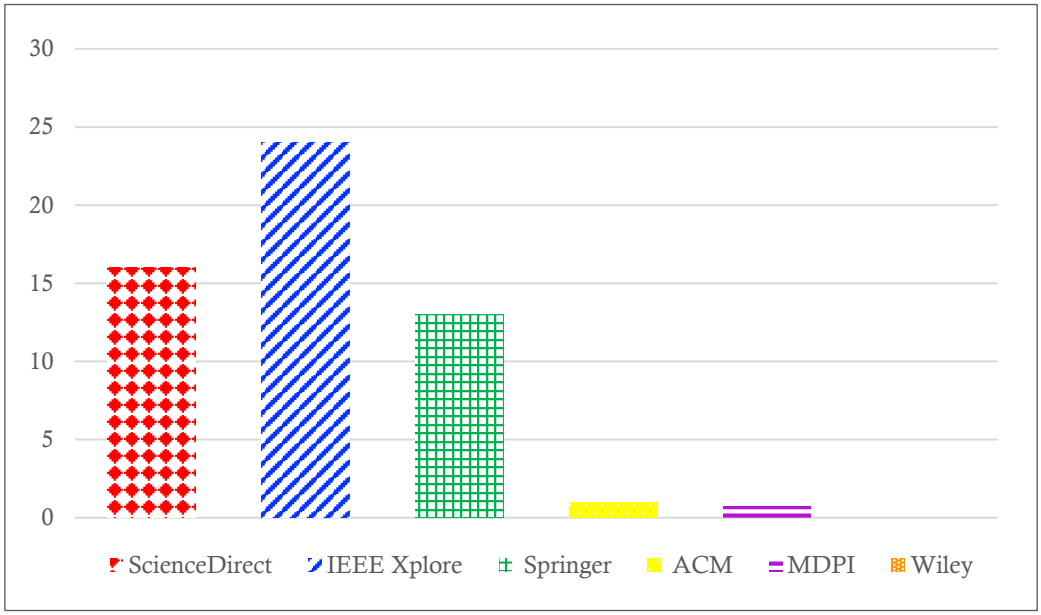


Figure 2. Number of articles in publishers from 2011 to April 2023.

3. Proposed Architecture Pattern for SIoTs

In striving for a more harmonious system within the realm of SIoTs, the reference model must align with a broad spectrum of requirements. In this section, we present our proposed architecture pattern designed to meet these imperative prerequisites. Building upon the discussion of key fundamental modules in SIoT from Section 4, we introduce the fundamental elements within the proposed SIoT architecture pattern, as visually depicted in Figure 3:

- SIoT service discovery;
- Social virtual entity (SVE) storage;
- SVE resolution;
- Relationship management (RM);
- Relationship behavior (RB);
- Monitoring.

In order to introduce a pattern for objects' interaction, we obtained the motivation of human social relations. Before this time, many researchers in the field of sociology examined human social attitudes, developed relationship theories, and recognized a variety of types of human interaction with details.

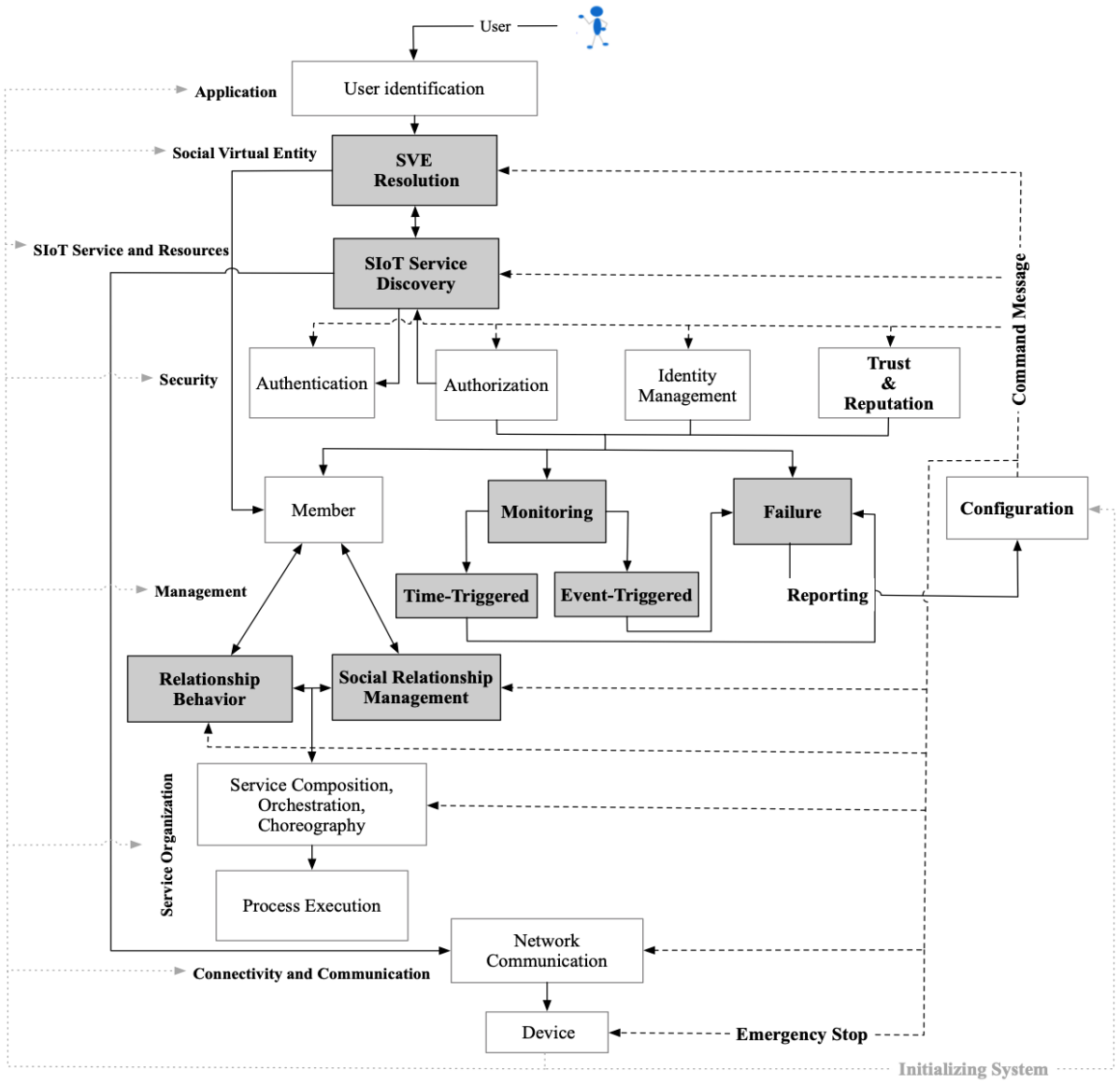


Figure 3. Proposed architecture pattern for SIoT.

3.1. Resolution of Social Virtual Entities

This component furnishes users with essential features and information required to establish a connection between the SVE and SIoT services. Within this context, the information encapsulated within the virtual social entity includes SIoT ID, service types (such as informational or activation-based), location details, and more. Operating at an abstract level, this feature embodies the digital counterpart of physical entities within the SVE. The interrelation between SVEs and services is crucial. Services act as gateways facilitating access to information associated with physical entities via resources tied to each service.

The SVE service specification orchestrates this connection between an SVE and the service, exploring the compatibility of characteristics between the social virtual service and the SVE. This endeavor often involves uncovering novel and predominantly dynamic connections between the SVE and its associated services. In this process, aspects like eligibility, location, proximity, and other contextual cues are factored in for the discovery operation. If no existing connection is found, a new one is established. Users have the option to subscribe or unsubscribe to receive continuous reports regarding suitable connections based on the characteristics of the virtual social entity or other services. Upon

receiving a report, a corresponding function is invoked. Similarly, users can opt to subscribe or unsubscribe from receiving search reports from SVE services—services that exhibit SVE resources.

Furthermore, this component facilitates communication management, offering functionalities such as the insertion, deletion, and updating of communication links between the SVE and SIoT entities associated with it. The SIoT service monitoring component plays a vital role in autonomously discovering new connections, subsequently incorporating them into the virtual entity separation component. These new connections stem from existing connections, service descriptions, and information pertaining to the SVE, enriching the ecosystem of interactions within the SIoT environment.

3.2. Repository of Social Virtual Entity

SVE embodies a digital rendition of a physical entity within the control phase, functioning via mapping and discovery mechanisms utilizing predictive identifiers. The concept of digital counterparts within SIoT platforms stems from cloud/fog computing. These virtual profiles of devices serve several roles at the application layer:

- Housing metadata pertaining to physical devices, offering detailed semantic descriptions that aid service discovery amidst device diversity.
- Enhancing the functionalities of resource-constrained devices.

In practice, SVEs reside in remote cloud–edge storage, distinct from the physical devices, devoid of resource limitations in terms of computing, storage, or power. Although virtual representations exist at the application layer, locating an SVE at the network control stage is imperative for implementation purposes. The SVE inherits advantages akin to a virtual entity (VE). However, unlike a VE, primarily an application layer process, an SVE is essentially a simpler data structure emerging from the network control phase, containing SIoT device information. Specifically, an SVE is a "social" virtual representation, maintaining connections with devices in a friendship relationship with the represented device. This is achieved via the SVE's friends table, housing entries for each friend's device.

3.3. Relationship Behavior

Alan Fisk, an American anthropologist, investigated mankind relations and its cultural changes. He developed a theory based on a relational pattern in which individuals' social behaviors are shaped on the basis of four elementary relational models [4]. In order to apply human interaction patterns (CS, EM, AR, and MP) to objects' social behavior, observing pervasive application topologies as well as foreseeing inter-object communication is necessary.

By implementing Fiske's theory, doubtlessly, the individuality of shared objects will be sacrificed for services provided to users. The principles of this theory of interaction are summarized in Table 1. For instance, some engaged interactions are in an "au pair" manner so that each object carries its own service to the community. In the first step, the object must search for the type of relationship (OOR, C-LOR, C-WOR, POR, or SOR) that it serves with other objects. Then, it will be able to interact based on the pattern of the social relation (CS, EM, AR, or MP). In order to select the most appropriate relationship types and then optimize the service discovery, a hierarchical set of relationships compatible with the requested service is proposed. This method improves the chance of optimum servicing according to specified parameters.

3.4. Failure

This component is outlined by typically making a detailed drawing of high-level system goals and fault tolerance, which is required to rule a SIoT. In order to decrease expenses, a way is to put aside dissimilar needs and parameterize the system plan [16]. Nevertheless, even with identical users, unanticipated actions may appear, like a sudden crash

in SIoT devices, connection failure, and overhead in a chain, which are very common due to the low reliability of equipment. In order to lessen these situations' effects, this component should have a precise inspection of the environment. In addition, to confront unexpected behavior of SIoT devices, some measures such as forecasting potential failure, discovering available failure, diminishing negative impacts, and restoring should be taken. The responsibility of fault administration is categorized into three default functions: response to fault discovery by disseminating alarms to all involved components, logging the history of faults, and managing to correct undesirable behaviors. To this aim, this function inspects for fault and, whether necessary, generates a chain of actions to defy a problem either by changing or setting its state back to a previous healthy condition.

3.5. Configuration

This component is in charge of system initialization, such as assigning the introductory value and assembling and also storing the configuration of different functions and elements. Furthermore, it is accountable for tracking current configuration changes as well as predicting future extensional design in the system. As such, the main roles of this function are set configuration and retrieve configuration, which is responsible for authorizing the state and recouping the system.

3.6. Member

This component has supervisory control over membership and entity-relevant information. Generally, it is about creating a database to store entities related information and operates in close collaboration with the security of the system. By default, two roles are assumed for this component: Updating members' status and a member recovery function.

3.7. Reporting

This component covers communication over other management components and summarizes the information. The implicit capability of this function is keeping system health under tight observation by gathering and examining its performance data. By developing this issue, the expectation of future states becomes feasible. The only defined role of this function is reporting retrieval, which produces reports of the system.

3.8. Monitoring

This component monitors and diagnosticates the condition of the SIoT system at a particular time. Like the fault component, for the prompt anticipation of the system, the realization of past, present, and future performance is necessary. Observation includes a behavioral performance that drives the system to a unique or set of states. The rationale is that, whereas some malicious applications may intrude on the system unexpectedly, this function has to put the system under constant intense scrutiny and inspect the consistency of alteration command. While spotting disorders, it disseminates the sequence of orders to modify the configuration. The observatory system up-to-date trust scores by employing the two following scenarios:

- The periodic time-triggered: trust value is renovated per regular time interval, rather than seeking for an incident.
- The reactive event-triggered: upon the occurrence of an event, for example, a new individual entry or the initiation or termination of a transaction, the trust value is reconstructed for that specific node.

4. Fundamental Key Modules of SIoTs

As highlighted in the preceding section, we delineated a comprehensive taxonomy detailing the foundational components within the construct of SIoT [33]. Illustrated in Figure 4, the pivotal elements of SIoT are systematically categorized into nine distinct realms:

SIoT architecture, trust management, relationship management, navigability, friend selection, service discovery, fault tolerance, cloud–fog computing, and clustering techniques. Each category signifies the chronological progression of studies or their significance in relevant public events, as outlined in the subsequent subsections. This depiction offers a comprehensive overview of the evolution and relevance of each aspect within the SIoT landscape.

In our extensive literature review, summarized in Table 3, we present a comparative analysis of recent works against our survey, shedding light on various dimensions of SIoT, including architecture, trust management, relationship management, navigability, friend selection, service discovery, fault tolerance, and cloud–fog computing. This table highlights the advancements and gaps within these areas across selected studies. For instance, while studies by [26,34] and [35] offered significant insights into relationship management, they did not fully explore the nuances between friend selection and relationship management. Moreover, [23] provided an in-depth look into object social ties and trust patterns within SIoT, yet their coverage of critical aspects such as fault tolerance, network navigability, service discovery, and cloud–fog computing remained limited. Our survey, in contrast, aims to bridge these gaps by offering a comprehensive examination across all these dimensions. Our analysis reveals a pressing need for more holistic approaches in SIoT research that address these underexplored areas, thereby fostering a more robust and interconnected SIoT ecosystem.

Table 3. Comparative analysis of SIoT components in recent literature.

Ref.	Year	SIoT Architecture	Trust Management	Relationship Management	Navigability	Friend Selection	Service Discovery	Fault Tolerance	Cloud–Fog Computing
[19]	2019	✓	×	✓	✓	✓	✓	×	×
[23]	2020	×	×	×	✓	×	✓	✓	×
[24]	2019	✓	×	×	×	×	×	×	×
[25]	2021	✓	×	×	✓	✓	×	✓	✓
[26]	2022	×	×	×	×	✓	×	✓	×
[35]	2021	✓	✓	×	×	×	✓	✓	✓
[36]	2020	✓	✓	✓	×	✓	✓	×	×
[37]	2021	✓	×	✓	✓	✓	✓	×	×
[38]	2016	✓	×	✓	✓	✓	✓	×	×
[34]	2022	×	×	×	×	✓	×	✓	✓
This study		✓	✓	✓	✓	✓	✓	✓	✓

✓ indicates the component is discussed in the referenced study. × indicates the component is not discussed in the referenced study.

In Table 3, the "✓" symbol indicates the presence or positive evaluation of the component within the referenced SIoT architecture, while the "×" symbol denotes the absence or negative evaluation of the component. This notation provides a succinct overview of how each referenced work contributes to the various facets of SIoT.

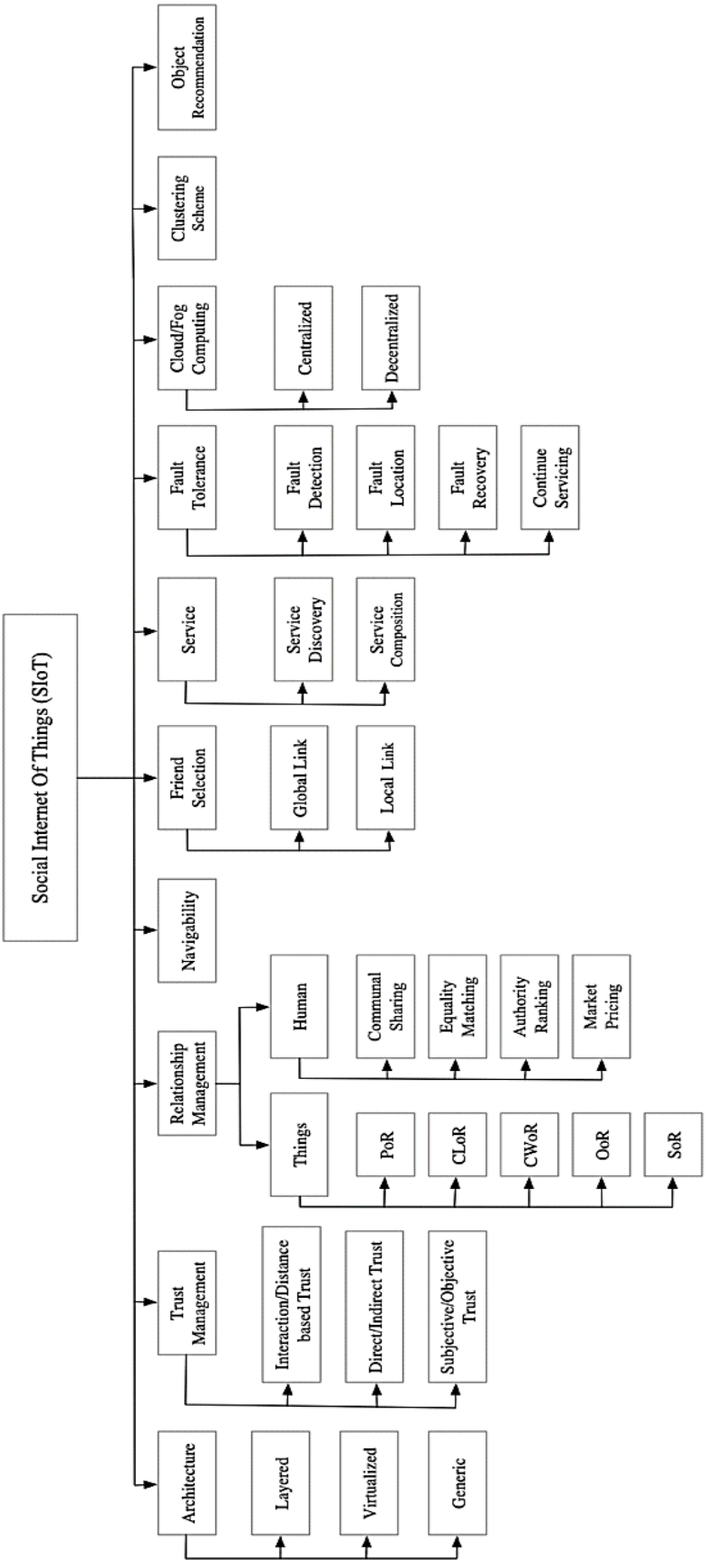


Figure 4. Taxonomy of key components in SIoT structure.

4.1. Service Requirement in SIoTs

Service diagnosis empowers objects to autonomously acquire required services for their owners. This process facilitates inter-object relationships, allowing previously independent or newly added objects to collectively analyze and process data. Consequently, they can automatically identify an object that aligns with the specific request. Service composition forms an ecosystem where intelligent objects and their corresponding data engage with the most suitable friend category, aided by refined friend selection algorithms. This involves establishing social ties between entities, whether human or objects, seeking to offer services. Upon broadcasting the query among nearby entities, they analyze it using their available services or nearby objects, considering preferences and backgrounds. Subsequently, a set of relevant objects exhibiting the most compatible quality of service is directed to the requester. In the upcoming section, we delve deeply into the latest and most innovative papers in this field of study.

Nitti et al. [38] explored the concept of establishing distributed social friendships as a means to achieve scalability. Addressing the deficiencies in social ties and enhancing service composition within SIoT, Dhelim et al. [8] leveraged artificial intelligence derived from social computing. Farahbakhsh et al. [16] delved into this issue by employing trust mechanisms and modules for evaluating relationships, performance, and global reputation alongside punitive measures. Their approach included identifying greedy nodes and calculating trust based on the desires of faithful nodes. In a novel social-like semantic approach within IoT, Xia et al. [39] introduced a non-centralized inspection method using similarity and fuzzy algorithms to assess the type of connections.

In addressing resource discovery within SIoT, Fan et al. [40] proposed an optimal searching algorithm, broadening connectivity in heterogeneous information networks to gauge cohesiveness. Stelea et al. [41] applied SIoT definitions to construct heritage services, employing a trust-based approach to devise a model for service composition and provisioning. Their three-layered pattern segments trust into social perception, topology, and service features.

4.2. Navigability

Network navigability is a constitutional aspect for queries in SIoT, which indicates the existence of a short, direct route via almost every pair of nodes for communication [42]. The SIoT is a network of many objects, which are generally connected in a friendly manner based on social relationships, their characteristics, and profile information. Due to the abundance of issues, the friend selection procedure evoked an extra assessment cost and fallen network productivity [43]. Some advanced algorithms for the shortest path and navigability are explored below. Nitti et al. [44] explained five heuristics of local link choice to establish proper social relations per node for SIoT navigability and scalability as well. But they did not consider trust management for honest friend selection. They specified a certain number of ties for each node, and any increase in their numbers resulted in a longer path among nodes.

Amin et al. [45] arrived at network navigability by the small-world phenomena. For link selection, they employed the policy of an old mutual links removal based on trust metrics. However, not concerning trust for navigability and the static threshold for link selection are drawbacks in their strategy. Amin et al. [34] presented a distributed service query in which the SIoT objects utilize centrality and the friends of friends' information to find neighbors and hence guarantee the scalability. To further improve the concept of navigability in the small world, Amin et al. [46] initiated the service query in various hops by sending a request to the closest node upon service requirement. This search procedure was repeated until the identification of the target node and the establishment of a permanent linkage between the requester and the provider.

Typically, Ramasamy et al. [47] proposed a heuristics link choice per object. They discussed a strategy for the old mutual friend removal without taking trust metrics. To

achieve navigability in SIoT, Rajendran et al. [48] suggested recommendation-based tie picking. They took advantage of trust and modeled using the contentment rating and SOR-based grey wolf algorithm. Although the model was simulated on two real-world datasets, using only an undirected graph is the weakness of this study. Pashaei et al. [49] embedded the learning automata for influential node selection in the SIoT and chose the next-hop neighbor by high centrality. Then, they claimed a well-navigable SIoT, and the searching process was settled in a short time.

Atzori et al. [50] assimilated social properties into IoT and defined social relationship characteristics for navigability. Although there was inadequacy for the practical architecture of SIoT and its functionalities, they defined space possibility issues of related objects, that is, OOR by a power-law distribution, SOR in the tiny-scale by a power-law and large-scale by the exponential distribution, and CWOR by a gamma behavior. They supposed the distance in the CLOR is insignificant, and that POR is not reliant on distance. Their advantageous achievement lights a candle for future analysis and maintaining these relations, for instance, in [42].

4.3. SIoT Architecture

While there is not yet a consistent architecture for SIoT, most publications exploited a three-layer model, including the base layer with a storing database on ontologies, linguistic engine, and transmission. The intermediate ground cares for the object-to-object, tie-to-tie, or object-to-tie transactions, and the upper layer is dedicated to human participation in applications by transaction among discrete items with SIoT server for the sketch and fellowship reformation and service query [24].

The fundamental SIoT architecture was introduced by Atzori et al. [22,51] in the three-tier diagram: (1) the physical, (2) the network, and (3) the application layer. The bottom layer includes "things" aware of the dynamic SIoT infrastructure. The second domain includes digital pairs of sensing things by similar communal aptitudes. They act as an interface between attached devices and process the data from the bottom to the top service surface. The application execution is lodged in the cloud area and responds to the social agent functions such as service delivery, authorization, profiling, and friend selection based on trust rate. However, this basic solution created disadvantages as given below:

- Centralized trust management on the SIoT server.
- There was a lack of a centralized storage area or distributed trust evaluation unit.
- Transmission traffic from the sensing machine to SIoT administration across the network layer.
- Occurrence of a single point of failure by cause of consolidated trust element.

To tackle these problems, Mohammadi et al. [42] spread trust functionality over all the layers. Nonetheless, some deficiencies, such as local collaboration, continuous interaction to form the CLoR, CWoR, and SoR ties, and reliability evaluation, remain unsolved in their semi-centralized SIoT trust approach.

4.4. Relationship Management

Various types of intelligent relationships have given rise to numerous things and humans who work at the same time or places [52] by concerning the profiles, motions, and preferences. Below are the inferred precedence and object interpretation for different relationships [36]:

- Co-location object relationship (CLoR): forms between objects situated in close proximity or at the same physical location.
- Co-work object relationship (CWoR): emerges when objects collaborate to accomplish shared tasks or objectives.
- Parental–object relationship (PoR): occurs between objects originating from the same production batch or manufacturer.

- Social–object relationship (SoR): develops when objects interact sporadically or regularly with each other.
- Ownership (OoR): establishes connections among diverse objects possessed by a single user.

The relationship concept yields a community-based manner paradigm [53] in which objects are empowered by common characteristics to recognize each other and, hence, easily make/terminate social links [28]. For instance, due to the distributed essence of SIoT in [54], objects received more responses to queries than in a traditional IoT environment. Mohammadi et al. [42] chose the properties of social relationships so that they comply with SIoT navigability. The authors demonstrated the dependence of relationships typology with links distance probability distribution. Wu et al. [55] drew an architecture for a definition of the cognitive internet of things (CIoT). Then, Kassis et al. [56] presented a relationship pattern for the cognitive IoT by conceptual and intelligent web software agents. Despite a theoretical prototype by an illustration scenario, the datasets were not verified. Wu et al. [57] studied machine learning for the choice of a social group by triple matrix construction, feature extraction, and community identification.

4.5. Trust Management

A multifaceted property in the SIoT paradigm is dedicated as an exclusive alternative while cryptography solutions are ineffective or unavailable to guarantee system reliability in case of malicious intruders' disturbance. In an (S)IoT service-oriented environment, trust contributes as an inter-layer between all requester and supplier components to supervise the reliable service composition. In real life, and especially for cooperation, trust plays a role in relationship establishment. The wheel of trust in life is summarized in four phases [58]:

- Observation: collect the information on objects;
- Weigh: assign a reputation score;
- Selection: prioritize suitable objects;
- Reward/Punishment: after the transaction, gather feedback.

Nitti et al. [59] discussed the subjective and objective trust model. Subjective trust is measured by the node's own experience or the belief of its friends. The objective trust is stored in a dispersed hash table. Designing a single object is the deficiency of their model. To advance their job, Chen et al. [60] updated the trust score in the incident of affairs. The trust was estimated by first-hand monitoring α or indirect recommendation β to administrate trust propagation and aggregation as well as to improve its accuracy in dynamic situations. Talbi and Bouabdallah [61] evaluated trust values by either direct or indirect preference. To assess direct trust, a global value was calculated by preferences, and for indirect trust, we obtained the trustor's sincere recommendations from potential honest recommenders [62]. Mohammadi et al. [42] defined a trust evaluation framework based on the joint probability distribution of static trust and dynamic trust. Static or distance-based trust is calculated on all static owner variables and inferred on the Bayesian method in terms of distance X. The dynamic or interaction-based trust is calculated on the Bayesian inference of time-varying issues like relations and transactions. Table 4 depicts an analogy of the latest SIoT trust paradigms.

Marche et al. [63] strengthened and facilitated the service provision by objects' trustworthiness. In their model, the objects' major features, e.g., typology, associated functionalities, and the characteristics of the applications, were taken into account. The inquiry techniques were examined by a communal view of local and global navigability. Despite unsatisfying performance in average global path length or local routing, the authors achieved query success either in hops degree or time spent.

Table 4. Trust management in state-of-the-art SIoT environment.

Study	Model	Trust Metrics	Trust Model	Relationships
[42]	Probability distribution Function	Distance and interaction	Static and dynamic trust	PoR, OoR, CWoR, CloR, SoR
[63]	Probability distribution Function	Time and space	Global and local	All except CWoR and OoR
[59]	P2P Network	Direct and indirect	Objective and subjective	All

4.6. Friendship and Link Selection

Nitti et al. [44] declared themselves early researchers on link selection and friendship concepts in the SIoT. They perceived five heuristics for friend choice with the least local hubs, which gave rise to fruitful global navigability. To remit this obstacle, the authors lowered the central routing cost and distributed the task locally to higher-degree neighbors. Additionally, they put a threshold on the number of hubs and clustering and hence gained the shortest path with frequency division similar to the power law. However, the authors declared the benefit of the game theory friends adjustment without any negative impact on navigability. Obviously, the fixed threshold on the number of friends leads to negative impacts. The authors of [24] argued the gray wolf theory for smart node recommendation and the closeness scale for friend choice in SIoT. The method investigation by real-world datasets obtained achievements in mean space, MAE, RMSE, recall, and precision. They explored social trust via satisfaction and advocacy, which can be employed as a measure of relationships for the future.

SIoT delegated authority to the smart nodes for the creation or elimination of friendship without human intervention [64]. In addition, they can individually store information [65] and therefore obtain better navigation and more precise search mechanisms for service queries. This superiority has been fulfilled in the shadow of relationship management, but it will become tricky due to the node's growth [66]. This can be explained due to battery life and constraints in the storage area of SIoT devices, which is a scalability issue, or the destructive effect of malicious or selfish nodes, which is a navigability issue. For those reasons, ample attention to the number of each node's friends is required. The proper friend selection algorithm concerning the number, type, and rate of friendships, is of importance for SIoT sustainability. By taking into consideration all above-mentioned complications of tie classification, the authors of [42] well described a system model with an intelligent friend election strategy by exhaustive optimization search.

4.7. Fault Tolerance

Conventional IoT infrastructures somehow deteriorated with the data abundance and device heterogeneity because of power constraints or weak connectivity among devices [67]. These failures cause extreme disruptions, like information loss, recovery expenses, or latency. This complication reveals the necessity for developing fault-tolerant algorithms with the least energy consumption. Despite all advancements, there is still a remarkable absence of fault tolerance methods in SIoT. With regard to heterogeneity and numerous manufacturers of IoT devices, attaining data about failure, recovery, and troubleshooting consequences requires pervasive sources of data. This information is utilized by self-organized components for identification and recovery of faults. These autonomic components develop a fault resilient system with self-repair characteristics [68].

In [69], fault tolerance capacity was considered the first parameter among IoT management features. Given the three layers architecture of IoT, this research presented a hybrid fault tolerance in the second layer of the IoT platform (i.e., cloud computing). The authors claimed the maximum utilization of active, reactive, and preventive policies and all fault detection criteria, and the implementation of most existing strategies in the recovery phase was carried out. The proposed FCAPS architecture is implemented in both Cloudsim and Pegasus–WMS emulators. The reliability of architecture was modeled by

fuzzy logic and inference systems. In the recovery phase, the fault coverage weakness is noteworthy.

These wireless sensor nodes (WSN) are naturally susceptible to faults due to launching in an unreachable zone or restriction on expenses, leading to poor performance. The authors of [70] proposed fault management with clustering algorithms to tackle these deficiencies. All permanent and transient errors are modeled using the Markov chains by the self-diagnostic method in the detection phase. In the recovery phase, with regard to hardware flaws a new status is appointed to nodes and next retrieved. The simulation results on the fault-tolerant framework proceeded on power usage, the live nodes, accuracy, and deteriorated false alarm value. Due to the limited energy in wireless sensor devices, the biggest drawback of this architecture is the use of the weakest error detection method, namely self-troubleshooting.

In [71], the author provided an inquisitive architecture to sketch the characteristics of wireless loop control in the event of information depletion or hardware damage. A discrete-time Markov model includes basic elements such as sensor or actuator ties and recuperation to cope with their failures. The two performance criteria, namely the average input linger in management devices and the average time to fail, were defined. The performance criteria were investigated via hypothetical tests and Monte Carlo simulations. They depicted an underlying trade-off between mean activity in the regular operation of the control loop and recovery activity in abnormal operation due to faulty nodes. The optimal framework is strongly built upon measures, e.g., return sensors and connections to a healthy state, the likelihood of unsuccess in links, and the control loops. This theoretical model for optimization in multiple control systems was proposed as future work.

Casado-Vara et al. [72] estimated the dispersed continuous-time fault for various devices in IoT using a combination of participatory control and state forecast mechanism. First, a state-dependent intermediate value matrix is designed to estimate defective values of the IoT. Second, the continuous-time Markov transition matrix, called the Kolmogorov differential equation, was modeled to determine the system feedback and compare it with the output values. This provided sufficient stability to automatically correct IoT errors, replace faulty devices with virtual devices, and prevent inaccurate data collection. However, data security, confidentiality, and reliability were not considered. The authors plan to solve this problem in the future with artificial intelligence, blockchain technology, and control algorithms.

4.8. Cloud and Fog Computing in IoT

In the event of failure and crash in SDN networks with distributed low traffic, the authors of [73] introduced a multi-tiered architecture for fault handling by using fog computing. The optimized solution for rerouting and energy depletion with a small-scale network was formulated mathematically and empowered by a sub-optimal heuristic algorithm to tackle the computational complications in a large network. In terms of reliability, this study focused on fault avoidance. The performance of the two proposed algorithms was evaluated concerning average path length, link congestion, the number of fog nodes, task virtualization, the probability of failure occurrence, and reactions. They did not encompass queuing latency and power utilization in their study's edge devices and transmission links. To reduce the mentioned expenses, the unnecessary nodes will be temporarily deactivated or set to idle mode. Additionally, they decided to advance their heuristic algorithm by including the sequence of platform task virtualization.

In [74], the authors came up with a three-tiered hybrid cloud–fog-dependent architecture to schedule dynamic miscellaneous prompt IoT users. They placed various requirements with small communication overheads in the cloud servers and more communication requirements with fewer computational overheads in the fog virtual machines. However, this approach suffers the communication cost of data transmission from the IoT layer to fog and a crucial monetary expense for cloud recourses utilization. To overcome

these drawbacks, the authors offer engaging on-demand multi-tenant virtual machines rather than pre-arranged hosts in the cloud layer.

To recognize the information interaction across humans, human-to-thing, and thing-to-thing in SIoT, the authors of [75] suggested a cloud–edge collaborative dynamic information dissemination model (CCDIDM) in SIoT. By reflecting on individuals' interplays and things' information dissemination, the coupled relationship between nodes is created. Then, efficient interaction and cognition awareness of users are achieved by real-time processing as well as cloud–edge computing feedback. Abstract studies include the regulation of the parameter size to promote or inhibit the information dissemination threshold and the stability of the equilibrium point via LaSalle's invariance and the Lyapunov method. It was found that the more the perception awareness of individuals, the less the propagation scale. In the future, the authors plan to study the secure correlation of communication factors in the IoT layer as well as the delay between edge and cloud processing impact on information transmission in the SIoT.

4.9. Clustering in IoT

Power preservation and lifespan rise are two principal concerns for deploying edge-computing-based Internet of Medical Things. In this context, several approaches developed clustering techniques to obtain energy efficiency. However, they mostly suffer energy cuts due to unreliable communication protocols and packet failure during transmission. The authors of [76] developed a procedure to choose cluster head nodes based on their high remaining energy and proximity to the base station to overcome the disadvantages. They depicted the proposed model's superiority by decreasing energy utilization and increasing sustainability and lifetime using a uniform distribution of cluster heads. Nevertheless, security and multi-hop data transmission to preserve the power in medical nodes have been neglected in their research. The authors promised to develop hierarchical multiple-hop clustering algorithms to achieve security in real-time communication.

To address computing service utilization concerning energy and delay minimization in constrained IoT applications, the study by the authors of [77] explored resource allocation within hierarchical fog nodes and cloud server computing paradigms. They devised a process offloading game for user competition, establishing the presence of a pure Nash equilibrium and an upper bound for stability deficiency. To mitigate the exponentially increasing time complexity resulting from the number of users, they employed a near-perfect resource distribution strategy with polynomial achievement. The experimental analysis illustrated the achieved quality of experience, showcasing low-latency service for delay-sensitive IoT devices. The authors also suggested further exploration into online assignment techniques for dynamic task allocation and the collective designation of mass spectrum determination within cellular systems, offering promising prospects for reducing waiting periods in 5G networks.

In data clustering, there is a potent data mining technique applicable to vast data volumes in IoT sensor devices; however, there is a trade-off involving privacy risks associated with clustering methods. Bloom et al. [78] introduced a differential key–mean privacy algorithm as an efficient solution, yet its outcomes were limited due to data distortion. In this study [79], a novel clustering approach for data availability and privacy (PADC) was proposed. Leveraging the k-means algorithm and differential privacy, this method improved initial point selection and distance calculations to the center point by integrating cluster weight based on density. Additionally, it aimed to mitigate the impact of outlier detection via clustering. Performance evaluations exhibited enhanced clustering availability with a comparable privacy level compared to existing key–mean algorithms. Designing a fault-tolerant system applicable to SIoT environments remains a significant modern challenge. Future research directions include robust solutions for identifying link failures, fault tolerance in routing or service provision, device territory adaptations, and advancements in cloud and fog computing methods within SIoT.

4.10. Object Recommendation in SIoT

One significant challenge within SIoT revolves around enhancing recommendation algorithms to efficiently pair intelligent objects with users amidst vast text resources. An approach proposed by [80] tackles this challenge via an SIoT method termed Object Recommendation based on Topic Learning and Joint Object-Related Text Features (ORTJ). This approach utilizes "thing–thing" connections in IoT, evaluating the compatibility of user requirements and smart objects while considering multiple service relevance attributes and their respective weights to augment recommendation quality. The ORTJ algorithm, derived via MAP assessment, meticulously analyzes software and hardware information, potential characteristic features, relationships among smart objects, and associated descriptive texts. This results in highly accurate recommendations and fine-tuning via parameter adjustments. However, limitations arise due to the model's neglect of link information, leading to biased topic–word distribution and adversely impacting recommendations, compounded by limited user attribute richness. To address these shortcomings, the authors intend to enhance their model with user requirement profiles.

In the SIoT realm, a diverse array of smart objects shares similar responsibilities and facilitates user-friendly resource accessibility. However, effective service discovery hinges on various attributes of object centrality. In [48], an Object Recommendation based on Friendship Selection (ORFS) was proposed to manage navigability and social relationships among intelligent objects in SIoT. ORFS emphasizes trust-based social communications. The approach employs a Grey Wolf Algorithm-based User Object Affiliation (GWA-UOA) mechanism for Smarter Object Recommendation (SOR) and Object Friendship Selection (OFS) using Maximum Ranked Neighborhood (MRN) approaches for navigability. This method ultimately utilizes social-driven relationship links validated via real-world datasets. Empirical findings demonstrate ORFS's performance for navigating smart social objects within SIoT, showcasing metrics such as MAE, RMSE, computation time, average path length, recall, precision, and F1 score.

5. Analysis of Challenges and Directions

Heterogeneity: Within the vast realm of SIoT, a plethora of diverse objects, each with distinct standards and features, pose a substantial challenge in achieving interoperability and compatibility. Creating relationships such as PoR can guarantee uniformity, while additional interfaces or identification policies can bolster consistent functionality among objects sourced from different manufacturers [81,82].

Dynamicity and Mobility: The dynamic behavior inherent in both smart objects and the SIoT environment itself leads to frequent changes in network status. To address this dynamism, owners must dedicate efforts to maintain network topology stability and ensure adaptability. Moreover, objects consistently change locations and behavior, prompting the formation of relational communities in SIoT based on distinguishing features, movements, or shared social interests. Schemes based on location or interactions employ functions like probability distribution [42], Euclidean metrics, or adjacency matrices to adapt their positions [83].

Resource Constraints: SIoT devices, constrained by energy limitations, impact the network's longevity, yet their mobile nature enhances computational power. Mohammadi et al. [42] introduced a trustworthy friend selection algorithm aimed at optimizing variables to reduce energy consumption during the service discovery process in SIoT. However, effective remedies such as fault tolerance mechanisms, clustering, and distributed computing are still lacking to alleviate this predicament [54,84].

Security and Privacy: The limited processing power and storage capacity of SIoT devices render them susceptible to attacks. The heterogeneous, dynamic, and complex infrastructure of SIoT further exposes vulnerabilities. In response, researchers recommend employing cost-effective, self-synchronizing end-to-end encryption models [85]. Additionally, securing communication protocols to trace components is essential. Techniques such

as access control, secure data sharing, trust management, and predicting object attitudes based on community relations [86] need to be prioritized, ensuring higher levels of privacy protection for real identities from disruptions.

Scalability and Navigability: Challenges in service discovery and friend selection impose burdens on the SIoT environment. Implementing effective local/global detection algorithms or community creation based on similarity measures can substantially reduce intra/inter-community transaction times and enhance network flexibility [87].

Smart Object Recommendation: The underutilization of extensive textual information poses unresolved challenges. The reference data within SIoT, derived from human interactions and vast data sources, including comments generated during socialization or interactions with smart IoT objects, remain largely untapped. These data, encompassing both structured (user profiles) and unstructured (rich texts related to intelligent objects) factors, hold immense potential for enhancing the SIoT recommendation system. Furthermore, the heterogeneous nature of IoT objects, characterized by diverse traits, levels, protocols, standards, and features, poses significant limitations.

6. Conclusions

To conclude our comprehensive examination of the Social Internet of Things (SIoT), we affirm the transformative potential of integrating socialization principles into IoT. Our systematic review illuminates the path forward by identifying pivotal yet underexplored domains such as fault tolerance, cloud–fog computing, and clustering. The taxonomy developed via our analysis not only clarifies the current landscape of SIoT research but also highlights significant gaps that must be addressed to advance the field. As we chart future research directions, it is imperative that forthcoming studies delve into these identified areas to enhance the robustness, efficiency, and scalability of SIoT systems. Our findings underscore the necessity for continued innovation and exploration to realize the full potential of SIoT in connecting devices and facilitating interactions with a level of social intelligence akin to human networks.

Author Contributions: Conceptualization, J.L.; Methodology, M.H. and J.L.; Formal analysis, M.H.; Investigation, V.N.; Resources, V.N.; Data curation, V.N.; Writing—original draft, V.M. and V.N.; Writing—review & editing, M.H. and J.L.; Visualization, V.N.; Supervision, Mehdi Hosseinzadeh; Project administration, M.H. and J.L.; Funding acquisition, J.L. All authors have read and agreed to the published version of the manuscript.

Funding: The result was created through solving the student project "Security analysis and developing lightweight ciphers and protocols" using objective oriented support for specific university research from the University of Finance and Administration, Prague, Czech Republic.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Acknowledgments: Authors thank Michal Merta, and Zdeněk Truhlář for their help with the research connected with the topic of the article.

Conflicts of Interest: We declare that this manuscript is original, has not been published before, and is not currently being considered for publication elsewhere.

References

1. Khanna, A.; Kaur, S. Internet of things (IoT), applications and challenges: A comprehensive review. *Wirel. Pers. Commun.* **2020**, *114*, 1687–1762.
2. Khelloufi, A.; Ning, H.; Dhelim, S.; Qiu, T.; Ma, J.; Huang, R.; Atzori, L. A social-relationships-based service recommendation system for SIoT devices. *IEEE Internet Things J.* **2020**, *8*, 1859–1870.
3. He, P.; Tang, T. Community-oriented multimedia content maximization mechanism in social Internet of Things. *IEEE Access* **2020**, *8*, 22826–22833.
4. Fiske, A.P. The four elementary forms of sociality: Framework for a unified theory of social relations. *Psychol. Rev.* **1992**, *99*, 689.

5. Holmquist, L.E.; Mattern, F.; Schiele, B.; Alahuhta, P.; Beigl5, M.; Gellersen, H.W. Smart-its friends: A technique for users to easily establish connections between smart artefacts. In *Ubicomp 2001: Ubiquitous Computing: International Conference, Atlanta, GA, USA, 30 September–2 October 2001*; Proceedings 3; Springer: Berlin/Heidelberg, Germany, 2001; pp. 116–122.
6. Ali, O.; Ishak, M.K.; Bhatti, M.K.L. Emerging IoT domains, current standings and open research challenges: A review. *PeerJ Comput. Sci.* **2021**, *7*, e659.
7. Aman, A.H.M.; Yadegaridehkordi, E.; Attarbashi, Z.S.; Hassan, R.; Park, Y.J. A survey on trend and classification of internet of things reviews. *IEEE Access* **2020**, *8*, 111763–111782.
8. Dhelim, S.; Ning, H.; Farha, F.; Chen, L.; Atzori, L.; Daneshmand, M. IoT-enabled social relationships meet artificial social intelligence. *IEEE Internet Things J.* **2021**, *8*, 17817–17828.
9. Zhu, T.; Dhelim, S.; Zhou, Z.; Yang, S.; Ning, H. An architecture for aggregating information from distributed data nodes for industrial internet of things. In *Cyber-Enabled Intelligence*; Taylor & Francis: Abingdon, UK, 2019; pp. 17–35.
10. Kleinberg, J.M. Navigation in a small world. *Nature* **2000**, *406*, 845–845.
11. Kleinberg, J. The small-world phenomenon: An algorithmic perspective. In Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, Portland, OR, USA, 21–23 May 2000; pp. 163–170.
12. Militano, L.; Nitti, M.; Atzori, L.; Iera, A. Enhancing the navigability in a social network of smart objects: A shapley-value based approach. *Comput. Netw.* **2016**, *103*, 1–14.
13. Ahmed, N.M.; Chen, L. An efficient algorithm for link prediction in temporal uncertain social networks. *Inf. Sci.* **2016**, *331*, 120–136.
14. Yao, L.; Sheng, Q.Z.; Ngu, A.H.; Li, X. Things of interest recommendation by leveraging heterogeneous relations in the internet of things. *ACM Trans. Internet Technol. (TOIT)* **2016**, *16*, 1–25.
15. 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.
16. Farahbakhsh, B.; Fanian, A.; Manshaei, M.H. TGSM: Towards trustworthy group-based service management for social IoT. *Internet Things* **2021**, *13*, 100312.
17. Shirvani, M.H.; Masdari, M. A survey study on trust-based security in Internet of Things: Challenges and issues. *Internet Things* **2023**, *21*, 100640.
18. Liu, Y.; Wang, J.; Yan, Z.; Wan, Z.; Jäntti, R. A survey on blockchain-based trust management for Internet of Things. *IEEE Internet Things J.* **2023**, *10*, 5898–5922.
19. Imran, M.; Jabbar, S.; Chilamkurti, N.; Rodrigues, J.J. Enabling technologies for social Internet of Things. *Future Gener. Comput. Syst.* **2019**, *92*, 715–717.
20. Rho, S.; Chen, Y. Social Internet of Things: Applications, architectures and protocols. *Future Gener. Comput. Syst.* **2018**, *82*, 667–668.
21. Ortiz, A.M.; Hussein, D.; Park, S.; Han, S.N.; Crespi, N. The cluster between internet of things and social networks: Review and research challenges. *IEEE Internet Things J.* **2014**, *1*, 206–215.
22. Atzori, L.; Iera, A.; Morabito, G. Siot: Giving a social structure to the internet of things. *IEEE Commun. Lett.* **2011**, *15*, 1193–1195.
23. Malekshahi Rad, M.; Rahmani, A.M.; Sahafi, A.; Nasih Qader, N. Social Internet of Things: Vision, challenges, and trends. *Hum. Centric Comput. Inf. Sci.* **2020**, *10*, 1–40.
24. Roopa, M.S.; Pattar, S.; Buyya, R.; Venugopal, K.R.; Iyengar, S.S.; Patnaik, L.M. Social Internet of Things (SIoT): Foundations, thrust areas, systematic review and future directions. *Comput. Commun.* **2019**, *139*, 32–57.
25. Saura, J.R.; Ribeiro-Soriano, D.; Palacios-Marqués, D. Setting privacy "by default" in social IoT: Theorizing the challenges and directions in Big Data Research. *Big Data Res.* **2021**, *25*, 100245.
26. Amin, F.; Majeed, A.; Mateen, A.; Abbasi, R.; Hwang, S.O. A systematic survey on the recent advancements in the Social Internet of Things. *IEEE Access* **2022**, *10*, 63867–63884.
27. Neilson, A.; Daniel, B.; Tjandra, S. Systematic review of the literature on big data in the transportation domain: Concepts and applications. *Big Data Res.* **2019**, *17*, 35–44.
28. Saura, J.R.; Palacios-Marqués, D.; Iturricha-Fernández, A. Ethical design in social media: Assessing the main performance measurements of user online behavior modification. *J. Bus. Res.* **2021**, *129*, 271–281.
29. Madakam, S.; Lake, V.; Lake, V.; Lake, V. Internet of Things (IoT): A literature review. *J. Comput. Commun.* **2015**, *3*, 164.
30. Al-Jarrah, O.Y.; Yoo, P.D.; Muhaidat, S.; Karagiannidis, G.K.; Taha, K. Efficient machine learning for big data: A review. *Big Data Res.* **2015**, *2*, 87–93.
31. Martinez, I.; Viles, E.; Olaizola, I.G. Data science methodologies: Current challenges and future approaches. *Big Data Res.* **2021**, *24*, 100183.
32. Ribeiro-Navarrete, S.; Saura, J.R.; Palacios-Marqués, D. Towards a new era of mass data collection: Assessing pandemic surveillance technologies to preserve user privacy. *Technol. Forecast. Soc. Change* **2021**, *167*, 120681.
33. Saura, J.R.; Ribeiro-Soriano, D.; Palacios-Marqués, D. From user-generated data to data-driven innovation: A research agenda to understand user privacy in digital markets. *Int. J. Inf. Manag.* **2021**, *60*, 102331.
34. Amin, F.; Hwang, S.O. Automated Service Search Model for the Social Internet of Things. *Comput. Mater. Contin.* **2022**, *72*, 5871–5888.
35. Farhadi, B.; Rahmani, A.M.; Asghari, P.; Hosseinzadeh, M. Friendship selection and management in social Internet of Things: A systematic review. *Comput. Netw.* **2021**, *201*, 108568.
36. Wang, C.H.; Kuo, J.J.; Yang, D.N.; Chen, W.T. Collaborative social Internet of Things in mobile edge networks. *IEEE Internet Things J.* **2020**, *7*, 11473–11491.

37. 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.
38. Nitti, M.; Murroni, M.; Fadda, M.; Atzori, L. Exploiting social internet of things features in cognitive radio. *IEEE Access* **2016**, *4*, 9204–9212.
39. Xia, H.; Hu, C.Q.; Xiao, F.; Cheng, X.G.; Pan, Z.K. An efficient social-like semantic-aware service discovery mechanism for large-scale Internet of Things. *Comput. Netw.* **2019**, *152*, 210–220.
40. Fan, X.; Li, Y.; Sun, J.; Zhao, Y.; Wang, G. Effective and efficient Steiner maximum path-connected subgraph search in large social Internet of Things. *IEEE Access* **2021**, *9*, 72820–72834.
41. Stelea, G.A.; Popescu, V.; Sandu, F.; Jalal, L.; Farina, M.; Murroni, M. From things to services: A social IoT approach for tourist service management. *IEEE Access* **2020**, *8*, 153578–153588.
42. Mohammadi, V.; Rahmani, A.M.; Darwesh, A.; Sahafi, A. Trust-based Friend Selection Algorithm for navigability in social Internet of Things. *Knowl. Based Syst.* **2021**, *232*, 107479.
43. Wu, J.; Dong, M.; Ota, K.; Liang, L.; Zhou, Z. Securing distributed storage for Social Internet of Things using regenerating code and Blom key agreement. *Peer Peer Netw. Appl.* **2015**, *8*, 1133–1142.
44. Nitti, M.; Atzori, L.; Cvijikj, I.P. Friendship selection in the social internet of things: Challenges and possible strategies. *IEEE Internet Things J.* **2014**, *2*, 240–247.
45. Amin, F.; Abbasi, R.; Rehman, A.; Choi, G.S. An advanced algorithm for higher network navigation in social Internet of Things using small-world networks. *Sensors* **2019**, *19*, 2007.
46. Amin, F.; Choi, G.S. Advanced service search model for higher network navigation using small world networks. *IEEE Access* **2021**, *9*, 70584–70595.
47. Ramasamy, T.; Arjunasamy, A. Advanced heuristics for selecting friends in social internet of things. *Wirel. Pers. Commun.* **2017**, *97*, 4951–4965.
48. Rajendran, S.; Jebakumar, R. Object Recommendation based Friendship Selection (ORFS) for navigating smarter social objects in SIoT. *Microprocess. Microsyst.* **2021**, *80*, 103358.
49. Pashaei Barbin, J.; Yousefi, S.; Masoumi, B. Navigation in the social internet-of-things (SIoT) for discovering the influential service-providers using distributed learning automata. *J. Supercomput.* **2021**, *77*, 11004–11031.
50. 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.
51. Atzori, L.; Iera, A.; Morabito, G. From "smart objects" to "social objects": The next evolutionary step of the internet of things. *IEEE Commun. Mag.* **2014**, *52*, 97–105.
52. Ahmed, I.; Ahmad, M.; Jeon, G.; Piccialli, F. A framework for pandemic prediction using big data analytics. *Big Data Res.* **2021**, *25*, 100190.
53. Saura, J.R.; Herráez, B.R.; Reyes-Menendez, A. Comparing a traditional approach for financial Brand Communication Analysis with a Big Data Analytics technique. *IEEE Access* **2019**, *7*, 37100–37108.
54. 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: Berlin/Heidelberg, Germany, 2016; pp. 153–173.
55. Wu, Q.; Ding, G.; Xu, Y.; Feng, S.; Du, Z.; Wang, J.; Long, K. Cognitive Internet of Things: A new paradigm beyond connection. *IEEE Internet Things J.* **2014**, *1*, 129–143.
56. Kasnesis, P.; Patrikakis, C.Z.; Kogias, D.; Toumanidis, L.; Venieris, I.S. Cognitive friendship and goal management for the social IoT. *Comput. Electr. Eng.* **2017**, *58*, 412–428.
57. Wu, L.; Zhang, Q.; Chen, C.H.; Guo, K.; Wang, D. Deep learning techniques for community detection in social networks. *IEEE Access* **2020**, *8*, 96016–96026.
58. Cho, J.H.; Chan, K.; Adali, S. A survey on trust modeling. *ACM Comput. Surv. (CSUR)* **2015**, *48*, 1–40.
59. Nitti, M.; Girau, R.; Atzori, L. Trustworthiness management in the social internet of things. *IEEE Trans. Knowl. Data Eng.* **2013**, *26*, 1253–1266.
60. 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.
61. Talbi, S.; Bouabdallah, A. Interest-based trust management scheme for social internet of things. *J. Ambient Intell. Humaniz. Comput.* **2020**, *11*, 1129–1140.
62. Mohammadi, V.; Rahmani, A.M.; Darwesh, A.M.; Sahafi, A. Trust-based recommendation systems in Internet of Things: A systematic literature review. *Hum. Centric Comput. Inf. Sci.* **2019**, *9*, 1–61.
63. Marche, C.; Atzori, L.; Pilloni, V.; Nitti, M. How to exploit the social Internet of Things: Query generation model and device profiles' dataset. *Comput. Netw.* **2020**, *174*, 107248.
64. Li, Z.; Chen, R.; Liu, L.; Min, G. Dynamic resource discovery based on preference and movement pattern similarity for large-scale social internet of things. *IEEE Internet Things J.* **2015**, *3*, 581–589.
65. Jung, J.; Chun, S.; Jin, X.; Lee, K.H. Quantitative computation of social strength in Social Internet of Things. *IEEE Internet Things J.* **2018**, *5*, 4066–4075.
66. Wei, L.; Wu, J.; Long, C.; Li, B. On designing context-aware trust model and service delegation for social internet of things. *IEEE Internet Things J.* **2020**, *8*, 4775–4787.

67. Bakhshi Kiadehi, K.; Rahmani, A.M.; Sabbagh Molahosseini, A. A fault-tolerant architecture for internet-of-things based on software-defined networks. *Telecommun. Syst.* **2021**, *77*, 155–169.
68. Caporuscio, M.; Flammini, F.; Khakpour, N.; Singh, P.; Thornadtsson, J. Smart-troubleshooting connected devices: Concept, challenges and opportunities. *Future Gener. Comput. Syst.* **2020**, *111*, 681–697.
69. Nazari Cheraghlou, M.; Khadem-Zadeh, A.; Haghparast, M. A novel hybrid fault tolerance architecture in the internet of things. *Wirel. Pers. Commun.* **2021**, *118*, 383–411.
70. Moridi, E.; Haghparast, M.; Hosseinzadeh, M.; Jafarali Jassbi, S. Novel fault management framework using markov chain in wireless sensor networks: FMMC. *Wirel. Pers. Commun.* **2020**, *114*, 583–608.
71. Park, P. Markov chain model of fault-tolerant wireless networked control systems. *Wirel. Netw.* **2019**, *25*, 2291–2303.
72. Casado-Vara, R.; Novais, P.; Gil, A.B.; Prieto, J.; Corchado, J.M. Distributed continuous-time fault estimation control for multiple devices in IoT networks. *IEEE Access* **2019**, *7*, 11972–11984.
73. Tajiki, M.M.; Shojafar, M.; Akbari, B.; Salsano, S.; Conti, M.; Singhal, M. Joint failure recovery, fault prevention, and energy-efficient resource management for real-time SFC in fog-supported SDN. *Comput. Netw.* **2019**, *162*, 106850.
74. Stavrinides, G.L.; Karatza, H.D. A hybrid approach to scheduling real-time IoT workflows in fog and cloud environments. *Multimed. Tools Appl.* **2019**, *78*, 24639–24655.
75. Zhang, Y.; Zou, L.; Pan, D. Cloud-Edge Collaboration Dynamics Information Dissemination Model for Social Internet of Things. *IEEE Trans. Netw. Sci. Eng.* **2023, Vol 10, No.4**.
76. Han, T.; Zhang, L.; Pirbhulal, S.; Wu, W.; de Albuquerque, V.H.C. A novel cluster head selection technique for edge-computing based IoMT systems. *Comput. Netw.* **2019**, *158*, 114–122.
77. Shah-Mansouri, H.; Wong, V.W. Hierarchical fog-cloud computing for IoT systems: A computation offloading game. *IEEE Internet Things J.* **2018**, *5*, 3246–3257.
78. Blum, A.; Dwork, C.; McSherry, F.; Nissim, K. Practical privacy: The SuLQ framework. In Proceedings of the Twenty-Fourth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems, Baltimore, Maryland, 13–15 June 2005; pp. 128–138.
79. Xiong, J.; Ren, J.; Chen, L.; Yao, Z.; Lin, M.; Wu, D.; Niu, B. Enhancing privacy and availability for data clustering in intelligent electrical service of IoT. *IEEE Internet Things J.* **2018**, *6*, 1530–1540.
80. Zhang, H.; Zhu, L.; Dai, T.; Zhang, L.; Feng, X.; Zhang, L.; Zhang, K. Smart object recommendation based on topic learning and joint features in the social internet of things. *Digit. Commun. Netw.* **2023**, *9*, 22–32.
81. Ray, P.P. A survey on Internet of Things architectures. *J. King Saud Univ. Comput. Inf. Sci.* **2018**, *30*, 291–319.
82. Asghari, P.; Rahmani, A.M.; Javadi, H.H.S. Service composition approaches in IoT: A systematic review. *J. Netw. Comput. Appl.* **2018**, *120*, 61–77.
83. Mei, A.; Stefa, J. SWIM: A simple model to generate small mobile worlds. In *IEEE INFOCOM 2009*; IEEE: New York, NY, USA, 2009; pp. 2106–2113.
84. Nitti, M.; Pilloni, V.; Colistra, G.; Atzori, L. The virtual object as a major element of the internet of things: A survey. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 1228–1240.
85. Shen, J.; Zhou, T.; Wei, F.; Sun, X.; Xiang, Y. Privacy-preserving and lightweight key agreement protocol for V2G in the social Internet of Things. *IEEE Internet Things J.* **2017**, *5*, 2526–2536.
86. Yang, Y.; Lichtenwalter, R.N.; Chawla, N.V. Evaluating link prediction methods. *Knowl. Inf. Syst.* **2015**, *45*, 751–782.
87. Kowshalya, A.M.; Valarmathi, M.L. Community detection in the social internet of things based on movement, preference and social similarity. *Stud. Inf. Control* **2016**, *25*, 499–506.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.