Journal of Computer Science

Review

A Comprehensive Survey on Security, Trust Management and Privacy Preservation for Social-Internet-of-Things (S-IoT)

Rahul, Venkatesh and Venugopal K. R.

Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bengaluru-560001, India

Article history
Received: 19-08-2022
Revised: 07-11-2022
Accepted: 09-11-2022

Corresponding Author:
Rahul
Department of Computer Science and Engineering,
University Visvesvaraya College of Engineering,
Bangalore University,
Bengaluru-560001, India
Email: rahul.g@uvce.ac.in

Abstract: The Social Internet of Things (S-IoT) is a new paradigm that evolved with a convergence of social networking concepts and internet of things concepts. This paradigm helps develop intelligent devices and services with higher utility. The new paradigm enriches the social interaction between human's objects, heterogenous social objects interaction, the discovery of service and scalability. In recent years, S-IoT has been researching a hot topic and has drawn the attention of researchers, resulting in research on trust management, privacy preservation, service provisioning and security mechanisms. However, S-IoT faces new research challenges like interoperability, trustworthiness, security threats, scalability, navigability, service discovery and composition. In line with the research trend, this article provides a systematic survey of fundamental concepts of S-IoT and IoT, distinguishable characteristics of S-IoT and IoT and research challenges in S-IoT. This survey thoroughly reviews secure communication mechanisms, privacy-preservation techniques and the trust-evaluation model in S-IoT. Furthermore, we accentuate the privacy-preservation mechanism proposed in the literature for seven years and explored research areas. The holistic survey gives an overview of trust-evaluation models with respect to the service provider's perspective. This article overviews secure communication protocols and architecture in the S-IoT context. Finally, various research gaps, applications of S-IoT and research directions help a researcher to carry out research work in S-IoT.

Keywords: Index Terms-Social Networks, Internet-of-Things (IoT), Social-Internet-of-Things (S-IoT), Trust Management, Privacy-Preservation, Security, Social Relationships, Social Objects (SOs)

Introduction

The Internet of Things (IoT) is a network of linked computation devices that may communicate with one another and share useful data without the need for human intervention. Social networking is the practice of maintaining contact with friends, family, colleagues, customers, or clients using internet social media platforms. Rapid breakthroughs in the fields of the Social Networks and Internet have pushed us to the brink of a real-time linked society. As a result, a new paradigm is known as Social-Internet-of-Things (S-IoT).

The S-IoT is a fusion of social networking and Internet-of-Things (IoT) technology. As a result, social networks are formed in which items function as nodes to create social connections, much as people do. Every node in the S-IoT model is an item that may interact socially with other objects on its own by rules established by its owner.

S-IoT is capable of defending against malicious attacks. Social IoT can combat various vulnerable security attacks, enabling Device-to-Device communication (D2D), content sharing and establishing secure communication links with legitimate devices. The privacy breach in users' private information leads to the disclosure of property loss and personal information. Therefore, the urgent requirement in S-IoT is to construct privacy-preserving method that overcomes privacy breach problems in data mining process in S-IoT.

Internet-of-Things (IoT)

The Internet-of-Things (IoT) is a collection of heterogeneous physical devices or items that communicate and interact with one another through the

Science Publications

© 2023 Rahul, Venkatesh and Venugopal K. R. This open-access article is distributed under a Creative Commons Attribution (CC-BY) 4.0 license.

internet, allowing users to monitor and manage them remotely. IoT has grown significantly in recent years and it is beginning to fill our lives in a variety of settings, including hospitals, homes, roadways and much more. The Internet of Things is poised to become the technology of the future in the next years as a result of its rapid expansion. Sensors are commonly found in IoT devices and these sensors capture a variety of data and send it over the internet to monitor, control, or make decisions. Most of these data are collected in real-time to make the best judgment possible about the device status. Figure 1, some of the promising IoT-based applications are shown.

Heterogeneous devices in IoT constantly move from one location to another, changing their identities and people around the user also change their location. Many researcher (Li *et al*., 2015) proposed context-aware middle-ware architecture to provide context data sharing and adaptive behaviour in IoT applications proactively.

An efficient trust model is vital in accepting blockchain technology in smart cities (Hakak *et al*., 2020). The privacy and security of sensitive data are influencing factors on trust. The author in (Hakak *et al*., 2020) identified essential properties of blockchain technology that make it suitable and acceptable for IoT-based smart cities application, where in trust between device is maintained.

To address research problems in IoT, the authors of (Din *et al*., 2018a) conducted a systematic study on virtualization, smart cities, fog computing, WSN-based data centric IoT devices, heterogeneous IoT devices, data mining, a cellular connection, real-time analytics and context-awareness. The author presented the elements of distinct IoT features with their general purposes and functionalized of various IoT modules. Further, the author summarized the design issues and research solutions discussed throughout this study. Finally, several open research issues in the aforementioned domains were presented for the IoT acceptability intuition.

Sobin (2020) have thoroughly examination of most IoT principles, including architecture, protocols, security and privacy, scalability and energy efficiency and so forth. For research, the author has briefly addressed the most current research problems and listed the papers as principles stated and open issues.

IoT applications perform data reasoning through data analysis and model data to extract useful, valuable insights from several captured data. IoT application use context aware system to convert data into contextual information, which helps IoT application to act cognitively. Contextual information and context sharing enable context interoperability among objects in IoT (de Matos *et al*., 2020) reviewed various context-sharing platform requirements of context sharing, characteristics and challenges. Then, IoT application use context-aware system to convert data into contextual information, which helps IoT application to act cognitively.

The deployment of IoT-based applications in the industry brought many benefits and optimized industrial operations (Khan *et al*., 2020a). would automate data sensing, data gathering, data aggregation, data processing and communication in other industry entities. Khan *et al*. (2020a) highlighted state-of-the-art techniques with respect to the Industrial IoT framework, architectures, data handling methods, communication protocols and algorithms, etc. The author emphasized factors that binder the success of IoT.

The self-assembling solution are proposed in (Lemoine *et al*., 2020) to manage a huge number of heterogeneous devices, such devices are characterized by higher degree of physical distribution and achieve a common goal. The proposed solution builds the main train assembly of service that satisfies functional requirements, structural requirements and QoS.

The heterogeneous connected device in IoT is increasing exponentially. Standardizing various communication protocols, channels, architecture, middleware etc., is essential for the future success of IoT. Further, the data generated by these IoT devices is huge. Therefore, understanding, reasoning and learning of huge variety of data are paramount for success of IoT applications. The author in (Sezer *et al*., 2017) highlighted the importance of intelligent IoT systems in understanding context (environment, sense of situation with the help of sensors) and making appropriate decisions in an autonomous way.

An extensive literature review on SDN and edge computing systems to solve challenging issues in IoT is done by the author in (Rafique *et al*., 2020). The author has presented SDN-based IoT architecture using edge computing. The author in (Rafique *et al*., 2020) emphasized efforts and key requirements in integrating SDN and edge computing into IoT.

The authors in (Dias *et al*., 2020) proposed an extension to the popular visual programming NODE-RED. These extensions make a heterogeneous node to be reliability and resilient toward multifunctionality. It enhances dependability and take appropriate actions. The proposed self-resilient system is built with the objective to improve reliability and dependability. The proposed system was tested with different conditions and scenarios.

Research Challenges in IoT

A. Security in IoT

The mutually authenticated scheme is proposed in (Wu *et al*., 2016) based on ECC. The mutually authenticated proposed scheme can resist offline guessing attack and desynchronization attack. It has strong forward security.

Adat and Gupta (2018) have discussed and analyzed IoT architecture in the context of security. The author also provides detailed taxonomy of security challenges taxonomy of defense mechanisms. The author emphasizes a research direction on defending IoT from various attacks.

Khan *et al.* (2018a), have studied customer security breaches in IoT-enabled Consumer Electronic (CEIoT) devices. The author has proposed a framework to mitigate security violation of consumer. The author identified five means of security values in CEIoT. The security values are due to resale, retire, borrow, rent and gift is explored. The consumer activities demonstrate CEIoT consumers' communal behavior, which may result in posing severe security for its customers. The CEIoT items or devices can be maintained, supported, working and moved ahead by their producers until they reach their End of Life (EoL). Still, after that, they become vulnerable to assaults and if not properly decommissioned, some significant consequences may ensue.

Amanullah *et al*. (2020) reviewed possible vulnerable security breaches in IoT or IoT-enabled applications. The author reviewed state of art methods to prevent or avoid security breaches and deep learning based techniques for IoT security breaches are discussed in this study. The author emphasized using big data techniques to perform processing, discover knowledge and security threats in IoT-enabled devices.

The security and sensitive data breaches in IoT base sessions threaten the success of IoT products or applications. Authors in (Khan *et al*., 2016) have identified critical features and characteristics of IoT that are vulnerable to security requirements in terms of consumer's perceptive are identified in (Khan *et al*., 2016). The author proposed a security model that satisfies consumers' perceived security requirements.

Khan *et al*. (2018b) highlighted consumers' potential acts that cause security violations. The possible actions of customers are (1) Borrowing IoT-based products from other consumers. (2) Offering his/her IoT products or service to another user. (3) A consumer gives their IoT product to another consumer as a gift. (4) Resale of IoT products. (5) Non-use of IoT products or creating IoT waste.

B. Privacy Preservation in IoT

To maintain location privacy in IoT, (Ullah *et al*., 2018) have suggested an Enhanced-Semantic-Obfuscation-Technique (ESOT). In the age of IoT, location privacy is a common problem that must be addressed. Numerous experiments have been conducted to determine whether the suggested ESOT approach is effective. In ESOT, consider the reliable distance between the obfuscated locations and original range to achieve a balance between location privacy and service utility. ESOT is a broad approach that may be used everywhere.

Using longitude (building height) to maintain location privacy is an enhancement to the existing approach. In the future, the author intends to expand levels of obfuscation depending on division of regional areas, namely semi-rural, rural, semi-urban and urban.

The customer's privacy violated in IoT-enabled Consumer Electronic (CEIoT) devices has discussed in (Khan *et al*., 2018a). The author has proposed a structure to mitigate privacy violation of consumer. The author identified five means of privacy values in CEIoT. The privacy values are due to resale, retire, borrow, rent and gift is explored. The consumer activities demonstrate CEIoT consumers' communal behavior, which may result in the disclosure of customer's private locations and privacy concerns for its customers.

Khan *et al*. (2019) proposed a consumer trust model that satisfies privacy and security requirements. The author presented customer privacy requirements in terms of where data is stored, when to use data, what to generate data and who to share data. The author suggested solutions to address these requirements while developing IoT products or IoT devices.

Consumer trust may be effectively created if the consumer's perceived privacy expectations are satisfied. Khan *et al*. (2016) have described IoT's critical features and characteristics. From per consumer perceptive, (Khan *et al*., 2016) identified the importance of privacy requirements. The author proposed a privacy model that satisfies consumers' perceived privacy requirements and highlighted some important attacks and challenges at different stages of the privacy model.

Khan *et al*. (2018b), the author discusses privacy breaches from five different angles or acts. The author gives some suggestions regarding IoT waste i.e., IoT waste becomes a very important door for cyber attackers to get private information. The potential acts of customers are (1) Borrowing other services in IoT-based products. (2) Consumers offering their IoT products to another user. (3) Consumer give their IoT product to another consumer as a gift. (4) Resale of IoT products. (5) Non-use of IoT products or creating IoT waste. The authors of (Khan *et al*., 2018b) also made some suggestions to resolve the privacy risks raised by those five communal behaviors of consumers.

C. Trust Management in IoT

In recent years, several trust managements schemes have been designed based on blockchain technology. The proposed schemes gather customer feedback, their recommendation and neighbouring device of a device. The author in (Lahbib *et al*., 2019) creates a time-stamped log of trust information and embeds the trust score of devices into blockchain transactions. Context based trust model is proposed in (Rafey *et al*., 2016). Trust score is measured by integrating direct observations and indirect recommendations factors.

For SOA based IoT technique, the author in (Chen *et al*., 2014) developed and evaluated an adaptive and scalable trust management technique. Three different social connections might bind item owners together: Friendship, which stands for intimacy; a community interest, which stands for social contact; and social experiences or knowledge, which stands for proximity and closeness. By utilizing these social interactions, S-IoT smart devices may have greater collaboration and services with others with excellent relationships. Additionally, the author designed an adaptive filtering method in which each hub modifies its ideal weighing factors to add indirect and direct trust to the overall level of trust. The author used simulation to demonstrate the benefits of the adaptable IoT trust protocol over Peer-Trust and Eigen-Trust in terms of convergence, convergence and robustness against harmful nodes that engage in self-promotion, defamation, ballot stuffing and opportunistic service attacks. Only persistent attackers-those who engage in attacks such as ballot stuffing, self-promotion, opportunistic service and badmouthing with a probability of one-or whenever there is a chance-were evaluated in (Chen *et al*., 2014). To further evaluate the robustness characteristic of adaptive and scalable trust protocol architecture, the authors in (Chen *et al*., 2014) want to investigate different attacker behaviour models such as opportunistic collusion assaults, insidious attacks and random attacks.

Hammi *et al*. (2018) suggested an innovative concept called bubbles of trust. In bubbles of trust (Bubbles of trust means trust in devices), safe virtual zones are formed in which devices may connect in a secure manner. The trust bubble approach may be used to a variety of IoT settings, services and circumstances. Bubbles of trust are based on public Blockchain; therefore, it has all security features. In addition, the author developed a threat model and specified the security requirements for IoT authentication system. The suggested threat model demonstrates its ability to satisfy the necessary security standards and its resilience to assaults. Furthermore, the author offered exhaustive research on time and energy consumption, where several devices were assessed. In future work, the author plans to (1) Create the framework for a selected subset of bubbles to communicate in a regulated manner; (2) Build a method for revocation for compromised devices; and (3) Research and develop a protocol's objectives to maximize both numbers of miners in a specified system and the placement of the chosen miners.

The IoT application success depends on consumers' perception of security and privacy in IoT products or applications. The author in (AlHogail, 2018) identified factors influencing customer trust on IoT products/applications. The author in (AlHogail, 2018) have presented a trust model that covers the factors that strongly influence the user's decision to adopt IoT products. The identified factors are product-related, security-related and social-related.

The researcher in (Tang *et al*., 2019) presented a decentralized IoT trust framework based on Blockchain. The proposed framework has five collaborative rules concerning the data repository set of addition to be performed. Device access on occur rent cross platform access rules and incentives rules. These five collaborative rules are accomplished using smart contracts. The authors also suggested different (i.e., proposed framework collaborative process, access control and hierarchical) ways to implement. In future work, the author has suggested to design context aware access framework, cross-platform trust framework and policy administrators' verification based on Blockchain.

Many techniques have been suggested in the literature to compute trust in IoT environment. Similarly, several approaches are proposed in the literature to address security issues. These approaches are failed since some authentic IoT objects are captured by attackers and exploited as gateways to introduce new threats. To improve the trust level in IoT products or applications, the author in (Ahmed *et al*., 2019) have introduced thematic taxonomy to calculate trust. The author includes several parameters while calculating trust in IoT. The parameters are the role of entity/entities, properties of trust, application of trust, management of a trust, matrices used in trust calculation, threats and attack on Trust and Reputation (TR).

The Internet of Things' trust methods are addressed in (Din *et al*., 2018a). Relevant strategies are identified and their contributions and limits are provided based on a complete review of trust management. According to I. Ud Din *et al*. (2018b), this study will help IoT research group focused on trust management understand the perspectives and challenges that IoT confronts in terms of trust administration.

Centralized trust management has several benefits, such as flexibility and adaptability. But security vulnerabilities are more due to dynamic topology in the internet of vehicles. Dynamic access control can be granted based trustworthiness of nodes (i.e., roadside components). Cinque *et al*. (2020) proposed Blockchain-based decentralized trust management that exploits consistency and security guarantee features of Blockchain. The proposed solution has better load balancing, fault tolerance and scalability.

Applications of IoT

A. Smart Parking

The new smart-parking sensors or switches will be hidden in parking places to track the arrival and exit of cars. Smart parking offers comprehensive parking management systems that enable drivers to save time and fuel use.

B. Smart Home

Smart home is highly accepted and widely accepted IoT applications on all measured channels. A home has various electronic gadgets such as fans, heaters, air conditioners, microwave ovens, lights and refrigerators. In smart home automation these gadgets can be equipped with actuators and sensors to maximize energy efficiency and improve user comfort. These sensors can gauge the temperature.

C. Smart City

National smart cities project is an urban renewal, redeveloping and retrofitting project initiated by various government across the world. IoT-based smart cities extensively use IoT device to collect and analyse data. The collected and analysed data is useful in improving infrastructure, public utilize and services (i.e., traffic management, waste management and monitoring environment).

D. Smart Health

IoT-based health monitoring system helps out doctor's/health center to collect real-time data effortlessly and monitor critical physiological parameters at regular intervals. The doctors/health center provide valuable information to individual.

E. Smart Cars

Machine to Machine (M2M) communications, particularly those made possible by Smart Cars, may assist to reduce accidents. These autonomous vehicles will offer functionality beyond safety, such as time savings, reduced driving stress, etc.

F. Smart Water Supply

Smart cities must keep an eye on their water supplies to make sure is sufficient access for commercial and residential needs. Wireless Sensor Networks offer the technologies necessary for monitoring cities. Explore their water pipe networks, more precisely biggest dangers of water loss. Cities facing water issues sensor technology leakage issues are resulting in high from their investment and money.

Social-Internet-of-Things (S-IoT)

The Social Networks and the Internet-of-Things (IoT) concepts have been merged in a new approach called "Social Internet of Things" (S-IoT), which enables linked devices and people to communicate inside a social network structure to facilitate new social navigation.

The Internet-of-Things (IoT) is a new paradigm that strives to make the world intelligent in order to better serve humans. A smart city's constituents contain n smart buildings, smart health, smart grid, smart industry, smart learning, smart transportation and smart home. Despite significant progress in areas like as big data analytics, security and architecture, the idea of smarter planet is still a long way off due to unforeseen hurdles. For example, necessitates a worldwide platform that allows objects to connect, interact and build social ties (e.g., co-work, co-location, social, parental, or co-ownership) in order to sharing resources (e.g., computation and information) and provide better services. Social-Internet-of-Things (S-IoT) is a new multidisciplinary sector that permits autonomous connection between social networking and the IoT. Table 1 compares the IoT and S-IoT.

In general, S-IoT depends only on the application. Based on these, different techniques and algorithms are provided as part of the evolution of connected objects. Figure 2 indicates the general evolution of S-IoT.

From a literary standpoint, the author of (Imran *et al*., 2019) editorial briefly describes the concept of S-IoT. The motivation behind S-IoT and its problems are also discussed in (Imran *et al*., 2019). Furthermore, the author in (Imran *et al*., 2019) identifies and classifies the fifteen papers approved in this Special Issue that are closely related to S-IoT and provides a brief synopsis of work.

The principles of S-IoT and the detailed survey on trust areas are explained in the survey (Roopa *et al*., 2019). The authors analyzed the most recent research on relationship management, service composition, relationship management, trust management and service discovery in S-IoT context. In in-depth analysis, the author fails to compare the most recent trust management methods suggested for S-IoT.

According to the stress cognition hypothesis, since member of network are stressed, unsecured it takes longer time to achieve (Chung and Liang, 2020). If members' confidence is high, they can adjust quickly, which makes knowledge exchange easier.

A comprehensive survey (Amin *et al*., 2022) emphasizes service discovery by objects, network navigability, components of S-IoT, distinct S-IoT application components, S-IoT architecture model components, models, publicly available datasets, tools, and platforms. The relationship between objects and users in S-IoT, multidivisional trust, trust management in S-IoT, key challenges and future research issues are discussed empathetically.

The key characteristics of the most recent resource-constrained hardware stages for S-IoT applications are described by the author in (Afzal *et al*., 2019). Based on these characteristics, specific OSs are recommended for each phase to effectively utilize their hardware capabilities. The author developed model OS architecture and its operational procedure are articulated to improve device-to-device interactions in S-IoT applications. It gives useful guidelines for designers to design an effective OS to meet the need of futuristic IoT and S-IoT applications.

In S-IoT large numbers of mobile devices are connected to each other, requiring additional frequency spectrum. The term "CR-S-IoT" refers to the usage of the Cognitive Radio (CR) spectrum as an opportunistic communication method for the Internet of Things. However, routing design is more challenging because of unpredictable spectrum availability in CR-S-IoT. The drawbacks of CR-S-IoT can be resolved by Opportunistic Routing (OR). ECOR, a novel energy-aware coded OR technique for CR-S-IoT, is suggested in (Zhong *et al*., 2020). In ECOR, the author developed a novel way of analysing the social aspects of CR-S-IoT. The proposed protocol leverages dynamic broadcast characteristics of the wireless channel and considers energy efficiency and social factors to select forwarding nodes. To maximize spectrum utilization, the author has proposed a channel allocation scheme based on an interference graph.

With the use of social, behavioral and inclination-based linkages in S-IoT, (Roopa *et al*., 2020) proposed a SIoV-based approach to the control of traffic congestion to alleviate traffic congestion and control traffic jams. These links are made between the cars, the commuters and the Roadside Units (RSUs). Create a road intersection with several pathways for each type of vehicle movement. Based on their requirements, the cars that move along the road path create social bonds with one another. The author of (Roopa *et al*., 2020) proposed a technique for optimizing the stream of no conflicting traffic by dynamically structuring it. The simulation's outcomes demonstrated how altering the pace at which cars enter the system may increase throughput, reduce waiting times on average and shorten the total distance travelled by vehicles along the network of roads. The throughput maximization is achieved by exploring social, behavioral and traffic.

The advancement in communication technologies enables the heterogeneous device to be part of IoT (Iqbal *et al*., 2019). The success of IoT applications depends on the trustworthy service provided by IoT applications. The author proposed trust model that considers various direct/indirect influence factor are context, reputation of object, expectation of vehicles, social relationship between vehicles, timely evaluation of trust and desire to connect. The author suggested a trust model incorporating advanced technologies like Blockchain and fog computing.

The author has explained the advantages of integrating S-IoT and IoT. Alam *et al.* (2015) proposed a structure of message based on ontologies and developed a social graph based traveler information system.

An agent-based platform ispiens is used to define roles and responsibilities and ways of interaction among the connected devices. Cicirelli *et al.* (2017) proposed a smart environment that allows heterogeneous devices to interact. The author suggests that a smart environment should support interoperability, reputation, service, device smart environment leverage, edge computing, and S-IoT paradigm.

Butt *et al.* (2018) conceptualizing the S-IoT in the automobile industry, proposed a scaled S-IoV structure based on secure internet technologies. The proposed architecture has six levels: Physical-world layer includes physical elements such as cars, pedestrians, drivers, passengers, environmental sensors and other physical objects. (1) Fog layer, (2) Gateway layer, (3) Physical world layer, (4) Application layer, (5) Cloud layer and (6) The user layer. The physical world layer includes physical elements such as cars, pedestrians, drivers, passengers, environmental sensors and other physical objects. In order to collect data from sensors and other physical objects carried by pedestrian's driver and passengers, the physical layer is essential. It acts as the SIoV architecture's electrical, mechanical and intelligent interface. A smart car module and a roadside device make up the gateway layer. It acts as a gateway between the physical-world layer and cloud-based infrastructure, collecting physical-world data and sending it to the fog layer. Large amounts of data are stored close to the end user via the fog layer, which is made up of fog nodes, instead of being sent over the Internet to centralized data centers. As a result, the quantity of data required for Internet communication is deducted. The cloud layer is a centralized node that uses cloud technology to provide a centralized back end that can store enormous quantities of data transferred between social interactions and their cars and data received from environmental sensors.

Research Challenges of S-IoT

Many S-IoT challenges might be critical for researchers working on new solutions. The key challenges are as follows:

1. Heterogenicity: The S-IoT has millions of items with diverse platforms, standards, protocols platforms and sources and all objects and information must be recoverable. A heterogeneous network of objects has been produced due to these differences, which impacts how well they get along and interact with each other and increases complexity
2. Dynamicity and mobility: Smart objects are situated in a dynamic context where their locations are constantly altered, which leads to problems with efficient item selection and service delivery
3. Tracking objects: The most important problems with S-IoT and huge networks that are rarely considered are monitoring things, interactions and activities
4. Security, trust and privacy: The huge linked ecosystem of S-IoT's devices, services, possibilities and users make security a crucial component of information exchange in a safe manner. Therefore, in contrast to many other types of research that have been done in this area, it is still a serious problem that necessitates system modifications to survive various attacks in order to have reliability, security, availability and resilience in interactions

5. Resource constrained devices: Even though there is currently no perfect solution to handle this problem by taking energy limits into consideration at all design phases for more effective interactions. Because the S-IoT is a limited-resource system, this issue has a direct influence on network durability and information sharing
6. Efficient service search and discovery: Since there are so many S-IoT items, it isn't easy to scale the system, find services, or link the right things together. Costs in the S-IoT system are rising as a result of this issue

A. Security in S-IoT

The vulnerabilities or bugs in S-IoT applications are determined using fuzz testing that considers edge and path coverage (Zhu *et al*., 2020). To decrease the overhead and increase efficacy, (Zhu *et al*., 2020) suggested BECFuzz. To get around the issue of edge collision, BECFuzz suggests instrumenting at the edges. BECFuzz makes use of both coarse path coverage and edge coverage data.

Multivariate polynomials based on a post-quantum ring signature scheme is proposed in (Yi, 2021) for privacy protection. Further, a post-quantum blockchain method is proposed for securing S-IoTs devices. All messages from S-IoTs devices are secured using the Blockchain. With the help of a postquantum ring signature, all client can affix their signature to the message. Other clients can confirm the messages and the genuine identity of the message owner. Then, the messages and the signature are secured using the Blockchain.

Nie *et al*. (2021) discussed about the intrusion detection issue in Collaborative Edge Computing (CEC)-based S-IoT. Nie *et al*. (2021) proposed a GAN-based intrusion detection method. The proposed method can distinguish different attack by extracting features of social network data, the proposed strategy can be utilized to distinguish different attacks. Nie *et al*. (2021) proposed have three stages. The proposed method first pre-processes the flow and performs feature extraction. Then, plan intrusion detection algorithm pointing at single attack based on GAN. Third, an intrusion detection technique based on GAN that combines many intrusions detection models each pointing to single attack. The simulation results, proposed strategy can significantly improve precision of intrusion detection comparing with other two strategies. To improve precision of proposed method further, it will combine GAN and convolutional neural network method for extracting spatiotemporal highlights of network data. At required time, feature extraction algorithm is important to progress the real time execution of proposed method.

Wang *et al*. (2020a), the author has studied the issue of secure content transmission to find a balance between Quality of Experience (QoE) and security for S-IoT. The author proposed (Wang *et al*., 2020a) a User Preference Prediction (UPP) algorithm to provide secure data/content sharing in S-IoT. Further, the undirected hypergraph is a model suggested to effectively describe cumulative and uneven social interference. The developed an Uncoupled-User Concurrent Learning (UUCL) algorithm that can reach the pure optimum. The work in (Wang *et al*., 2020a) has introduced a novel idea for developing a safe strategy for content sharing in the S-IoT and has offered practical deployment strategies based on social trust to improve physical domain security.

Zhang *et al*. (2020), the author examined secure edge aided computations in S-IoT frameworks, which enable resource constrained IoT nodes to do large calculations safely and efficiently. Zhang *et al*. (2020) analyzed security threats in such a framework. Zhang *et al*. (2020) provides the security necessities that the outsourcing algorithms incorporate for these security threats. Also, the author suggested two secured outsourcing algorithms (modular exponentiation and matrix multiplication) that satisfy the specified security standards. To evaluate the proposed methods, the author performs hypothetical analyses and testing.

The author of this research looked at the viability of representing the S-IoT using BPMN. The author investigated the viability of utilizing BPMN to express the S-IoT in (Zhou *et al*., 2018). BPMN can capture the technical and social elements of the S-IoT environment due to the nature of business processes, which comprise both manual user actions and automatic service tasks. Based on this, (Zhou *et al*., 2018) proposed modeling the security needs using the third dimension. Traditional 2-D-based systems suffer from a complexity management problem. To address the limitations of 2-D-based solutions, the new 3-D security for design principle notation, which includes both symbolic and visual representation, was created. The application will be tested with real users in the future.

To solve the source location security issue, (Han *et al*., 2018) proposed a Source Location Protection Protocol Based on Dynamic Routing (SLPDR). The proposed scheme, bundles on the backbone will encounter a greedy route, followed by a directed route. Furthermore, Utilize the extra energy in the surrounding areas to your maximum advantage and create cyclical routes on a number of rings to distract the adversary. After this component covers the original source, allowing for important improved network security without compromising the network's lifetime. In future work, will include a more visible use of additional power outside the hotspot zone and the formation of a more efficient mechanism to ensure the source area.

Meena Kowshalya and Valarmathi (2018) the proposed trust model is compared to subjective, objectives and versatile trust model a novel system to improving trustworthiness among hubs in a S-IoT environment. Trust setting for each device in S-IoT environment is performed by fine-tuning the status and environment of devices. Two new trust models-first hand recommendation (Indirect Trust) and second-hand observation (Direct Trust), as well as a node's centrality and dependability-have been suggested in (Meena Kowshalya and Valarmathi, 2018) to measure the trust among nodes in a S-IoT network. In addition, the weighing elements were adjusted to determine the optimum application performance. Communications among nodes also are closely authenticated using secret codes. In the S-IoT system, the proposed framework also identifies Sybil zones. The similar approach can be expanded in a real time application for future work.

Lee *et al*. (2018) analyzed the restrictions of legacy vulnerability quantification strategies utilized to inspect social IoT network frameworks. Lee *et al*. (2018) propose a game-theory-based vulnerability evaluation strategy based on an attack tree. The evaluation method includes three phases game strategy modelling, cost impact analysis and payoff calculating. The effectiveness and competitiveness of the proposed strategy were confirmed by applying a case study to a social-IoT-based network environment. The proposed method compared, analyzed legacy methods. To quantify vulnerability. Security vulnerabilities in S-IoT are investigated. Suspectable quantification techniques are used to find a vulnerability in S-IoT. Utilizing the proposed strategy, a S-IoT administrator can impartially calculate the security vulnerability of a social IoT network system.

Kowshalya and Valarmathi (2016), the Ant Colony Optimization algorithms and the node characteristic similarity property are used to discover groups in the S-IoT environment. Sybil attacks are serious threats in present social situations. This study removed the Sybil nodes between communities. When compared to existing methods, the proposed approach effectively identifies communities with a high measured quality metrics.

B. Privacy Preservation in S-IoT

He *et al*. (2019) discusses the most challenging problem of the distributed agreement technique (He *et al*., 2019) has proposed a secure agreement-based Data Aggregation (DA) algorithm that gives guarantees on preserving the privacy of important data. The proposed algorithm has high accuracy, low complexity and is robust against network dynamics. However, the system collapses when nodes permanently fail.

A huge number of heterogeneous hubs constitute S-IoT. The heterogeneous hubs have different computing capabilities and provide location information. The location information includes minimum hop counts between the reference nodes and anchor node significance of each anchor node and contribution to the location information is computed based on fuzzy rough set theory. Zhou *et al*. (2022) proposed a ridge regression extreme learning machine that computes devices/users' positions based on a minimum number of hop counts from the device to the anchor node.

The study in (Zhang *et al*., 2021) analyzed and proposed a security enhancement mechanism to thrust attacks by the safety risk posed by adversarial sampling of Collaborative Edge Computing (CEC) nodes. A new adversarial text creation approach is suggested based on heuristic algorithm. In future work, continue to concentrate on research related to data security.

Yin *et al*. (2021) the author presented a novel hybrid privacy protecting strategy for decentralized learning and training devices. The proposed strategies combine Bayesian differential privacy and function encryption algorithm to adopt different data sets and protect the characteristics of the client's uploaded data. In order to improve the service quality of the model and provide more precise privacy protection, the Local Bayesian Differential Privacy approach is used to modify the privacy budget allocation of various datasets, modify the amount of noise addition and modify the degree of noise addition.

Deng *et al*. (2021), proposed a Lightweight-and-Privacy-Preserving-Image-Sharing (LPIS) method to address the challenge of finding unauthorized distributors in S-IoT. Deng *et al*. (2021) employed the additive secret sharing method to encrypt the shared picture in order to adapt to the S-IoT system. Using the encoded authentication data, LPIS can assist the image owner in determining the unauthorized distributors. It is difficult for unauthorized users to easily delete the encoded authentication information using typical attacks or JPEG compression attacks. None of the edge servers detected a leak of the image's unencrypted data. Additionally, the privacy-preserving embedding's design and execution increased the accuracy of identifying unauthorized distributors. With unauthorized distributor identification, LPIS can provide privacy-preserving picture sharing in S-IoT.

It is challenging to secure private and sensitive data extracted through the mining process and accurately mine data. Tian *et al*. (2021) proposed a Graph-Clustering-Privacy-Preserving (GCP) strategy based on structure-entropy to handle this issue. Proposed strategy where the focus is to mine the related data between the hubs of the graph structure and secure the privacy of the hub attributes.

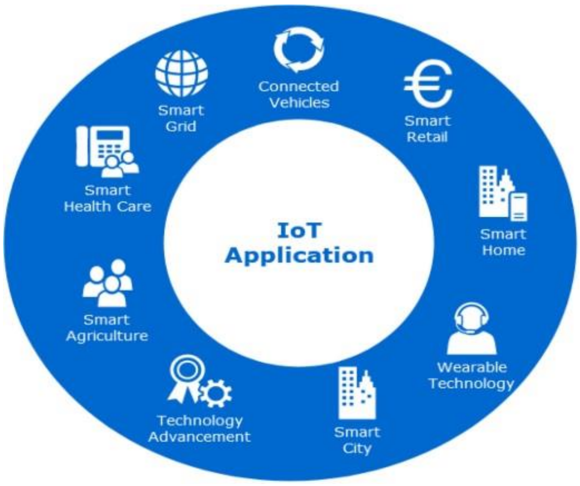

Fig. 1: Applications of IoT

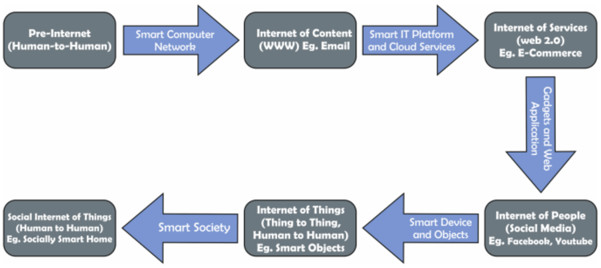
Pre-Internet (Human-to-Human)
Smart Computer Network
Internet of Content (WWW) Eg. Email
Smart IT Platform and Cloud Services
Internet of Services (web 2.0) Eg. E-Commerce
Gadgets and Web Application
Internet of People (Social Media) Eg. Facebook, Youtube
Smart Device and Objects
Internet of Things (Thing to Thing, Human to Human) Eg. Smart Objects
Smart Society
Social Internet of Things (Human to Human) Eg. Socially Smart Home

Fig. 2: Evolution of Social-Internet-of-Things (S-IoT)

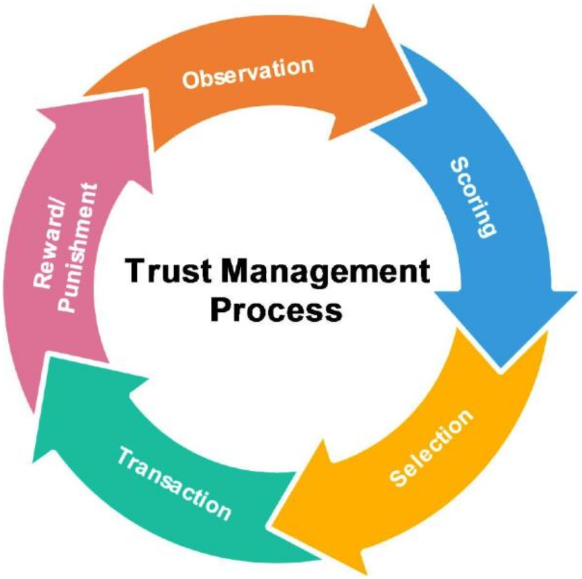

Fig. 3: Life cycle of trust management process

In the proposed scheme, the GCP secures the private data of the hubs and gets the optimal graph clustering impact using BGV homomorphic encryption and structural information theory.

Bi *et al*. (2020), proposes a privacy-preserving customized service system based on a static Bayesian game. In this privacy preserving personalized system, users independently generate their privacy options mixed with offsite fuzzy reasoning. Furthermore, it uses the equilibrium game mixing approach to ensure privacy. Meanwhile, the author uses information entropy in the proposed methodology to quantify privacy breaches. As an enhancement, fuzzy reasoning using neural networks and other user characteristics will improve effectiveness. The proposed method considers more variety of attackers and continuously improves its efficiency and comprehensiveness for privacy protection.

Gan *et al*. (2019) has tried to resolve the conflict between crowdsourcing's multi-hop incentive and the privacy-preserving incentive approach for protecting task requesters' privacy. Additionally, it creates a 1-hop myopic routing strategy and a multihop payment policy for effective crowdsourcing task routing in social IoT. This research's extension effort will design an incentive system based on the auction model while protecting privacy.

According to the author of (Wang *et al*., 2018), D2D-based caching in social IoT is important because it reduces downloading latency while ensuring reliable delivery. Wang *et al*. (2018) suggested a Content-Sharing-Oriented-Stable-Matching (CSOSM) algorithm in the first stage, considering both physical and social features. Resource allocation was changed into a many-to-one matching issue with peer effect in the second stage. Furthermore, NP hard formulation of the coverage technique was developed and a heuristic searching algorithm was suggested in order to find a near-optimal solution. Future work will involve data-driven modelling of social relationships, consideration of privacy protection in the data domain, etc.

Whenever more number of devices are connected to the S-IoT then a large amount of services is available also it is difficult for users to find ideal services among a large number of services. At the same time, it protects the data privacy of the users. To solve this problem, (Yan *et al*., 2021) proposed utilizes historical QoS information of clients within the smart things and presents the LSHF technique. A proposed S-IoT service recommendation approach called S-IoT-SR, which uses the LSHF technique to make an index offline. In the proposed scheme, when different stages share information with each other, only the hash value is obtained in the platforms, so the privacy of clients is secured.

Chen and Huang (2019) proposed a privacy user information inference strategy based on S-IoT key nodes, which infers other privacy node data through key nodes in S-IoT community. This inference strategy is based on the community's open data and the number of key hubs. The inference method is moderately simple. Chen and Huang (2019) has demonstrated to discover key nodes in information dispersal by learning the complete social data. The similarity rules of information between non-key hubs and key hubs are determined and the inference rule information set is obtained. Then the inference method of other non-key hubs or non-key hubs for key hubs in S-IoT is deduced. The network models are utilized to analyze the inference of key hubs and non-key hubs and the impact of key nodes to gather that private hub have obvious advantages. Future work focuses on information characteristics in different information sets and analyzes anonymous information through known information.

The author proposed a unique approach (Sharma *et al*., 2019) in fission computing, which utilised edge-crowd integration to preserve privacy regulations in S-IoT. Entropy modeling and crowdsourcing were employed in the proposed approach to maintaining trust. Numerical simulations were used to evaluate the proposed acceptable trust handoff and the privacy-preserving solution. The results were obtained by characterizing the quantity of dishonest clients compared to all other clients compared to the beginning circumstance. Further, it was discovered that employing the proposed generalized fission manager consistently maintained privacy rules.

Park *et al*. (2019), the author proposed a more secure dynamic privacy preserving and lightweight key agreement protocol for S-IoT's Vehicle-to-Grid (V2G). The proposed protocol fixed the security issues that were found. The proposed protocol guards against man-in-the-middle, trace attacks, replaying and offline guessing. The protocol achieves ultimate forward secrecy, anonymity and reliable mutual authentication. Park *et al.* (2019) demonstrated that protocol to be secure and more appropriate for application to practical V2G frameworks.

In order to examine privacy protection, Zhang *et al*. (2019) combines social interactions and connections into the S-IoT. Zhang *et al*. (2019) employed the conventional IoT network principles, protocols and incorporated social network build-up to understand client wants and service quality. This was done to improve the connections between clients and devices and the availability of computing devices. Zhang *et al.* (2019), the authors have applied client confidence-enhancing privacy protection technologies to enhance the value of data gathering. However, the space movement issue with edge computing is unsolved. In addition, the author in Zhang *et al.* (2019) needs to create complimentary wireless communication advances and improve the capability of the S-IoT.

Zouari *et al*. (2018) a fuzzy vault based matching protocol that provides a set of tunable parameters balanced to provide the desired trade-off between security and efficiency. Additionally, the choice of Blockchain for trust establishment provided an extra security layer that fitted superbly for the requirements of the trustless Peer-to-Peer (P2P) IoT interactions.

Shen *et al*. (2017) a lightweight key agreement protocol that emphasizes strong privacy and security. The protocol is more effective compared with Elliptical Curve Cryptography (ECC)-based protocols, which makes it both pertinent and practicable for resource-constrained environments. In addition, the proposed protocol addresses the dark aspects of smart grids, such as security and privacy issues. Experimental results analysis of the proposed protocol's performance and security indicates that it is both more effective and secure when compared to other applicable existing protocols.

C. Trust Management in S-IoT

The trust management life-cycle is shown in Fig. 3. The following five steps are interconnected to regulate the expansion of Trust Management (TM). Observation and gathering information, trust calculation and ranking of the objects based on trust score, selecting objects based on trust value, transaction/trust update and reward/punishment. In the initial step, the observer obtains data about the objects from which they want services or gives them access to system entity supervision parameters in order to derive objective findings regarding the reliability of the entities. After the data has been gathered, the second stage involves a centralized authority or an agent/object of interest giving each thing a reputation score, which is a suitable weight. These reputation points are applied to objects using a dependability rating process when there are several subjects. The most appropriate objects are chosen for a certain IoT transaction/service based on a specific set of criteria after calculating reputation points. Once an object is chosen, a transaction happens and further data about the object is gathered and saved by system components for the purpose of responding, the database being updated with the experience. Finally, various criteria differentiate between harmful and unreliable or active actors and honest and cooperative players with high local/global reputation ratings in the network. Improper actions will be penalized. Numerous research on trust management in the S-IoT environment have recently been published and comparative study has been presented in Table 2-5 by highlighting their distinct methodology and drawback.

The importance of trust management for S-IoT was emphasized by first survey on S-IoT trust management, published (Abdelghani *et al*., 2016). It provides a summary of the S-IoT's developments and network architecture. (Abdelghani *et al*., 2016) also emphasized the significance of trust management in S-IoT and the connected topics. The author describes its key characteristics and exhibits its use in S-IoT scenarios. In (Abdelghani *et al*., 2016) discusses trust-related threats and categorise S-IoT trust methods based on certain characteristics. Finally discussed the unsolved issues related to trust management in S-IoT.

Kowshalya and Valarmathi (2017), the author proposed an inspiring trust management model that evaluates trust based on the object's centrality, energy and service score, direct observation, indirect advice and other factors. The suggested trust model defends against dependable on-off targeted transmitting attacks. Regarding identification accuracy, the proposed trust model performs better than SOA-based, fuzzy and context-aware trust. The suggested trust management approach immediately separates the unreliable hubs and identifies them. The methodology, however, increases the chances of nodes with low trust values, all forms of attacker detection and attacks. Additionally, develop a strategy for managing a trust, study different attacker patterns and identify different types of attacks.

Rashmi and Raj (2019), the importance of the exponential extensive characteristic graph-based trust-computation method for S-IoT systems is emphasized. The different trust-related methods discussed in literature survey of trust models in S-IoT (Rashmi and Raj, 2019). Also, the various trust models are contrasted in view of S-IoT constraints, network topology and security-related issues.

Chahal *et al*. (2020) has presented specific information on IoT and S-IoT, their fundamental developments and proposed architectures. Chahal *et al*. (2020) presents a comparison study of different communication protocols utilized in IoT. A novel trust management framework is designed and examined after being drawn from several trust management concepts in IoT and S-IoT. This study is used to identify trust functions performed and trust goals they helped to achieve. It lists the benefits and drawbacks of current plans and details the trust functions used. Several forms of attacks launched against TMSs using the various communication protocols used in IoT are analyzed in the existing system. In the end, has discovered a few issues that S-IoT is facing and that need to be resolved; these issues can also lead to further investigation in this field.

The similarities and dissimilarities between the IoT and S-IoT transformation of physical objects to objects with social consciousness is explained in (Khan *et al*., 2020b). The trust administration frameworks and trust-evaluation techniques created for the S-IoT system are explored. A thorough comparison of S-IoT trust administration authorities and methods was presented. Finally, (Khan *et al*., 2020b) identified several S-IoT issues that should be addressed by developing appropriate cutting-edge arrangements.

The trustworthiness of an object plays a vital role in S-IoT applications because an untrustworthiness object may disrupt the system's functionality, quality and service reliability. A comprehensive review of trust-evaluation models for S-IoT has been carried out in (Sagar *et al*., 2022a). In this holistic survey, the author emphasizes five components: The essence of trust, trust management components, trust management schemes, the performance of trust-evaluation models and trust management in S-IoT-based applications.

Trust is perceived as the basis for decision-making. However, designing trust is difficult since heterogeneous quantifying and complex networks and nodes. Cho *et al*. (2015) did a comprehensive survey on trust model, properties of trust, trust information and calculation, trust assessment and trust in the context of complex, heterogenous nodes and applications. The four categories of trust models are cognitive, social, information and communicative trust. Similarly, the author assessed trust at a different level. The author has demonstrated how to construct trust and classified factor offering trust. The categorizing trust properties, including subjectivity, dynamicity, asymmetric, transitivity and contextual dependence, are described in (Cho *et al*., 2015).

Chen *et al*. (2020) designed a decentralized trust framework on Blockchain that allows only trusted nodes to participate in transportation and penalize trusted nodes. The trust model includes evaluating trust incentives for trusted nodes and a consensus model based on Blockchain. The reputation of an entity is used in evaluating trust and nodes are rewarded when they make a good and useful contribution and provide service.

Rehman *et al*. (2019) provides a comprehensive overview of the key trust challenges in the bitcoin ecosystem and several immediate, short-term and long-term remedies to resolve these challenges. Rehman *et al*. (2019) emphasized that resolving these trust challenges results in the emergence of a new generation of cryptocurrency systems. In the new cryptocurrency system, cryptocurrencies will be the primary drivers of financial institutions and the major streams of the economy. However, to create a long-term and sustainable operating environment, all participants-from authorities to service providers, traders and, mining systems must be aware of the technical and nontechnical effects of the cryptocurrency ecosystem.

Fan *et al*. (2020) discussed decentralized trust management approaches, their efficiency and resilience, from three distinct points of view. First, investigate six popular threat models' risk elements and negative consequences. Second, look at the representative trust measures and trust aggregation models. Third, provide a detailed study and comparison of various reference trust aggregation approaches in terms of efficacy and robustness. This study acts as a foundation for investigating and creating services and algorithms for next-generation trust aggregation that are used to anticipate risk elements and malicious attacks.

To enable the multimedia device to device agreeable communication author in (Yan *et al*., 2018) proposed a socially aware trust model. According to the trust system reliable communication is measured in terms of capability trust and social trust. The reliable user set was discovered from the relay users, using the decision-theoretic rough set based on naive Bayesian and after that, the relay users were separated into trustworthy users, observed users and untrustworthy users. Simulation results approved the proposed strategy effectively identified the trustworthy users, upgraded the multimedia service delivery rate and decreased the transmission cost. The future investigations will focus on the privacy assurance and attacking behaviors of D2D users.

Yang *et al*. (2018) used the Bayesian inference model to validate the message exchanged between vehicles. The Roadside Units (RSU) update the trust value of the vehicle based on validation results. The uploaded trust values are added as block in the trust Blockchain. It is maintained by RSU.

Khan *et al*. (2017) reviewed existing S-IoT trust management strategies, highlighted the importance trust management in social collaboration between objects. The author explained the hierarchical architecture and the idea of the Social-Collaborative-Internet-of-Things (SCIoT). Further, a new threat model was proposed that categorizes the different types of attacks on SCIoT. Finally, the potential challenges and issues in the SCIoT were discussed.

Trusting of an object plays a significant role in S-IoT application success because it directly influences the object's decision on service delegation. However, the solutions proposed in the literature consider only the service requester's requirements and evaluate the service requester's trustworthiness. Wei *et al*. (2022) proposed a solution that avoids a trust crisis between a service provider and a service requester. The proposed solution comprehensively evaluates the trustworthiness of service requesters and service providers. The proposed solution avoids prejudiced treatment by the adversary service requester. The proposed solution or trust model is a context-aware, opinion-based, evidence-based trust model. The proposed trust model isolates malicious service providers. However, the suggested bidirectional trust model does not take into account IoT object and service features. This paradigm is more suited to the non-heterogeneity and distinction of IoT objects.

Cai *et al*. (2021) comprehensively consider the object properties and service characteristics in a local and global context to select a reliable service provider. Multiple trust paths between a service requester and a service provider are constructed based on object properties and service characteristics. A Trust Inference method is proposed to compute trust relationships. A Trust Inference method contains two phases: Trust propagation phase and trust aggregation phase. In trust propagation phase, object identifies an object's trusted and connected one-hop or two-hop neighbors. The algorithm assigns ordered weights to more reliable neighbors in the trust aggregation phase. However, the proposed algorithm fails to mine indirect trust between objects.

Object-to-object communication and object-to-user communication in S-IoT application has enhanced service quality. It provides an accurate response to complex issues. Trust models are proposed in the literature to prevent detrimental communication and preserve personal information and system functionality. However, malicious devices still exist in S-IoT that tarnish the reputation of benign objects or devices. The authors in (Magdich *et al*., 2022) performed an in-depth analysis of the object's trustworthiness and proposed a method to detect malicious S-IoT objects. The proposed trust-evaluation model determines the trustworthiness score of the object. Object trustworthiness score is based on multiple factors such as type of device, capacity, common interest, co-work and transaction history.

The trustworthiness of a social object is evaluated based on the object or service provider's capability, commitment, reliability and feedback from others (Latif, 2022). The current trust-evaluation models primarily emphasize trust, the trustworthiness of objects that provides services; they do not consider the social relation between objects and characteristics of IoT objects; the social relation is non-static and volatile. Hence it is difficult.

The success of S-IoT application depends on the discovery of service providers, network navigability, trustable objects and reliable social connection among objects in S-IoT. The critical security attacks in S-IoT enrichments are self-promoting, whitewashing, opportunistic service attacks and ballot stuffing attacks. The authors in (Rajendran and Jebakumar, 2022) proposed a friendliness-based lightweight trust-evaluation model that ensures secure communication among devices. The proposed scheme leverages the friendliness property of a device or object in S-IoT environment. Objects' capability and credibility are computed based on mutual feedback from objects and friendship is maintained directly. The updated friendship directory is used to update a list of safe devices and secure communication among devices through encryption. However, the proposed scheme does not consider a community of objects while defining the trust of objects.

Amiri-Zarandi *et al*. (2022) leveraged Blockchain technology and social information of S-IoT objects and designed a trust evaluation method. The proposed trust-evaluation method is demonstrated on private Blockchain. The trust-evaluation model is resilient to threats and identifies or removes malicious nodes in the network.

Sagar *et al*. (2022b) used a knowledge graph to capture important trust metrics. The trust evaluation model considers current and previous transactions, reliability and fast behavior of an object and recommendation by other nodes. The neural network-based trust-evaluation framework is designed in (Sagar *et al*., 2022b). The proposed framework envisaged complex, nonlinear relations between objects, integrated present and previous interactions. An artificial neural network-based trust management model: Trust-S-IoT. Trust-S-IoT has been created to collect a variety of essential trust measures as input.

Table 1: Comparison between IoT and S-IoT

Environment	Architectural-components	Trust attributes	Features/ Characteristics	Challenges	Research issues
IoT	IoT gateways, IoT connectivity, smart IoT devices	Dependence trust, retribution trust, competence trust, fulfilment trust, reliability trust, temporal trust	Intelligence connectivity, sensing, analyzing, management,	Scalability, interoperability, self-organization abilities, Data management providing security, safeguards for privacy and data management maintaining of IoT nodes	Technology over-reliance, privacy issues, unemployment
S-IoT	Everything as a service (Eaas), socialized devices, manager of social relationships, reliability manager	Persistence trust relationship, desire trust, confidence trust, context specific trust, concentric trust, event sensitive trust	Object discovery, service composition, social interactions, social role, dynamic nature, intelligence	Combability, hardware device/ object-specific OS selection, I/O data, device setup, management, relationship management for objects	Facilitates laziness, reduces face-to-face communication abilities, Implications for ethics, abate the thoughtfulness and understanding

Table 2: Trust computation methods (recommendation-based)

Ref.	Methodology	Drawback
Khani *et al*. (2018)	This framework considers mutual friendship; QoS metric, feedback as recommendations and community-of-interest. The model performs well when tested against Bad-Mouthing-Attacks (BMA), On-Off Attacks (OOA), Self-Promoting-Attacks (SPA), and Ballot-Stuffing-Attacks (BSA)	No options are provided for adjusting trust standards in ever changing environments
Xia *et al*. (2019)	The model considers recommendations by other nodes, community-of-interest and context awareness. The model defends badmouthing attacks and grey-hole attacks	Not resilient against intelligent behaviour attacks and on-off attacks
Nitti *et al*. (2013)	The trust model considers both the objective and subjective credibility of a node. The credibility of the node computed is based on opinion or feedback	Transmission causes network traffic overhead. The model is sluggish to adapt to dynamic changes
Wei *et al*. (2020a)	The value and contribution of each trust are determined by experience and direct trust	The suggested technique comprises multiple trust attributes in order to determine the trust score
Chen *et al*. (2015)	The suggested model fine-tunes the trust parameters: Honesty, recommendations, a community of interest, and cooperativeness	Not resilient to on-off and intelligent behaviour attacks

Table 3: Trust computation methods (reputation-based)

Ref.	Methodology	Drawback
Truong *et al*. (2016)	A fuzzy based trust model considers experience; knowledge and reputation as trust metrics	The model fails to detect acting strangely objects
Truong *et al*. (2017a)	The proposed model uses trust-computation experience and reputation. The experience is defined in terms of neutral interaction, uncooperative, and cooperative. The reputation is classified the negative and positive reputation. The performance assessment is examined in terms of the algorithm's poor convergence	It is not stated how reputation and experience work together to determine an object's trustworthiness. There is no discussion of the trust computation and attacks linked to trust
Xiao *et al*. (2015)	This model uses two matrices, credit and reputation, to determine whether the nodes are trustworthy or untrustworthy	Direct observations and recommendations were not considered
Chen *et al*. (2016)	The model considers a device's social relationships, reputation, and energy status to determine the trust score	Model not resilient against trust-related attacks
Azad *et al*. (2020)	A decentralized trust management model to compute trustworthiness, reputation and experience	In the context of trust-related attacks, a performance evaluation of the model has not been done

Table 4: Trust Computation Methods (prediction-based)

Ref.	Methodology	Drawback
Aalibagi *et al*. (2021)	The matrix factorization, the Hellinger distance, and the bipartite graph are all used in a trust model based on the matrix factorization model to identify reliable nodes	The model is only suitable for a bipartite graph
Sagar *et al*. (2020c)	A trust-evaluation model that considers co-work similarity, friendship similarity, cooperativeness and community of interest has been proposed so as to nodes over a period of time	It is computationally intensive and has significant latency in a dynamic environment
Jayasinghe *et al*. (2018)	A data centric trust-evaluation model utilizes cooperativeness friendship similarity and community-of- interest	Not resilient against various trust-based attacks
Abderrahim *et al*. (2017a)	A community-based trust model considers recommendations, direct observation and sociability are proposed to find trust attacks	The behaviour of the model is not satisfied with other trust-related attacks
Marche *et al*. (2021)	Attack detection model based on SVM for trust-related attacks is considered perseverance score, usefulness score and goodness	There is no description of the many simulations parameters utilised for performance evaluation score

Table 5: Trust computation methods (policy-based)

Ref.	Methodology	Drawback
Al-Hamadi and Chen (2017)	Trust of an object is based on witness trust, rater's trust, location rating, reliability trust, risksand health probability for decision-making	Consider only static trust parameters
Chen (2018)	The model introduces a trust management model on quality of provider, bandwidth and energy status	The performance of the model is acted upon on a small number of hubes, which does not ensure scalability
García-Magariño (2018)	The framework that considers reputation and direct to identify hijacked nodes in the network	Not suitable for detecting BSA, OAA and BMA observation attacks
Li *et al*. (2017)	A secure and trustworthy model based on data observation and experience as history is proposed to assess the trustworthiness of both user and data	Policies are context-dependent and non-statistic

Cloud-based trust evaluation model is proposed in (Ali-Eldin, 2021). The proposed model computes trust based on subjective and objective scores of the objects and social similarity between objects. The model demonstrated how to compute social similarity among objects using friendship, shared interests and social contact similarities. Direct and global trust scores were computed as two measures of trust. In the future, machine learning techniques will be used to create a more complex social similarity model.

The trustworthiness of service providers is computing using edge computing interplay among the social network. The trustworthiness of the data provider is evaluated based on quality of the data and timeliness (Li *et al*., 2021). The reliability of the service requestor is evaluated based on local and global reputation.

Wei *et al*. (2020a), a context-aware trust framework for service delegations in the S-IoT is proposed. It creates a complete model of trust for the S-IoT by combining the trust theory along with social networks. The pair of competence, willingness and social connections will improve the effectiveness of determining trustworthiness. Additionally, the context dependent problem is addressed using the feature-property match approach. To protect against potential attacks A punishment mechanism and adaptive willingness calculation approach are proposed in (Wei *et al*., 2020a). The suggested trust model takes into account task features, object capabilities and object honesty, as well as the consequences of malicious behaviour. Experimental results suggest the sustainability of the suggested context aware trust framework and demonstrate its capacity to guarantee the effectiveness and security of activities in the S-IoT.

The cloud edge aided data model considers information diffusion and social interaction in S-IoT (Yi *et al*., 2020). Taking into account the interchange feature of data propagation and cloud-edge-aided social behaviour spreading, S-IoT hubs have recently been proposed as a coupling of the social owner and its linked IoT devices. Additionally, a model for cloud edge-assisted data diffusion from the specific edge in timely processing and feedback is proposed. Therefore, Blockchain-based trustworthy S-IoT design is suggested to address the information flare-up limit in the cloud-edge-aided connected framework. The Lyapunov approach is used to derive the steadiness investigation for the equilibriums. In the future, the S-IoT may be represented using tensor models and the link between various properties can be examined.

The author proposed a crossbreed trust management model for S-IoT systems in (Narang and Kar, 2021), which aims to exceed the limitations of current schemes. The System creates a Crossbreed Multi-Service-Social-Tie-graph (HMST) using a merger of human ideas and devices (or artificial). The OSN social tie-graphs of IoT device owners are the human insights aid to the HMST. Device intelligence is provided by IoT devices within the context of direct opinions for other devices, leading to the development of device social relationships inside the HMST. Each social relationship inside the HMST has a probability value associated with it, representing the accuracy of its evaluation of trustworthiness. The quantity of data distributions and computing requirements at IoT devices are reduced with the enhancement of static and dynamic trustworthiness evaluation techniques. The system just requires a few easily adjustable parameters to be regulated and is simple to set up and broadcast in a S-IoT network. As demonstrated by both hypothetical and simulated analyses of the system, the framework strengthens trust management by remaining trustworthy under various attack scenarios.

Social group crowdsourcing issue within the S-IoT systems is addressed in (Liu *et al*., 2021). Smart devices with effective detecting capabilities can act as either the information sensors or information requester. A social group crowd sourcing solution for Social Web of Things frameworks, Trust Aware-sensing-Quality-estimation-for-team-Crowd-sourcing (TAQ-Crowd), was designed by the author in (Liu *et al*., 2021). The TAQ-Crowd, to begin with, incorporates the consideration of trustworthy connections between nodes into sensing data quality assessment for the TAQ model plan. After designing a task assignment algorithm i.e., CS-Selection, detecting quality guides the participant choice to maximize the overall assignment valuation under a budget constraint. Understanding the group crowdsourcing issue comprises two coupled NP-Hard problems: Participating device selection and task coordination. The greedy task assignment approach can reveal the two coupling concerns by transforming them into an essentially submodular cost submodular knapsack issue.

For a distributed S-IoT system, the author presented a reliable group based service management approach termed as TGSM (Farahbakhsh *et al*., 2021). The proposed method has a few distinct characteristics. First, according to the author’s approach (Farahbakhsh *et al*., 2021), selfish objects could be effectively isolated by employing a punishing mechanism is based on the accuracy and consistency of the input received from the service. This technique encourages the objects to provide honest feedback and services, suppressing their selfishness. Farahbakhsh *et al*. (2021) used the HITS algorithm as a dynamic worldwide strategy for evaluating reputation/trust. The author intends to develop a game theory based punishing mechanism for a reliable, trustworthy model, which will help to evaluate how well S-IoT trust model functions. Utilizing machine learning methods to detect object behavior patterns to defend against various attacks is another area that may do more researched in the future.

It is proposed in (Aalibagi *et al*., 2021) to use Hellinger distance which builds a social network of trustors as an innovative trust administration method in the S-IoT using the trustor’s experiences and the opinions of its friends. The trustworthiness value of a trustee is predicted. Aalibagi *et al*. (2021) created a social trust model employing centrality and similarities measurements to use the feedback. The proposed technique takes into account IoT devices’ resource constraints and concerns with information sparsity. Evaluating the converging, reliability and attack resilience characteristics of the proposed mechanism’s variety of settings in an adversarial S-IoT environment allowed us to assess the applicability of the suggested trust management mechanism. The simulation suggested that the suggested approach successfully reduced the cold start issues, provided resilience to related attacks and assisted trustors in identifying reliable trustees. In further work, the author intends to model the S-IoT using hypergraphs because it was discovered using naıve edges.

Marche and Nitti (2020) has examined the many attack techniques that nodes may use to disrupt an IoT system. The developed trust management approach (Marche and Nitti, 2020) was constructed for a Social IoT scenario using a machine learning technique. The suggested approach (Marche and Nitti, 2020) has been tested against all forms of attacks, with the exception of the Sybil Attack (SA) as well as the Self-Promoting Attack (SPA), which are ignored by default. Studies have shown that the proposed approach can resist any attack. Additionally, contrast the suggested approach with the following two widely used state of the art models: According to simulations, even though the suggested algorithm performs slightly worse when subjected to attacks by simple and direct processes, such as Malicious with Everyone (ME), can also outperform the other two designs if taking into account a network through various attack types.

Babar and Mahalle, (2021), the author reviews the S-IoT model, the basics of trust, its characteristics and a model for trust computing. (Babar and Mahalle, 2021) has presented recent research works on S-IoT trust attacks and trust management. Malicious devices that carry out attacks on a system can be distinguished using a challenges and trust management system employing Machine Learning Algorithm (TM-MLA). To fix the weighted sum’s past problems, the TM-MLA model uses a machine learning based trust aggregation model. TM-MLA eliminates the limitations of the past trust update. It is, therefore, a more reliable procedure.

The author developed a novel fuzzy logic-based approach for identifying dishonest hosts and nodes in the S-IoT (Ouechtati *et al*., 2021) based on social relationships and recommendations. The proposed approach (Ouechtati *et al*., 2021) includes two major measures: (1) The assessment of the amount of confidence in the received suggestions and (2) The recognition of good mouthing, bad mouthing and Sybil attacks. It filters out dishonest hosts using recommendations and social relationship scores with other nodes. The Sybil, good and bad-mouthing attacks may all be identified using the proposed approach (Ouechtati *et al*., 2021).

An updated trust-related attack known as a manipulator was just introduced in (Ugur, 2021). Manipulator attacks are based on a set of trust values considered so far in the trust management framework. These trust values hold together and safeguard from known attacks. The proposed system adopts a proactive approach to finding trust values that are not found/determined due to decision malicious nodes. It finds new trust values from non-malicious nodes using friendly relationships. A number of vulnerable trust management strategies are proposed as protection against manipulator attacks.

In the S-IoT, trust-based cluster and optimized Routing algorithm for Low-Power and Lossy networks (RPL) are proposed in (Selvaraj *et al*., 2022). The cluster constitutes a high-trustable device and low-trustable device with similar interests and categories of device. The trustable-device-based cluster helps trustable devices in the data transmission process. A cluster of optimization scheme is used to optimize RPL performance by selecting trustworthiness nodes as the next forwarding nodes. The optimization approach is used to assess RPL performance by picking trustworthy nodes as the next step in the routing process. The trusted community and optimized RPL are an effective scheme for trust-based information transfer in S-IoT network.

Azad *et al*. (2020) have solved the problem of finding the trustworthiness of the nodes and IoT devices in the S-IoT. The author has designed a novel framework without considering a trusted third party to compute and update contestant nodes' trustworthiness in S-IoT Network. It uses homomorphic encryption to protect the privacy of participant nodes in S-IoT Network. The homomorphic encryption employs self-enforcement features to verify the trust score of every device attached to S-IoT and the trust score of every device is auto update. However, utilizing the prior trust grade and the most recent record of votes cast by its network neighbors. Every node or participant enforce to follow the zero-knowledge proofs protocol. This system guarantees correct computation, security and privacy of the nodes or users even if they have malicious nodes and are working secretly with users. The limitation is that it does not use any centralized trusted system; each node has to maintain the trust score.

Khanfor *et al*. (2020) devised or formulated a solution for the spatial recruiting process in Spatial Mobile Crowdsourcing (SMCS) platforms using S-IoT systems. A community detection technique is used in the proposed approach to reduce the number of trust work acceptable workers to be assigned to the recommended device to complete the assignment. The candidate set is then subjected to an Integer Linear Program (ILP) in order to optimize and produce the best suited collection of workers.

Jafarian *et al*. (2020) have described procedures for discriminating behavior among objects. Objects generally do not deliver the same range of services under specific conditions. The selfish attitude might be linked to a variety of factors, including a lack of resources, stronger links with other entities and so on. To overcome this problem, the authors suggested a Discriminative-Aware-Trust-Management (DATM) system that computes trust value using a weighted-KNN algorithm for trust evaluation. The total of each service provider's previous and current ratings is used to calculate this number. The context of the current service inquiry is compared to the contexts of other rater's queries to determine the weight of each rating.

Aslam *et al*. (2020) presented a service-oriented trust evaluation technique for the S-IoT scenario. A metric called Service Trust is presented after aggregating and analytically modeling the trust evaluation metrics. Service Trust and the modeled parameters have a positive association according to the dataset analysis. The type of correlation remained constant as the number of invalid/malicious services in the network increased. This research can be useful for future work by examining which trust assessment technique should be employed under different scenarios.

Talbi and Bouabdallah (2020), a model for interest based trust management in the S-IoT is proposed. This system evaluates whether S-IoT devices are trusted while considering the trustor's interests. In order to advance the field of the specified services, it gives a contemporary proposal framework based on the trustor and the recommender's proximity in terms of their shared interest preferences.

Sagar *et al*. (2020a), it was suggested to determine a unique trust grade for every S-IoT node using a machine learning based trust aggregation approach. Information is classified using k-means clustering to identify the reliable and unreliable interactions to collect the trust. A further suggested trust prediction system is used to identify the decision thresholds and calculate the effect of different variables on the total trust score. Finally, the simulation results show improved accuracy in identifying trustworthy interactions. In future work, research is anticipated to take interaction experience with other devices into account when calculating both direct and indirect trust.

Amiri-Zarandi and Dara (2020) have proposed a Blockchain based trust methodology for social IoT. The Blockchain-based framework is a secure and transparent mechanism for trust evaluation. Data entropy is used to access the reputation and other parameters of the device. The proposed trust management scheme efficiently identifies a device's trust score, managing devices in S-IoT. The proposed framework is robust and resilient for various attacks in S-IoT. Amiri-Zarandi and Dara (2020) also presented elements to consider when considering how the trust management framework may be utilised to invigorate social links among IoT devices based on reputation and mutual interactions.

Sagar *et al*. (2020b) explores the characteristics of objects in S-IoT in terms of personal interest, the community it belongs, workgroup, co-work relationship, friendship similarity, social status, etc., the objects similarity w.r.t characteristic. The dynamically weighted sum approach is used to synthesize the trust factors. Finally, the simulation results illustrate how the objects' trust alters over time in relation to the trust characteristics. Sagar *et al*. (2020b) recommends creating an attack model to test the correctness and convergence of the suggested model in a continually changing S-IoT environment.

Sagar *et al*. (2020c) presented efficient time aware trust evaluation methods to identify misbehaving devices in the S-IoT network. The suggested trust model uses similar persons, a community of interest, friendship, cooperativeness and coworker to measure trust. A machine learning driven aggregating technique is described by Sagar *et al*. (2020c) in order to combine various trust characteristics and determine a trust score for devices. Through the separation of trustworthy and untrustworthy items, simulation results demonstrate the model's suitability. They also show the variation in each hub's trust score over time. In future work, it is possible to confirm the proposed model's convergence and adaptability properties by implementing context-awareness in a dynamic S-IoT environment.

MS and Buyya (2020), the author looked at trust management in service-oriented S-IoT systems. In a service-oriented S-IoT system, locating a reliable service offered by a service provider is a crucial problem. The suggested trust management system is based on monitoring the present and previous behavior of objects and differing viewpoints on the trust of an item assist in comprehending the behavior of the object. The simulation results indicate that the suggested trust scheme TMSOS outperforms all other ATMS schemes. In the future, machine learning-based technologies will be utilized to identify trust related threats in S-IoT systems to counter them.

Wei *et al*. (2020b) focuses on the structure of S-IoT and trust management difficulties in S-IoT, as well as a blockchain-based trust management model for S-IoT. The blockchain-based S-IoT system can successfully prevent the Bad-Mouthing Attack (BMA), Self-Promotion Attack (SPA) and Ballot Stuffing Attack (BSA) due to the tamper resistance of the information in the Blockchain. Moreover, the information behavior of an object is vital in S-IoT. The malicious node's disposal of bad histories by leaving and re-joining the S-IoT, can be restricted. Blockchain technology, based on a trust management model, can secure interactions, services and ensure the adequacy of the trust management model in S-IoT. Furthermore, an efficient trust calculation technique based on Blockchain data improves the accuracy of object behavior evaluation and prediction.

Rehman *et al*. (2020), smart cities can benefit from introducing new services thanks to the information that residents submit on Online Social Networks (OSN). Additionally, implementing regional and global trust reduces the blending of fake data. The author identified the maintainable OSN that may be utilised to learn about people's opinions inside a smart city in (Rehman *et al*., 2020) used the suggested model to analyze three types of social networks. The objective of the analysis was to validate the model based on regional and global factors related to trust. The suggested model is also employed to research the problem of social network sustainability. Rehman *et al*. (2020) demonstrates that removing the most trustworthy individuals from networks considerably reduces the number of hubs. Only 36.3, 90.03 and 43.32% of hubs remain in the network after filtering on the social media sites Facebook, Twitter and Slashdot, respectively.

The author suggested a deep learning method based on a contemporary approach (Masmoudi *et al*., 2019) to recognize the types of trust related attacks conducted by malicious hubs. The model segregates such malicious hubs to attain a trustworthy environment. This method is according to supervised learning. Masmoudi *et al*. (2019) demonstrated the execution of the suggested attack detection framework with a recall rate of 94.4% and an accuracy value of 95.63%. This study will be expanded to define/design a trust management framework at the device level. This device level allows for the measurement of trust for the device node.

TOT, an energy and trust-aware opportunistic transmission strategy for CR-S-IoT, is suggested in (Wang *et al*., 2020b). Wang *et al*. (2020b), the author developed many forms of flow-oriented forwarding candidate selection algorithms based on optimum stopping theory. In addition, a new trustworthy channel assignment technique based on predicted network gain is created. Furthermore, the suggested secure OR outperforms CAODV, SoRoute, CANCOR, RTOT and ETOR. In the future, trust and cryptography will be used to increase the safe OR protocol's energy efficiency.

An enhanced trust expectation technique for the S-IoT is presented in (Wen *et al*., 2021). The proposed model overcomes the problem of frequent cold start issues in networks. The trust value assessment of new hubs may be affected by the huge delay imposed by the slow response issue. In an unusual approach, the suggested model proposes using a deep learning model, similar to the S-IoT server level trust model, to assess and forecast the trust value of linked nodes. The good hubs may be distinguished from the new hubs with great trust. It has the potential to significantly reduce the effect of malicious attacks on the malicious node.

Xia *et al*. (2019) discusses an efficient trustworthiness inference framework to prevent various types of malicious attacks and classify trust elements. After constructing an overall framework, classify the trust elements is arranged in an orderly manner. Subsequently, the author in (Xia *et al*., 2019) have presented methods to find different trust elements. Further, the fuzzy logic-based method has to introduce to synthesize trust elements. The author of (Xia *et al*., 2019) presented a technique for testing in two areas: Resistance to attacks and impact on network services. The extension works further verify a developed model's accuracy, convergence and resilience under dynamic changing environments. Analyzing how the framework for trust contributes to forming social connections is another approach.

Amin *et al*. (2019a) highlighted the importance of the S-IoT architecture's requirement for various definitions and notations. The need for architecture is supported by a number of factors, including the connections between the S-IoT and industry 4.0, the function of multi-agent systems in the S-IoT, the relationships between clusters and IoT nodes and the interaction between the social IoT and the cloud. Friendship-based architecture is expressed at the fundamental level. Service search, service composition and the service model are three partitioned groups in this design. Also divided into the trust updates, trust aggregation and trust formation groups are the trust-based group. Contrarily, there are three main categories of trust aggregation: Trust theory, Bayesian systems and dynamically weighted sums. The trust update department is split into two categories: Event-driven and time-driven. Future research should focus on analyzing novel social trust metrics and the best method to integrate them for S-IoT trust computation.

The author presents a unique residual energy dependent time variable trust calculation technique for SloT systems in (Premarathne, 2019). The results show that the suggested technique is suitable for identifying malicious nodes when attacks may violate social relationships. In contrast to the current trust computation metrics, context-dependent malicious behaviors are detected in the inconsistent trust across the network. It is suggested that the experimental confirmations be expanded to a larger network and additional SloT attack situations as future work.

To full fill, the objectives of IoT-Trust model (Um *et al*., 2019) proposed a framework for managing trust information. Trust information plays a vital role in building trust among various types of devices such as sensors, user digital equipment, network gateway, home gateways and cyber objects. Reliable trust information helps in decision-making and providing commercial services. The proposed framework consists of trustable agents, a trust information system and a broker, who provides trustworthy, secure information between physical objects, virtual objects and users. The framework enables a trustworthy ecosystem and social IoT to build a business.

Lin and Dong (2017) presented a new model for the S-IoT to overcome the drawbacks of the pre-existing trust mechanisms. Six fundamental components make up its relational structure: (1) The context, (2) The trustworthiness evaluation of the trustee, (3) The decision and its consequent action and result, (4) The trustee, (5) The goal and (6) The trustor. The trust model stands out for five reasons: Inferential transfer of trust with similar responsibilities: Mutuality of trustor and trustee; transitivity of trust; trustworthiness impacted by a changing environment; and updating trustworthiness with delegation results. In the suggested trust model, the trustee and the trustor conduct a bilateral evaluation of trustworthiness. This evaluation process prevents malicious nodes from performing a single parameter. After engaging in malicious behavior in one task, a node's future evaluations in tasks of a different kind that share one or more of the same features are affected. Malicious activities can be efficiently identified in this way. Finally, this model takes the changing environment into account while calculating trustworthiness. This makes it easier to discern between bad conduct and typical behavior in hostile environments.

Khani *et al*. (2018), the author recommended three trust settings for each device in S-IoT contexts, covering the devices' state, their surroundings (including time and location) and the activities they are performing. Khani *et al*. (2018) suggested a Mutual-Context-Aware-Trustworthy-Service-Evaluation (MCTSE) approach. The MCTE model was successfully designed and can distinguish between honest and dishonest devices. Future studies must propose the Mutual Context-Aware-Trustworthy-Service-Recommendation (MCTSR) model and validate it using more extensive datasets.

Ruggeri and Briante (2017) have developed social-aware e-health and IoT framework. The proposed framework is divided into five planes: (1) Objects, (2) Social Objects (S-Obj), (3) Network, (4) Virtual Entities (VEs) and (5) User. The object plane is the lowest plane, consisting of object/device capable of detecting and controlling the physical environment, such as sensors and actuators. However, due to their restricted resources and skills, they cannot form social relationships with comparable objects. The social object plane comprises smart SOs with storage and processing capabilities that can conduct sophisticated activities such as communicating and working with their peers to accomplish a specified objective. S-Obj contains both the social gateway S-GTW and the advanced application hosting device A-AHD. Together, S-Objs can communicate and send all data from the physical world to higher levels. A S-IoT based middleware is used to carry out S-Objs mutual authentication, resource discovery, social connection management and S-Objs registration. The VEs plane, often referred to as the application plane, comprises the VEs, which are in charge of processing raw input from the real world to provide enriched data and initiate real-world operations. Two examples of VEs used exclusively are the E-Butler and the virtual doctor.

Abderrahim *et al.* (2017b) CTMS-S-IoT is a centralized trust management system comprising a local Trust Management System (TMS) inside of a central TMS and each object on a trusted server. This TMS uses a decision tree tool to choose the most reliable objects that can offer the needed service in each scenario. The author considers both recent past behaviour data of a social object and context network to compute trust value of a social objects. The proposed approach considers the context of network, the ability of an object and the social relation among the objects. The proposed approach uses the decision tree to analyse the social relationship between various network components and the behaviour of objects. The proposed approach is dynamic and scalable.

Truong *et al.* (2017a) have designed novel trust evaluation model that evaluate the trust of physical objects, agents, service provider, in terms of opinion, direct observation and historical experience. The authors list three crucial qualities: Trustor inclination, trustworthiness and environmental issues. The public is given an evaluation of a trustee's trustworthiness based on their reputation, which is derived by gathering both negative and positive input from transaction participants on completing a particular task. Three qualities are used to calculate knowledge (a trustee's understanding): Ability, goodness and honesty.

The trustworthiness of physical objects, agents and service providers is decided based on the behaviour of objects. Meena Kowshalya and Valarmathi (2017) determines trustworthiness based on S-IoT trust parameters such as object centrality, direct trust, community interest, community of objects, cooperativeness, trust score and trustworthiness among devices. The method collects the past behaviors to compute trust and predicts futuristic behaviour protect the system from malicious objects. The periodical trust up-gradation isolates and guards against 'on off' attack. The suggested trust management system performs better in recovering the trust value of objects and total isolation of "on off" attackers compared to other current trust management methods.

Jayasinghe *et al.* (2017) focuses on classified devices as trustful devices and trustless device evaluating devices trust is significant because dishonest trustees can significantly affect the smooth execution of application-level forms as compared to other TMs. Jayasinghe *et al.* (2017), the author identifies characteristics that have been carefully considered and have a direct impact on the honesty TM. A successful alternative to the weighted summing of qualities, the author in (Jayasinghe *et al.*, 2017) offered an expectation method to predict future levels of honesty using various regression approaches. Future work will include developing a trust evaluation method that considers other important TMs and third-party ideas. Combining TAs and TMs, which provide an additional degree of confidence, is also crucial. As a result, numerous alternative prediction processes, including machine learning approaches, will be explored.

The trust in S-IoT reflect reliable, interaction, honest among objects. Premarathne, (2017) proposed a multiplicative attribute graph-based trust calculation. A reputation based trust model computer trust based number of edges among devices using directed analytic graph. (Premarathne, 2017) used multiplicative attribute graph to compute trust, where in association or affiliation between devices attributes indicates of two edge/social connections. The trustworthiness of device is based on direct observation, opinion of other devices and nodes credibility and centrality.

Truong *et al.* (2017b) provides a comprehensive trust evaluation method in S-IoT based on Reputation, Experience and Knowledge (REK). Truong *et al.* (2017b) examined vital Trustworthiness Attributes TAs of objects/agents from past historical interaction with other objects. To compute the knowledge attribute of objects, it considers three measurements capacity, goodness and integrity. Truong *et al.* (2017b) developed a mathematical model for Experience and Reputation. Further, Truong *et al.* (2017b) combines Knowledge, Experience and Reputation attributes by utilizing Semantic Web innovations for finalizing the overall trust value.

Abderrahim *et al.* (2017a) addresses trust administration in the S-IoT. In (Abderrahim *et al.*, 2017b), the author suggests a clustering design based on similarity of interest, with an administrator in charge of each cluster. Abderrahim *et al.* (2017a), the author develops the Trust Management Community of Interest (TMCoI)-S-IoT, a contemporary, trustworthy trust management framework for the IoT. In (Abderrahim *et al.*, 2017b), the author introduces a trust value assessment system based on an expectation mechanism. In future works, TMCoI-S-IoT can be progressed to identify more attacks.

For social IoT systems, (Chen *et al.*, 2015) have created and examined the adaptive trust management protocol. In distributed adaptive trust management protocol, every node updates its trust to other nodes in the network. The protocol performs a trust test and updates both direct observations, it indirect recommendations for other trusted nodes. It is the social connections involving the holders of IoT devices. Before developing an adaptive trust management protocol, the author considered the design tradeoff between trust management and trust fluctuation. A social IoT application is employed in the adaptive trust management protocol to determine the appropriate trust parameter.

In order to develop a versatile crowdsourcing network that can be used for extensive crowdsourcing applications. Wang *et al.* (2016), the author suggested a reliable crowdsourcing methodology for the S-IoT. This model presents the concepts of the social cloud and detecting entity. To actualize social data linkages, a message sending algorithm based on a social awareness component is exhibited within the sensing entity. An auction mechanism is incorporated into crowdsourcing to carry out winner selection and compensation determination by analysing the reliability of crowdsourcing participants and detecting untrustworthy individuals. Wang *et al.* (2016) points out a few investigative challenges on the trustworthiness of crowdsourcing.

Truong *et al.* (2016) presented the proposed trust service platform is used to assess trust between two entities in S-IoT it offers services. To figure out whether a person, service, device is trustworthy, the trustor considers knowledge and opinion from other entity/device and trustee's reputation. Truong *et al.* (2016) imitate the human process in assessing trust if incorporates recommendations, reputation of trustee, direct observation or knowledge on devices. The proposed trust model continuously updates recommendations and reputation of device/service. The author used fuzzy-based algorithm to measure knowledge, personalized utility theory to calculate trust score, feedback/reputation-based system to determine the reputation.

Kokoris-Kogias *et al.* (2016) is shown the important categories of malicious attacks that may come from an IoT entity-based system. Three main forms of harmful conduct are identified by Kokoris-Kogias *et al.* (2016) and may be combined to create a variety of distinct attacking scenarios. In order to enable rapid detection of the above attacks and improve the quality of service in the IoT, (Kokoris-Kogias *et al*., 2016) makes a clear difference between Trust and Reputation and introduces TRM-S-IoT, a T & R model. Kokoris-Kogias *et al*. (2016) compares the TRM-S-IoT against the most popular T and R models to demonstrate the viability, performance and scalability of TRM-S-IoT. In future development, the suggested model must be validated in the Cosmos project's real-world use-case scenarios and implemented to true IoT-systems to exhibit the biggest gain.

Jayasinghe *et al*. (2016) suggested a trust computation model (RpR) based on recommendations and reputations offered by objects in a distributed S-IoT scenario. First, the model distinguishes and recognizes the implications of recommendations and reputation in S-IoT and the significance of these measures in measuring trust. Then, the author (Jayasinghe *et al*., 2016) has used reputation and suggestion to assess the trustworthiness of each S-IoT object. The author explicitly analyzed important characteristics, including convergence, accuracy and resilience against misleading or deceptive conduct through a simulation. The suggested model provides a reliable technique to accurately calculate trust for thousands of items within a few iterations, particularly with the degrading feature over time for unreliable objects. Finally, (Jayasinghe *et al*., 2016) provided examples showing how the suggested algorithm performed better than other well-known ranking methods.

Xiao *et al*. (2015), a brand-new trust model for the Internet of Things, the Guarantor and Reputation based trust model is put out. Cyber-physical devices are referred to as social objects mimic social behaviour of human and develop a social relationship with other cyber-physical objects. However, objects social relationship with other objects depends on trust between objects. Cyber-physical objects can trust other edges' physical objects based on reputations, the information provided by other objects and the credits of objects.

D. Friend Selection

Rajendran and Jebakumar (2021) proposed a Grey-Wolf algorithm for Smarter Object Recommendation (SOR) and object affiliation. The author proposed a maximum-ranked neighborhood method for the selection of objects to form a social networking and navigating network. The proposed method ranks each object based on the Satisfactory Factor (SF) computer/identifier the smarter objects based on the Greywolf algorithm. The author analyser five distinct models for object recommendation. The five distinct models include common object prediction, social similarity, Ranking, GWA + Ranking and SF + GWA + Ranking. The desired service is delivered using a well-established friendship relationship.

The success of S-IoT application depends on service provided objects and the trustworthiness of objects. Mohammadi *et al*., 2021) utilised optimized decision theory for the selection of trust full object and friend of trust full object. The trust full friend selection process considers objects characteristics, past behaviour, functionality and topology to which the object belongs number of links and degree distribution. Mohammadi *et al*. (2021) proposed a method for choosing trustworthy friends. The suggested model from (Mohammadi *et al*., 2021) was then tested using the Netlogo simulator and compared to various scale-free architectures such as large components, Barab'asi-Albert networks and Random networks. The designed framework identifies each device's neighbor and constructs a communication topology based on a social network (Ching *et al*., 2021).

Ramasamy and Arjunasamy (2017) suggested metrices to be used while selecting objects friendship links are (1) Number of friends node harm. (2) Closeness of nodes to form a cluster. (3) Number of the node connected. (4) Shortest path between any two nodes. The heuristic approach for friendship links are given in Ramasamy and Arjunasamy (2017) suggested some strategies overcome limitation of heuristic approach.

Girau *et al*. (2016) have proposed three algorithms for network discovery; specifically, the first algorithm relies on channel scanning to discover neighbours, the second algorithm relies on device localization to discover these neighbours and third algorithm expands the existing network with new lines. In S-IoT, objects establish object socialization that enables inter-object communication. To implement objects social relationships, there is a need of neighbour discovery and communicate with every neighbour on network.

It is necessary to define the right rules and follow rules to select the right friends in S-IoT. The right object can provide the designed desired framework in (Nitti *et al*., 2014). In S-IoT, a node is an object that has capable of establishing social relationships with other objects according to rules set by the owner. Specifically, the rules are: Node can accept a new final relationship request if 1. A node accepts a friendship request until it reaches the maximum number of connections allowed. 2. A node accepts friendship request if minimize the average degree of its friends and 3. A new request is accepted if it minimizes its own local cluster coefficient.

It is necessary to route the data collected by the object to other objects in S-IoT applications. Hasan and Al-Turjman (2018) designed a K-disjoint routing path to route data between the source object and the destination object. The K-disjoint routing path algorithm assigns an object with a transmission range according to hop distance.

The S-IoT has the potential to provide service more effectively and efficiently. The data collected objects (devices) are delivered via multi-hop-device-to-device communication. Wang *et al.* (2017) proposed distributed scheme to enhance the overall success rate of context sharing between context helper and context requester. To minimize the success rate author considered optimized coding parameters, repair internal, selecting new caching objects (nodes) to repair the lost data, selecting Context-Helper (CH) for context requester and allocation of CH to new caching nodes.

Yang *et al*. (2021) to use the Formal Concept Analysis (FCA) theory to effectively identify maximum cliques in Online Social Networks (OSN) and control their growth. However, the properties of dynamic changes in maximum cliques in OSNs have not been taken into account. To aid clique discovery, (Yang *et al*., 2021) proposed two calculations: Add-FCA and Dec-FCA. The proposed algorithms can promptly and accurately identify the four categories of maximum cliques-namely, unaltered, modified, added and disappeared maximal cliques (Yang *et al*., 2021).

It is necessary to design/create a required topological structure of smart objects in S-IoT for providing various services and supervision of smart objects and discover smart objects. Hao *et al*. (2020) proposed maximal-clique to the relation between node/objects characterise common attributes for a given set of objects.

Amin *et al*. (2018), completely focused on different algorithms utilized for community detection. Amin *et al.* (2018), the author explored various graph-based network metrics, including algorithm complexity and network measurements, along with a comparison of them all. Amin *et al*. (2018), the author also presented many complicated network tools such as Gephi, Pajek, IGraph and NetMiner separately by highlighting their goals in terms of algorithm execution time.

Aljubairy *et al*. (2020), proposed a methodology called S-IoT Predict was proposed for forecasting future S-IoT interactions. The proposed method has three phases. In the first stage, raw movement data from IoT devices that are mobile and stationary is gathered. At stage 2, S-IoT temporal network sequences are formed based on the unprocessed IoT device movement data seen in stage 1. It is accomplished by extracting locations from movement data in their raw form, locating stays and labelling each stay with the extracted places. The number of connections between IoT nodes is evaluated by applying the Sweep-Line-Time-Overlap (SLTO) method. The Bayesian nonparametric model forecasts future connections among items at stage 3.

The topic of link selection in the S-IoT was discussed in Amin *et al*. (2019b). In this research, objects form friendship relationships with one another, forming a social network of items. First, look at network navigability in social networks using example-based scenarios and simulations because it’s crucial for service discovery. Second, suggested an enhanced method with a threshold value that can be dynamically altered based on number of hubs in network decentralized service discovery, the algorithm is executed to create new linkage and eliminates existing common friends. When one friend’s discovery is complete, the second hop’s search begins with a new friend. This phenomenon allows one friend to link with a high-degree friend, resulting in an increase in the network’s object navigability. In future work, it is possible to merge similar features in the same circumstance while utilizing trustworthiness.

Kim *et al*. (2017) displayed an end-user programming interface for the new S-IoT paradigm. Kim *et al*. (2017) described a new social interaction amongst gadgets to learn about and find fixes for new devices. Users can create their own rules and distribute them to others using the end user programming tool. Data about the user, connections between devices, social connections and services are all represented as semantic models that define their own rules. In a user research with 12 participants, none of whom had any programming knowledge, Socialite was used to create automation-based rules, rules including social interactions and new rules that the users wished after some practice.

Rabadiya *et al*. (2017) have analyzed use of S-IoT, IoT in social S-IoT, explored its evaluation history of S-IoT form IoT.

Arjunasamy and Rathi (2019), suggested a heuristic for choosing device mates without deviating from the mission of a device in a more sensible S-IoT network. An S-IoT network is simulated with incredible effort. When choosing friends, the reachability of the gadget and the service environment are given consideration along with navigability and the purpose of the device. This research focuses on navigability without compromising the essential objective of the device. It is challenging to accomplish a traversable network without averting from the objective of each device. Utilizing a more proficient rule set makes S-IoT more alluring future technology.

In S-IoT, paradigm boosts human-machine smart device interaction with a social network. IoT convergence is a wide range of technologies explicitly sensing, computing, information processing, intelligent control technologies and networking. An appropriate intelligent system/mechanism is required to integrate object, service provided by objects and people to handle data between them. The author in (Hussein *et al*., 2017) proposed a framework that discover services, objects, the proposed framework derive users' needs and accordingly it constructs social structure of objects, where it contains objects and smart service that could satisfies the requirement of user. Semantic service modelling algorithm matches objects, service offered by objects to user requirement.

Saleem *et al*. (2016), suggested a three-tier S-IoT design for service recommendation incorporating three layers: The interoperability layer, the network layer and the perception layer. Sensors and actuators, RFIDs, cameras, sensors and actuators and mobile phones are just a few examples of heterogeneous devices that detect and gather data and information at the perception layer. These devices then employ S-IoT techniques to build social networks and friendship group among themselves. Network layer must convert data from the perception layer that is received from IoT devices into telecommunication protocols before being transferred to the top layer for processing. Due to each IoT application's unique semantics, the interoperability layer is in charge of sending data between distinct IoT apps. The recommendation system is in-charge of collecting application data from IoT apps and data from the interoperability layer. In addition, it builds and manages social networks and profiles for objects and people using S-IoT data from the perception layer.

Wu *et al*. (2022) proposed a solution for item recommendations in S-IoT. The author explores and captures user interest and social influence, while item recommendations is more relevant in S-IoT since user interest and social networks change dynamically.

In S-IoT, it is essential to recommend suitable, available smart objects and services that meet users' requests. To facilitate smart objects, smart services recommendation on the basis of user need at a different time interval. Chen *et al*. (2019) proposed object recommendation mode that considers user's preferences at different times and the social similarity of objects. The authors in (Chen *et al*., 2019) uses a latent variable model to understand the user's preferences towards objects. The knowledge graph is designed/constructed to model to social relationship of smart objects. Finally, time-aware recommendation of objects is made on basis of learned user preference of the social relationship of objects.

E. Resource Selection

Ahmed *et al*. (2017) highlighted the benefits of social aware and device to device interaction convergence. Further discussion of the evolution of device to device interaction with regard to resource allocation and optimization may be found in (Ahmed *et al*., 2017). The author has proposed guidelines for resource allocation, optimizing resource allocation and requirement for social awareness enable device to device communication.

An effective and efficient resource allocation and selection in S-IoT is a challenging task. The process of resource allocation and resource selection can be either proactive or reactive, the available resources in S-IoT have classified a consumed resources and computational resources. The computational resources process the data and consumed resource sense data. Metrouh (2021) proposed two algorithms for computational, consumed resource selection allocation. The proposed algorithm checks/identifies location of resources and availability of resources. The algorithm collects user's resource requirements and performs selection of resources on the basis of parameter collected from user.

The success of S-IoT application is predominately determined by the way object interact with each other, the cooperative social behaviour of objects and common resource sharing among objects. The success of S-IoT application is predominately determined by network structure is mobility modes of objects. Zia *et al*. (2021) analysed profile based mobility. Impact of profile-based mobility on sharing common resources among objects of S-IoT. The author introduced two behaviour variables to extent i.e., scale. The extent represents the number of destinations an object has the scale represents how far away a destination is from another destination.

Applications of S-IoT

From the literature study above, some applications are listed below:

- Easing remote monitoring
- Managing industrial plants
- Managing cities and homes
- Monitoring the environment
- Providing automation and context detection
- Handling the vending machine section
- Overseeing healthcare systems

- Metering services (utility meters)
- Controlling facilities (elevators and energy)
- Pursuing and locating (rental bicycles and fleets)
- Maximizing engagement with social Gamification
- Influencing the ability of heterogeneous objects and services from different manufacturers
- Strategies for coordinating in a cooperative system where instances, social entities, places and data are coherently communicated with one another
- High levels of capability and resource heterogeneity.
- Handling naming services, migration and virtualization platforms
- Managing context acquisition
- Uncertainty regarding the reliability of a particular thing

Conclusion

IoT consists of sensors, actuators and other physical objects with each other over the internet. IoT enables physical object-physical object interaction and human-human interaction. However, existing techniques of IoT have failed to address emerging problems like human-to-object interaction, effective service discovery, efficient network navigability, scalability and exploiting the object relationship. In recent years, social networks enriched people-to-people interaction by allowing people to share opinions, thoughts, videos, images and sarcasm on topics of interest. Social-Internet-of-Things is a new paradigm that evolved due to the convergence of Internet-of-things concepts and social networking concepts. S-IoT extended to include the social interaction between social objects and discovering physical objects and their services. IoT only supports physical object-physical object interaction and human-physical object interaction. In addition to these two interactions, S-IoT adds human-physical object interaction using the social relationship. This study emphasizes recent research related to S-IoT from multiple views. This article gives basic knowledge, key concepts, distinguishable features of S-IoT and existing research challenges. This study has thoroughly reviewed the trust-evaluation model, secure communication protocols and privacy-preservation techniques. This survey enables researchers to understand existing techniques and find research gaps. We analyzed and compared trust-evaluation models on different parameters. We also highlighted their core concepts and weakness. As Future work, we planned to do a systematic exclusive survey on trust-evaluation models, research tools, publicly available datasets and use concepts of machine learning and deep learning techniques in the context of service discovery and network navigability in S-IoT.

Acknowledgment

Thank you to the teachers and research scholars for their support in the publication of this research article. We are grateful for the resources and platform provided by the Department of Computer Science and Engineering, which have enabled us to share our findings with a wider audience. We appreciate the efforts of the reviewers and editorial team in reviewing and editing our work, and we are thankful for the opportunity to contribute to the field of research through this publication.

Funding Information

The authors have not received any financial support or funding to report.

Author's Contribution

Rahul: Conceived ideas and designed the outline of the manuscript, collected the relevant data, papers from different source. Wrote review on each paper emphasizing on the concepts, proposed algorithms, limitations in the proposed approaches. Drafted the manuscript and designed the figures. Explored the research issues and challenges in S-IoT.

Venkatesh: Reviewed the manuscript, provided critical feedback. Identified key research issues and challenges in S-IoT, theory. Analyzed corrections in manuscript verification. Find out the future directions of S-IoT. Encouraged research scholar to investigated and supervised the findings of this study.

Venugopal K. R.: Developed the theoretical framework for the paper. Helped to complete the survey and analysis of the manuscript. Reviewed the final version of the manuscript. Motivated research scholar to explore, S-IoT. Provided valuable feedback to enhance the quality of the study.

Ethics

I undersigned that this article has not been published elsewhere. The authors declare no conflict of interest.

References

Aalibagi, S., Mahyar, H., Movaghar, A., & Stanley, H. E. (2021). A matrix factorization model for hellinger-based trust management in social internet of things. *IEEE Transactions on Dependable and Secure Computing*, *19*(4), 2274-2285. https://doi.org/10.1109/TDSC.2021.3052953

Abdelghani, W., Zayani, C. A., Amous, I., & Sèdes, F. (2016, September). Trust management in social internet of things: A survey. *In Conference on e-Business, e-Services and e-Society* (pp. 430-441). Springer, Cham. https://doi.org/10.1007/978-3-319-45234-0_39

Abderrahim, O. B., Elhdhili, M. H., & Saidane, L. (2017a, June). TMCoI-S-IOT: A trust management system based on communities of interest for the social Internet of Things. *In 2017 13th International Wireless Communications and Mobile Computing Conference* (IWCMC) (pp. 747-752). IEEE. https://doi.org/10.1109/IWCMC.2017.7986378

Abderrahim, O. B., Elhedhili, M. H., & Saidane, L. (2017b, June). CTMS-S-IOT: A context-based trust management system for the social Internet of Things. *In 2017 13th International Wireless Communications and Mobile Computing Conference* (IWCMC) (pp. 1903-1908). IEEE. https://doi.org/10.1109/IWCMC.2017.7986574

Adat, V., & Gupta, B. B. (2018). Security in Internet of Things: Issues, challenges, taxonomy and architecture. *Telecommunication Systems*, *67*(3), 423-441. https://doi.org/10.1007/s11235-017-0345-9

Afzal, B., Umair, M., Shah, G. A., & Ahmed, E. (2019). Enabling IoT platforms for social IoT applications: Vision, feature mapping and challenges. *Future Generation Computer Systems*, *92*, 718-731. https://doi.org/10.1016/j.future.2017.12.002

Ahmed, A. I. A., Ab Hamid, S. H., Gani, A., & Khan, M. K. (2019). Trust and reputation for Internet of Things: Fundamentals, taxonomy and open research challenges. *Journal of Network and Computer Applications*, *145*, 102409. https://doi.org/10.1016/j.jnca.2019.102409

Ahmed, E., Yaqoob, I., Gani, A., Imran, M., & Guizani, M. (2017). Social-aware resource allocation and optimization for D2D communication. *IEEE Wireless Communications*, *24*(3), 122-129.

Alam, K. M., Saini, M., & El Saddik, A. (2015). Toward social internet of vehicles: Concept, architecture and applications. *IEEE access*, *3*, 343-357. https://doi.org/10.1109/ACCESS.2015.2416657

Al-Hamadi, H., & Chen, R. (2017). Trust-based decision making for health IoT systems. *IEEE Internet of Things Journal*, *4*(5), 1408-1419. https://doi.org/10.1109/JIOT.2017.2736446

AlHogail, A. (2018). Improving IoT technology adoption through improving consumer trust. *Technologies*, *6*(3), 64. https://doi.org/10.3390/technologies6030064

Ali-Eldin, A. M. (2021, May). A Cloud-Based Trust Computing Model for the Social Internet of Things. *In 2021 International Mobile, Intelligentand Ubiquitous Computing Conference* (MIUCC) (pp. 161-165). IEEE. https://doi.org/10.48550/arXiv.2205.03226

Aljubairy, A., Zhang, W. E., Sheng, Q. Z., & Alhazmi, A. (2020, June). S-iotpredict: A framework for predicting relationships in the social internet of things. In International Conference on Advanced Information Systems Engineering (pp. 101-116). *Springer, Cham*. https://doi.org/10.1007/978-3-030-49435-3_7

Amanullah, M. A., Habeeb, R. A. A., Nasaruddin, F. H., Gani, A., Ahmed, E., Nainar, A. S. M., ... & Imran, M. (2020). Deep learning and big data technologies for IoT security. *Computer Communications*, *151*, 495-517. https://doi.org/10.1016/j.comcom.2020.01.016

Amin, F., Abbasi, R., Rehman, A., & Choi, G. S. (2019a). An advanced algorithm for higher network navigation in social Internet of Things using small-world networks. *Sensors*, 19(9), 2007. https://doi.org/10.3390/s19092007

Amin, F., Ahmad, A., & Sang Choi, G. (2019b). Towards trust and friendliness approaches in the social Internet of Things. *Applied Sciences*, 9(1), 166. https://doi.org/10.3390/app9010166

Amin, F., Ahmad, A., & Choi, G. S. (2018, October). Community detection and mining using complex networks tools in social internet of things. *In TENCON 2018-2018 IEEE Region 10 Conference* (pp. 2086-2091). IEEE. https://doi.org/10.1109/TENCON.2018.8650511

Amin, F., Majeed, A., Mateen, A., Abbasi, R., & Hwang, S. O. (2022). A systematic survey on the recent advancements in the Social Internet of Things. *IEEE Access*, 10, 63867-63884. https://doi.org/10.1109/ACCESS.2022.3183261

Amiri-Zarandi, M., & Dara, R. A. (2020, August). Blockchain-based trust management in social internet of things. *In 2020 IEEE Intl Conf 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) (pp. 49-54). https://doi.org/10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00024

Amiri-Zarandi, M., Dara, R. A., & Fraser, E. (2022). LBTM: A lightweight blockchain-based trust management system for social internet of things. *The Journal of Supercomputing*, 78(6), 8302-8320. https://doi.org/10.1007/s11227-021-04231-3

Arjunasamy, A., & Rathi, S. (2019). Relationship based heuristic for selecting friends in social Internet of Things. *Wireless Personal Communications*, *107*(4), 1537-1547. https://doi.org/10.1007/s11277-019-06344-8

Aslam, M. J., Din, S., Rodrigues, J. J., Ahmad, A., & Choi, G. S. (2020). Defining service-oriented trust assessment for social internet of things. *IEEE Access*, *8*, 206459-206473. https://doi.org/10.1109/ACCESS.2020.3037372

Azad, M. A., Bag, S., Hao, F., & Shalaginov, A. (2020). Decentralized self-enforcing trust management system for social Internet of Things. *IEEE Internet of Things Journal*, *7*(4), 2690-2703. https://doi.org/10.1109/JIOT.2019.2962282

Babar, S., & Mahalle, P. (2021). Trust management approach for detection of malicious devices in S-IoT. *Tehnički Glasnik*, *15*(1), 43-50. https://doi.org/10.31803/tg-20210204180217

Bi, R., Chen, Q., Chen, L., Xiong, J., & Wu, D. (2020). A privacy-preserving personalized service framework through Bayesian game in social IoT. *Wireless Communications and Mobile Computing*, 2020. https://doi.org/10.1155/2020/8891889

Butt, T. A., Iqbal, R., Shah, S. C., & Umar, T. (2018). Social Internet of Vehicles: *Architecture and Enabling Technologies. Computers & Electrical Engineering*, *69*, 68-84. https://doi.org/10.1016/j.compeleceng.2018.05.023

Cai, B., Li, X., Kong, W., Yuan, J., & Yu, S. (2021). A reliable and lightweight trust inference model for service recommendation in S-IoT. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2021.3125347

Chahal, R. K., Kumar, N., & Batra, S. (2020). Trust management in social Internet of Things: *A taxonomy, open issuesand challenges. Computer Communications*, *150*, 13-46. https://doi.org/10.1016/j.comcom.2019.10.034

Chen, G., & Huang, T. (2019). Community privacy estimation method based on key node method in space social Internet of Things. *International Journal of Distributed Sensor Networks*, *15*(10), 1550147719883131. https://doi.org/10.1177/1550147719883131

Chen, J. I. Z. (2018). Embedding the MRC and SC schemes into trust management algorithm applied to IoT security protection. *Wireless Personal Communications*, *99*(1), 461-477. https://doi.org/10.1007/s11277-017-5120-4

Chen, R., Bao, F., & Guo, J. (2015). Trust-based service management for social internet of things systems. *IEEE Transactions on Dependable and Secure Computing*, *13*(6), 684-696. https://doi.org/10.1109/TDSC.2015.2420552

Chen, R., Guo, J., & Bao, F. (2014). Trust management for SOA-based IoT and its application to service composition. *IEEE Transactions on Services Computing*, *9*(3), 482-495. https://doi.org/10.1109/TSC.2014.2365797

Chen, X., Ding, J., & Lu, Z. (2020). A decentralized trust management system for intelligent transportation environments. *IEEE Transactions on Intelligent Transportation Systems*, *23*(1), 558-571. https://doi.org/10.1109/TITS.2020.3013279

Chen, Y., Zhou, M., Zheng, Z., & Chen, D. (2019). Time-aware smart object recommendation in social internet of things. *IEEE Internet of Things Journa*l, *7*(3), 2014-2027. https://doi.org/10.1109/JIOT.2019.2960822

Chen, Z., Ling, R., Huang, C. M., & Zhu, X. (2016). A scheme of access service recommendation for the Social Internet of Things. *International Journal of Communication Systems*, *29*(4), 694-706. https://doi.org/10.1002/dac.2930

Ching, C. W., Huang, H. S., Yang, C. A., Kuo, J. J., & Hwang, R. H. (2021, December). Efficient Online Decentralized Learning Framework for Social Internet of Things. *In 2021 IEEE Global Communications Conference* (GLOBECOM) (pp. 1-6). IEEE. https://doi.org/10.1109/GLOBECOM46510.2021.9685824

Cho, J. H., Chan, K., & Adali, S. (2015). A survey on trust modeling. ACM Computing Surveys (CSUR), *48*(2), 1-40. https://doi.org/10.1145/2815595

Chung, K. C., & Liang, S. W. J. (2020). An empirical study of social network activities via social Internet of Things (S-IoT). *IEEE Access*, *8*, 48652-48659. https://doi.org/10.1109/ACCESS.2020.2978151

Cicirelli, F., Guerrieri, A., Spezzano, G., Vinci, A., Briante, O., Iera, A., & Ruggeri, G. (2017). Edge computing and social internet of things for large-scale smart environments development. *IEEE Internet of Things Journal*, *5*(4), 2557-2571. https://doi.org/10.1109/JIOT.2017.2775739

Cinque, M., Esposito, C., Russo, S., & Tamburis, O. (2020). Blockchain-empowered decentralised trust management for the Internet of Vehicles security. *Computers & Electrical Engineering*, *86*, 106722. https://doi.org/10.1016/j.compeleceng.2020.106722

de Matos, E., Tiburski, R. T., Moratelli, C. R., Johann Filho, S., Amaral, L. A., Ramachandran, G., ... & Hessel, F. (2020). Context information sharing for the Internet of Things: A survey. *Computer Networks*, *166*, 106988. https://doi.org/10.1016/j.comnet.2019.106988

Deng, T., Li, X., Jin, B., Chen, L., & Lin, J. (2021). Achieving lightweight privacy-preserving image sharing and illegal distributor detection in social IoT. *Security and Communication Networks*, 2021. https://doi.org/10.1155/2021/5519558

Dias, J. P., Lima, B., Faria, J. P., Restivo, A., & Ferreira, H. S. (2020, June). Visual self-healing modelling for reliable internet-of-things systems. *In International Conference on Computational Science* (pp. 357-370). Springer, Cham. https://doi.org/10.1007/978-3-030-50426-7_27

Din, I. U., Guizani, M., Hassan, S., Kim, B. S., Khan, M. K., Atiquzzaman, M., & Ahmed, S. H. (2018a). The Internet of Things: A review of enabled technologies and future challenges. *IEEE Access*, *7*, 7606-7640. https://doi.org/10.1109/ACCESS.2018.2886601

Din, I. U., Guizani, M., Kim, B. S., Hassan, S., & Khan, M. K. (2018b). Trust management techniques for the Internet of Things: A survey. *IEEE Access*, *7*, 29763-29787. https://doi.org/10.1109/ACCESS.2018.2880838

Fan, X., Liu, L., Zhang, R., Jing, Q., & Bi, J. (2020). Decentralized trust management: Risk analysis and trust aggregation. *ACM Computing Surveys* (CSUR), *53*(1), 1-33. https://doi.org/10.1145/3362168

Farahbakhsh, B., Fanian, A., & Manshaei, M. H. (2021). TGSM: Towards trustworthy group-based service management for social IoT. *Internet of Things*, *13*, 100312. https://doi.org/10.1016/j.iot.2020.100312

Gan, X., Li, Y., Huang, Y., Fu, L., & Wang, X. (2019). When crowdsourcing meets social IoT: An efficient privacy-preserving incentive mechanism. *IEEE Internet of Things Journal*, *6*(6), 9707-9721. https://doi.org/10.1109/JIOT.2019.2930659

García-Magariño, I., Sendra, S., Lacuesta, R., & Lloret, J. (2018). Security in vehicles with IoT by prioritization rules, vehicle certificatesand trust management. *IEEE Internet of Things Journal*, *6*(4), 5927-5934. https://doi.org/10.1109/JIOT.2018.2871255

Girau, R., Martis, S., & Atzori, L. (2016, December). Neighbor discovery algorithms for friendship establishment in the social Internet of Things. *In 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)* (pp. 165-170). IEEE. https://doi.org/10.1109/WF-IoT.2016.7845484

Hakak, S., Khan, W. Z., Gilkar, G. A., Imran, M., & Guizani, N. (2020). Securing smart cities through blockchain technology: Architecture, requirements and challenges. *IEEE Network*, *34*(1), 8-14. https://doi.org/10.1109/MNET.001.1900178

Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security*, *78*, 126-142. https://doi.org/10.1016/j.cose.2018.06.004

Han, G., Zhou, L., Wang, H., Zhang, W., & Chan, S. (2018). A source location protection protocol based on dynamic routing in WSNs for the Social Internet of Things. *Future Generation Computer Systems*, *82*, 689-697. https://doi.org/10.1016/j.future.2017.08.044

Hao, F., Pei, Z., & Yang, L. T. (2020). Diversified top-k maximal clique detection in Social Internet of Things. *Future Generation Computer Systems*, *107*, 408-417. https://doi.org/10.1016/j.future.2020.02.023

Hasan, M. Z., & Al-Turjman, F. (2018). SWARM-based data delivery in Social Internet of Things. In Smart things and femtocells (pp. 167-206). *CRC Press*. https://doi.org/10.1016/j.future.2017.10.032

He, J., Cai, L., Cheng, P., Pan, J., & Shi, L. (2019). Consensus-based data-privacy preserving data aggregation. *IEEE Transactions on Automatic Control*, *64*(12), 5222-5229. https://doi.org/10.1109/TAC.2019.2910171

Hussein, D., Han, S. N., Lee, G. M., Crespi, N., & Bertin, E. (2017). Towards a dynamic discovery of smart services in the social internet of things. *Computers & Electrical Engineering*, *58*, 429-443. https://doi.org/10.1016/j.compeleceng.2016.12.008

Imran, M., Jabbar, S., Chilamkurti, N., & Rodrigues, J. J. (2019). Enabling technologies for social internet of things. *Future Generation Computer Systems*, *92*, 715-717. https://doi.org/10.1016/j.future.2018.11.018

Iqbal, R., Butt, T. A., Afzaal, M., & Salah, K. (2019). Trust management in social internet of vehicles: factors, challenges, blockchainand fog solutions. *International Journal of Distributed Sensor Networks*, *15*(1), 1550147719825820. https://doi.org/10.1177/1550147719825820

Jafarian, B., Yazdani, N., & Haghighi, M. S. (2020). Discrimination-aware trust management for social internet of things. Computer Networks, *178*, 107254. https://doi.org/10.1016/j.comnet.2020.107254

Jayasinghe, U., Lee, G. M., Um, T. W., & Shi, Q. (2018). Machine learning based trust computational model for IoT services. *IEEE Transactions on Sustainable Computing*, *4*(1), 39-52. https://doi.org/10.1109/TSUSC.2018.2839623

Jayasinghe, U., Lee, H. W., & Lee, G. M. (2017, April). A computational model to evaluate honesty in social internet of things. *In Proceedings of the symposium on applied computing* (pp. 1830-1835). https://doi.org/10.1145/3019612.3019840

Jayasinghe, U., Truong, N. B., Lee, G. M., & Um, T. W. (2016, July). Rpr: A trust computation model for social internet of things. *In 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of Peopleand Smart World Congress* (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld) (pp. 930-937). IEEE. https://doi.org/10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0146

Khan, W. Z., Aalsalem, M. Y., & Khan, M. K. (2018). Communal acts of IoT consumers: A potential threat to security and privacy. *IEEE Transactions on Consumer Electronics*, *65*(1), 64-72. https://doi.org/10.1109/TCE.2018.2880338

Khan, W. Z., Aalsalem, M. Y., & Khan, M. K. (2018, January). Five acts of consumer behavior: A potential security and privacy threat to Internet of Things. *In 2018 IEEE international conference on consumer electronics* (ICCE) (pp. 1-3). IEEE. https://doi.org/10.1109/ICCE.2018.8326124

Khan, W. Z., Aalsalem, M. Y., Khan, M. K., & Arshad, Q. (2016). Enabling consumer trust upon acceptance of IoT technologies through security and privacy model. In Advanced multimedia and ubiquitous engineering (pp. 111-117). Springer, Singapore. https://doi.org/10.1007/978-981-10-1536-6_15

Khan, W. Z., Aalsalem, M. Y., Khan, M. K., & Arshad, Q. (2017). When social objects collaborate: Concepts, processing elements, attacks and challenges. *Computers & Electrical Engineering*, *58*, 397-411. https://doi.org/10.1016/j.compeleceng.2016.11.014

Khan, W. Z., Aalsalem, M. Y., Khan, M. K., & Arshad, Q. (2019). Data and privacy: Getting consumers to trust products enabled by the Internet of Things. *IEEE Consumer Electronics Magazine*, *8*(2), 35-38. https://doi.org/10.1109/MCE.2018.2880807

Khan, W. Z., Rehman, M. H., Zangoti, H. M., Afzal, M. K., Armi, N., & Salah, K. (2020a). Industrial internet of things: Recent advances, enabling technologies and open challenges. *Computers & Electrical Engineering*, *81*, 106522. https://doi.org/10.1016/j.compeleceng.2019.106522

Khan, W. Z., Hakak, S., & Khan, M. K. (2020b). Trust management in social internet of things: Architectures, recent advancementsand future challenges. *IEEE Internet of Things Journal*, *8*(10), 7768-7788. https://doi.org/10.1109/JIOT.2020.3039296

Khanfor, A., Hamrouni, A., Ghazzai, H., Yang, Y., & Massoud, Y. (2020, June). A trustworthy recruitment process for spatial mobile crowdsourcing in large-scale social IoT. *In 2020 IEEE Technology & Engineering Management Conference* (TEMSCON) (pp. 1-6). IEEE. https://doi.org/10.1109/TEMSCON47658.2020.9140085

Khani, M., Wang, Y., Orgun, M. A., & Zhu, F. (2018, November). Context-aware trustworthy service evaluation in social internet of things. *In International Conference on Service-Oriented Computing* (pp. 129-145). Springer, Cham. https://doi.org/10.1007/978-3-030-03596-9_9

Kim, J. E., Fan, X., & Mosse, D. (2017, April). Empowering end users for social internet of things. *In Proceedings of the Second International Conference on Internet-of-Things Design and Implementation* (pp. 71-82). https://doi.org/10.1145/3054977.3054987

Kokoris-Kogias, E., Voutyras, O., & Varvarigou, T. (2016, September). TRM-S-IoT: A scalable hybrid trust & reputation model for the social internet of things. *In 2016 IEEE 21st international conference on emerging technologies and factory automation* (ETFA) (pp. 1-9). Ieee. https://doi.org/10.1109/ETFA.2016.7733612

Kowshalya, A. M., & Valarmathi, M. L. (2017). Trust management in the social internet of things. *Wireless Personal Communications*, 96(2), 2681-2691. https://doi.org/10.1007/s11277-017-4319-8

Kowshalya, M. A., & Valarmathi, M. L. (2016). Detection of Sybil's across communities over Social Internet of Things. *Journal of Applied Engineering Science*, *14*(1), 75-83. https://doi.org/10.5937/jaes14-10176

Lahbib, A., Toumi, K., Laouiti, A., Laube, A., & Martin, S. (2019, April). Blockchain based trust management mechanism for IoT. *In 2019 IEEE Wireless Communications and Networking Conference* (WCNC) (pp. 1-8). IEEE. https://doi.org/10.1109/WCNC.2019.8885994

Latif, R. (2022). ConTrust: A Novel Context-Dependent Trust Management Model in Social Internet of Things. *IEEE Access*, *10*, 46526-46537. https://doi.org/10.1109/ACCESS.2022.3169788

Lee, S., Kim, S., Choi, K., & Shon, T. (2018). Game theory-based security vulnerability quantification for social internet of things. *Future Generation Computer Systems*, *82*, 752-760. https://doi.org/10.1016/j.future.2017.09.032

Lemoine, F., Aubonnet, T., & Simoni, N. (2020). Self-assemble-featured Internet of Things. *Future Generation Computer Systems*, *112*, 41-57. https://doi.org/10.1016/j.future.2020.05.012

Li, T., Huang, G., Zhang, S., & Zeng, Z. (2021). NTSC: a novel trust-based service computing scheme in social internet of things. *Peer-to-Peer Networking and Applications*, *14*(6), 3431-3451. https://doi.org/10.1007/s12083-021-01200-8

Li, W., Song, H., & Zeng, F. (2017). Policy-based secure and trustworthy sensing for internet of things in smart cities. *IEEE Internet of Things Journal*, *5*(2), 716-723. https://doi.org/10.1109/JIOT.2017.2720635

Li, X., Eckert, M., Martinez, J. F., & Rubio, G. (2015). Context aware middleware architectures: Survey and challenges. *Sensors*, *15*(8), 20570-20607. https://doi.org/10.3390/s150820570

Lin, Z., & Dong, L. (2017). Clarifying trust in social internet of things. IEEE Transactions on Knowledge and Data Engineering, *30*(2), 234-248. https://doi.org/10.1109/TKDE.2017.2762678

Liu, X., Fu, J., Chen, Y., Luo, W., & Tang, Z. (2021). Trust-Aware sensing Quality estimation for team Crowdsourcing in social IoT. *Computer Networks*, *184*, 107695. https://doi.org/10.1016/j.comnet.2020.107695

Magdich, R., Jemal, H., & Ben Ayed, M. (2022). Context-awareness trust management model for trustworthy communications in the social Internet of Things. *Neural Computing and Applications*, *34*(24), 21961-21986. https://doi.org/10.1007/s00521-022-07656-w

Marche, C., & Nitti, M. (2020). Trust-related attacks and their detection: A trust management model for the social IoT. *IEEE Transactions on Network and Service Management*, 18(3), 3297-3308. https://doi.org/10.1109/TNSM.2020.3046906

Masmoudi, M., Abdelghani, W., Amous, I., & Sèdes, F. (2019, October). Deep learning for trust-related attacks detection in social internet of things. *In International Conference on e-Business Engineering*. (pp. 389-404). Springer, Cham. https://doi.org/10.1007/978-3-030-34986-8_28

Meena Kowshalya, A., & Valarmathi, M. L. (2017). Trust management for reliable decision making among social objects in the Social Internet of Things. *IET Networks*, *6*(4), 75-80. https://doi.org/10.1049/iet-net.2017.0021

Meena Kowshalya, A., & Valarmathi, M. L. (2018). Dynamic trust management for secure communications in social internet of things (S-IoT). *Sādhanā*, *43*(9), 1-8. https://doi.org/10.1007/s12046-018-0885-z

Metrouh, A. (2021). Social Internet of Things: a novel selection approach for dynamic resources substitution. *Evolutionary Intelligence*, 1-9. https://doi.org/10.1007/s12065-021-00580-3

Mohammadi, V., Rahmani, A. M., Darwesh, A., & Sahafi, A. (2021). Trust-based Friend Selection Algorithm for navigability in social Internet of Things. *Knowledge-Based Systems*, *232*, 107479. https://doi.org/10.1016/j.knosys.2021.107479

MS, R., & Buyya, R. (2020, December). Trust management for service-oriented s-Iot systems. In 2020 The 8th international conference on information technology: *IoT and Smart City* (pp. 216-222). https://doi.org/10.1145/3446999.3447635

Narang, N., & Kar, S. (2021). A hybrid trust management framework for a multi-service social IoT network. *Computer Communications*, *171*, 61-79. https://doi.org/10.1016/j.comcom.2021.02.015

Nie, L., Wu, Y., Wang, X., Guo, L., Wang, G., Gao, X., & Li, S. (2021). Intrusion detection for secure social internet of things based on collaborative edge computing: A generative adversarial network-based approach. *IEEE Transactions on Computational Social Systems*, *9*(1), 134-145. https://doi.org/10.1109/TCSS.2021.3063538

Nitti, M., Atzori, L., & Cvijikj, I. P. (2014). Friendship selection in the social internet of things: Challenges and possible strategies. *IEEE Internet of Things Journal*, *2*(3), 240-247. https://doi.org/10.1109/JIOT.2014.2384734

Nitti, M., Girau, R., & Atzori, L. (2013). Trustworthiness management in the social internet of things. *IEEE Transactions on knowledge and data engineering*, *26*(5), 1253-1266. https://doi.org/10.1109/TKDE.2013.105

Ouechtati, H., Nadia, B. A., & Lamjed, B. S. (2021). A fuzzy logic-based model for filtering dishonest recommendations in the Social Internet of Things. *Journal of Ambient Intelligence and Humanized Computing*, 1-20. https://doi.org/10.1007/s12652-021-03127-7

Park, K., Park, Y., Das, A. K., Yu, S., Lee, J., & Park, Y. (2019). A dynamic privacy-preserving key management protocol for V2G in social internet of things. *IEEE Access*, *7*, 76812-76832. https://doi.org/10.1109/ACCESS.2019.2921399

Premarathne, U. S. (2017, December). MAG-S-IoT: A multiplicative attributes graph model based trust computation method for social Internet of Things. *In 2017 IEEE International Conference on Industrial and Information Systems* (ICIIS) (pp. 1-6). IEEE https://doi.org/10.1109/ICIINFS.2017.8300344.

Premarathne, U. S. (2019, December). Residual energy aware trust computation method for social internet of things. *In 2019 14th Conference on Industrial and Information Systems* (ICIIS) (pp. 470-475). IEEE. https://doi.org/10.1109/ICIIS47346.2019.9063292

Rabadiya, K., Makwana, A., & Jardosh, S. (2017, December). Revolution in networks of smart objects: Social Internet of Things. *In 2017 International Conference on Soft Computing and its Engineering Applications* (icSoftComp) (pp. 1-8). IEEE. https://doi.org/10.1109/ICSOFTCOMP.2017.8280086

Rafey, S. E. A., Abdel-Hamid, A., & Abou El-Nasr, M. (2016, April). CBSTM-IoT: Context-based social trust model for the Internet of Things. *In 2016 International Conference on Selected Topics in Mobile & Wireless Networkin*g (MoWNeT) (pp. 1-8). IEEE. https://doi.org/10.1109/MoWNet.2016.7496623

Rafique, W., Qi, L., Yaqoob, I., Imran, M., Rasool, R. U., & Dou, W. (2020). Complementing IoT services through software defined networking and edge computing: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *22*(3), 1761-1804. https://doi.org/10.1109/COMST.2020.2997475

Rajendran, S., & Jebakumar, R. (2021). Object Recommendation based Friendship Selection (ORFS) for navigating smarter social objects in S-IoT. *Microprocessors and Microsystems*, *80*, 103358. https://doi.org/10.1016/j.micpro.2020.103358

Rajendran, S., & Jebakumar, R. (2022). Friendliness Based Trustworthy Relationship Management (F-TRM) in Social Internet of Things. *Wireless Personal Communications*, *123*(3), 2625-2647. https://doi.org/10.1007/s11277-021-09256-8

Ramasamy, T., & Arjunasamy, A. (2017). Advanced heuristics for selecting friends in social internet of things. *Wireless Personal Communications*, *97*(4), 4951-4965. https://doi.org/10.1007/s11277-017-4759-1

Rashmi, M. R., & Raj, C. V. (2019). A review on trust models of social Internet of Things. *Emerging Research in Electronics, Computer Science and Technology*, 203-209. https://doi.org/10.1007/978-981-13-5802-9_19

Rehman, A. U., Naqvi, R. A., Rehman, A., Paul, A., Sadiq, M. T., & Hussain, D. (2020). A trustworthy s-IoT aware mechanism as an enabler for citizen services in smart cities. *Electronics*, *9*(6), 918. https://doi.org/10.3390/electronics9060918

Roopa, M. S., Pattar, S., Buyya, R., Venugopal, K. R., Iyengar, S. S., & Patnaik, L. M. (2019). Social Internet of Things (S-IoT): Foundations, thrust areas, systematic review and future directions. *Computer Communications*, *139*, 32-57. https://doi.org/10.1016/j.comcom.2019.03.009

Roopa, M. S., Siddiq, A., Buyya, R., Venugopal, K. R., Iyengar, S. S., & Patnaik, L. M. (2020). Dynamic management of traffic signals through social IoT. Procedia Computer Science, *171*, 1908-1916. https://doi.org/10.1016/j.procs.2020.04.204

Ruggeri, G., & Briante, O. (2017, August). A framework for iot and e-health systems integration based on the social internet of things paradigm. *In 2017 international symposium on wireless communication systems* (ISWCS) (pp. 426-431). IEEE. https://doi.org/10.1109/ISWCS.2017.8108152

Sagar, S., Mahmood, A., Sheng, Q. Z., & Zhang, W. E. (2020a, June). Trust computational heuristic for social Internet of Things: A machine learning-based approach. *In ICC 2020-2020 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.* https://doi.org/10.1109/ICC40277.2020.9148767

Sagar, S., Mahmood, A., Kumar, J., & Sheng, Q. Z. (2020b, December). A time-aware similarity-based trust computational model for social internet of things. *In GLOBECOM 2020-2020 IEEE Global Communications Conference* (pp. 1-6). IEEE. https://doi.org/10.1109/GLOBECOM42002.2020.9322540

Sagar, S., Mahmood, A., Sheng, M., Zaib, M., & Zhang, W. (2020c, December). Towards a machine learning-driven trust evaluation model for social internet of things: A time-aware approach. In MobiQuitous 2020-17th EAI International Conference on Mobile and Ubiquitous Systems*: Computing, Networking and Services* (pp. 283-290). https://doi.org/10.1145/3448891.3448927

Sagar, S., Mahmood, A., Sheng, Q. Z., Pabani, J. K., & Zhang, W. E. (2022a). Understanding the Trustworthiness Management in the Social Internet of Things: A Survey. *arXiv preprint arXiv:2202.03624*. https://doi.org/10.48550/arXiv.2202.03624

Sagar, S., Mahmood, A., Wang, K., Sheng, Q. Z., & Zhang, W. E. (2022b). Trust-S-IoT: Towards Trustworthy Object Classification in the Social Internet of Things. arXiv preprint arXiv:2205.03226. https://doi.org/10.48550/arXiv.2205.03226

Saleem, Y., Crespi, N., Rehmani, M. H., Copeland, R., Hussein, D., & Bertin, E. (2016, December). Exploitation of social IoT for recommendation services*. In 2016 IEEE 3rd World Forum on Internet of Things* (WF-IoT) (pp. 359-364). IEEE. https://doi.org/10.1109/WF-IoT.2016.7845500

Selvaraj, S., Thangarajan, R., & Saravanan, M. (2022). Trust-Based and Optimized RPL Routing in Social Internet of Things Network. *In Mobile computing and Sustainable Informatics*. *Springer, Singapore*. pp: 513-529. https://doi.org/10.1007/978-981-16-1866-6_36

Sezer, O. B., Dogdu, E., & Ozbayoglu, A. M. (2017). Context-aware computing, learningand big data in internet of things: A survey. *IEEE Internet of Things Journal*, *5*(1), 1-27. https://doi.org/10.1109/JIOT.2017.2773600

Sharma, V., You, I., Jayakody, D. N. K., & Atiquzzaman, M. (2019). Cooperative trust relaying and privacy preservation via edge-crowdsourcing in social Internet of Things. *Future Generation Computer Systems*, *92*, 758-776. https://doi.org/10.1016/j.future.2017.12.039

Shen, J., Zhou, T., Wei, F., Sun, X., & Xiang, Y. (2017). Privacy-preserving and lightweight key agreement protocol for V2G in the social Internet of Things. *IEEE Internet of things Journal*, *5*(4), 2526-2536. https://doi.org/10.1109/JIOT.2017.2775248

Sobin, C. C. (2020). A survey on architecture, protocols and challenges in IoT. *Wireless Personal Communications*, *112*(3), 1383-1429. https://doi.org/10.1007/s11277-020-07108-5

Talbi, S., & Bouabdallah, A. (2020). Interest-based trust management scheme for social internet of things. *Journal of Ambient Intelligence and Humanized Computing*, *11*(3), 1129-1140. https://doi.org/10.1007/s12652-019-01256-8

Tang, B., Kang, H., Fan, J., Li, Q., & Sandhu, R. (2019, May). IoT passport: A blockchain-based trust framework for collaborative internet-of-things. *In Proceedings of the 24th ACM symposium on access control models and technologies* (pp. 83-92). https://doi.org/10.1145/3322431.3326327

Tian, Y., Zhang, Z., Xiong, J., Chen, L., Ma, J., & Peng, C. (2021). Achieving graph clustering privacy preservation based on structure entropy in social IoT. *IEEE Internet of Things Journal*, *9*(4), 2761-2777. https://doi.org/10.1109/JIOT.2021.3092185

Truong, N. B., Um, T. W., Zhou, B., & Lee, G. M. (2017a, December). From personal experience to global reputation for trust evaluation in the social internet of things. *In GLOBECOM 2017-2017 IEEE Global Communications* Conference (pp. 1-7). IEEE. https://doi.org/10.1109/GLOCOM.2017.8254523

Truong, N. B., Lee, H., Askwith, B., & Lee, G. M. (2017b). Toward a trust evaluation mechanism in the social internet of things. *Sensors*, *17*(6), 1346. https://doi.org/10.3390/s17061346

Truong, N. B., Um, T. W., & Lee, G. M. (2016). A reputation and knowledge based trust service platform for trustworthy social internet of things. *Innovations in Clouds, Internet and Networks (ICIN), Paris, France*, 104-111.

Ugur, A. (2021, April). Manipulator: A novel collusion attack on trust management systems in social IoT. *In Computer Science On-line Conferenc*e (pp. 578-592). Springer, Cham. https://doi.org/10.1007/978-3-030-77442-4_49

Ullah, I., Shah, M. A., Wahid, A., Mehmood, A., & Song, H. (2018). ESOT: A new privacy model for preserving location privacy in Internet of Things. *Telecommunication Systems*, *67*(4), 553-575. https://doi.org/10.1007/s11235-017-0352-x

Um, T. W., Lee, E., Lee, G. M., & Yoon, Y. (2019). Design and implementation of a trust information management platform for social internet of things environments. *Sensors*, *19*(21), 4707. https://doi.org/10.3390/s19214707

Rehman, M. H., Salah, K., Damiani, E., & Svetinovic, D. (2019). Trust in blockchain cryptocurrency ecosystem. *IEEE Transactions on Engineering Management*, *67*(4), 1196-1212. https://doi.org/10.1109/TEM.2019.2948861

Wang, B., Sun, Y., Duong, T. Q., Nguyen, L. D., & Zhao, N. (2020a). Security enhanced content sharing in social IoT: A directed hypergraph-based learning scheme. *IEEE Transactions on Vehicular Technology*, *69*(4), 4412-4425. https://doi.org/10.1109/TVT.2020.2975884

Wang, X., Zhong, X., Li, L., Zhang, S., Lu, R., & Yang, T. (2020b). TOT: Trust aware opportunistic transmission in cognitive radio Social Internet of Things. *Computer Communications*, *162*, 1-11. https://doi.org/10.1016/j.comcom.2020.08.007

Wang, B., Sun, Y., Li, S., & Cao, Q. (2018). Hierarchical matching with peer effect for low-latency and high-reliable caching in social IoT. *IEEE Internet of Things Journa*l, *6*(1), 1193-1209. https://doi.org/10.1109/JIOT.2018.2867617

Wang, K., Qi, X., Shu, L., Deng, D. J., & Rodrigues, J. J. (2016). Toward trustworthy crowdsourcing in the social internet of things. *IEEE Wireless Communications*, 23(5), 30-36. https://doi.org/10.1109/MWC.2016.7721739

Wang, L., Wu, H., Han, Z., Zhang, P., & Poor, H. V. (2017). Multi-hop cooperative caching in social IoT using matching theory. *IEEE Transactions on Wireless Communications*, *17*(4), 2127-2145.

Wei, L., Wu, J., & Long, C. (2020a, November). Enhancing trust management via blockchain in Social Internet of Things. *In 2020 Chinese Automation Congress* (CAC) (pp. 159-164). IEEE. https://doi.org/10.1109/CAC51589.2020.9326856

Wei, L., Wu, J., Long, C., & Li, B. (2020b). On designing context-aware trust model and service delegation for social internet of things. *IEEE Internet of Things Journal*, *8*(6), 4775-4787. https://doi.org/10.1109/JIOT.2020.3028380

Wei, L., Yang, Y., Wu, J., Long, C., & Lin, Y. B. (2022). A Bidirectional Trust Model for Service Delegation in Social Internet of Things. *Future Internet*, *14*(5), 135. https://doi.org/10.3390/fi14050135

Wen, Y., Xu, Z., Zhi, R., & Chen, J. (2021). Trust Prediction Model Based on Deep Learning in Social Internet of Things. *In International Conference on Internet of Things as a Service (pp. 557-570). Springer, Cham.* https://doi.org/10.1007/978-3-030-67514-1_44

Wu, B., Zhong, L., Yao, L., & Ye, Y. (2022). EAGCN: An Efficient Adaptive Graph Convolutional Network for Item Recommendation in Social Internet of Things. *IEEE Internet of Things Journal.* https://doi.org/10.1109/JIOT.2022.3151400

Wu, F., Xu, L., Kumari, S., Li, X., Das, A. K., Khan, M. K., ... & Baliyan, R. (2016). A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks. *Security and Communication Networks*, *9*(16), 3527-3542. https://doi.org/10.1002/sec.1558

Xia, H., Xiao, F., Zhang, S. S., Hu, C. Q., & Cheng, X. Z. (2019, April). Trustworthiness inference framework in the social Internet of Things: A context-aware approach. *In IEEE INFOCOM 2019-IEEE Conference on Computer Communications* (pp. 838-846). IEEE. https://doi.org/10.1109/INFOCOM.2019.8737491

Xiao, H., Sidhu, N., & Christianson, B. (2015, August). Guarantor and reputation based trust model for social internet of things. *In 2015 International wireless communications and mobile computing conference* (IWCMC) (pp. 600-605). IEEE. https://doi.org/10.1109/IWCMC.2015.7289151

Yan, B., Yu, J., Yang, M., Jiang, H., Wan, Z., & Ni, L. (2021). A novel distributed social internet of things service recommendation scheme based on LSH forest. *Personal and Ubiquitous Computing*, *25*(6), 1013-1026. https://doi.org/10.1007/s00779-019-01283-4

Yan, J., Wu, D., & Wang, R. (2018). Socially aware trust framework for multimedia delivery in D2D cooperative communication. IEEE Transactions on Multimedia, *21*(3), 625-635. https://doi.org/10.1109/TMM.2018.2890196

Yang, Y., Hao, F., Pang, B., Min, G., & Wu, Y. (2021). Dynamic maximal clique's detection and evolution management in social internet of things: A formal concept analysis approach. *IEEE Transactions on Network Science and Engineering*, *9*(3), 1020-1032. https://doi.org/10.1109/TNSE.2021.3067939

Yang, Z., Yang, K., Lei, L., Zheng, K., & Leung, V. C. (2018). Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet of Things Journal*, *6*(2), 1495-1505.

Yi, H. (2021). Secure social internet of things based on post-quantum blockchain. *IEEE transactions on Network Science and Engineering*. https://doi.org/10.1109/TNSE.2021.3095192

Yi, Y., Zhang, Z., Yang, L. T., Deng, X., Yi, L., & Wang, X. (2020). Social interaction and information diffusion in Social Internet of Things: Dynamics, cloud-edge, traceability. *IEEE Internet of things Journal*, *8*(4), 2177-2192. https://doi.org/10.1109/JIOT.2020.3026995

Yin, L., Feng, J., Xun, H., Sun, Z., & Cheng, X. (2021). A privacy-preserving federated learning for multiparty data sharing in social IoTs. *IEEE Transactions on Network Science and Engineering*, *8*(3), 2706-2718. https://doi.org/10.1109/TNSE.2021.3074185

Zhang, H., Yu, J., Obaidat, M. S., Vijayakumar, P., Ge, L., Lin, J., ... & Hao, R. (2020). Secure edge-aided computations for social Internet-of-Things systems. *IEEE Transactions on Computational Social Systems.* https://doi.org/10.1109/TCSS.2020.3030904

Zhang, P., Wang, Y., Kumar, N., Jiang, C., & Shi, G. (2021). A Security-and Privacy-Preserving Approach Based on Data Disturbance for Collaborative Edge Computing in Social IoT Systems. *IEEE Transactions on Computational Social Systems*, *9*(1), 97-108. https://doi.org/10.1109/TCSS.2021.3092746

Zhang, L., Zhu, X., Han, X., & Ma, J. (2019, October). Differentially privacy-preserving social IoT. In *2019 11th International Conference on Wireless Communications and Signal Processing (WCSP)* (pp. 1-6). IEEE.

Zouari, J., Hamdi, M., & Kom, T. H. (2018, June). Privacy preserving profile matching protocol for human-centric social Internet of Things. In 2018 IEEE 27th International Conference on Enabling Technologies: *Infrastructure for Collaborative Enterprises* (WETICE) (pp. 181-186). IEEE. https://doi.org/10.1109/WETICE.2018.00042

Zhong, X., Li, L., Zhang, S., & Lu, R. (2020). ECOR: An energy aware coded opportunistic routing for cognitive radio social internet of things. *Wireless Personal Communications*, *110*(1), 1-20. https://doi.org/10.1007/s11277-019-06708-0

Zhou, B., Maines, C., Tang, S., Shi, Q., Yang, P., Yang, Q., & Qi, J. (2018). A 3-D security modeling platform for social IoT environments. *IEEE Transactions on Computational Social Systems*, *5*(4), 1174-1188. https://doi.org/10.1109/TCSS.2018.2878921

Zhou, M., Li, Y., Pu, Q., Nie, W., Wilford, A., & Jiang, Q. (2022). Connectivity-Based Localization Scheme for Social Internet of Things. *IEEE Transactions on Computational Social Systems*. https://doi.org/10.1109/TCSS.2022.3152172

Zhu, X., Wen, S., Jolfaei, A., Haghighi, M. S., Camtepe, S., & Xiang, Y. (2020). Vulnerability detection in S-IoT applications: A fuzzing method on their binaries. *IEEE Transactions on Network Science and Engineering*. https://doi.org/10.1109/TNSE.2020.3038142

Zia, K., Farooq, U., Shafi, M., & Arshad, M. (2021). An Agent-Based Model of Task-Allocation and Resource-Sharing for Social Internet of Things. *IoT*, *2*(1), 187-204. https://doi.org/10.3390/iot2010010