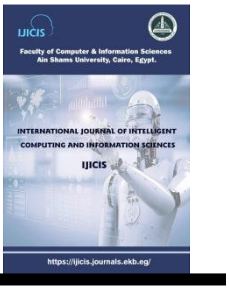
IJICIS, Vol.24, No.3, 70-82
DOI :10.21608/ijicis.2024.321224.1356

International Journal of Intelligent Computing and Information Sciences

https://ijicis.journals.ekb.eg/


IJICIS
Faculty of Computer & Information Sciences Ain Shams University, Cairo, Egypt.
INTERNATIONAL JOURNAL OF INTELLIGENT COMPUTING AND INFORMATION SCIENCES
IJICIS
https://ijicis.journals.ekb.eg/

A REVIEW OF TRUST MANAGEMENT IN CYBER-PHYSICAL-SOCIAL SYSTEMS

Ahmed Zedaan M. Abed
Information Systems Dept,
Faculty of Computer and
Information Science, Ain Shams
University,
Cairo, Egypt
Ahmed4abed@hotmail.com

Tamer Abdelkader*
Information Systems Dept,
Faculty of Computer and
Information Science, Ain Shams
University,
Cairo, Egypt
tammabde@cis.asu.edu.eg

Mohamed Hashem
Information Systems Dept,
Faculty of Computer and
Information Science, Ain Shams
University,
Cairo, Egypt
Mhashem100@cis.asu.edu.eg

Received 2024-09-16; Revised 2024-09-16; Accepted 2024-09-30

Abstract: *Cyber-Physical-Social Systems (CPSS) bring together an assortment of resources from the physical network, cyberspace, and the social sphere. These systems rely on communication, computation, and control infrastructures, which usually comprise several tiers across the three realms, utilizing diverse resources such as sensors, actuators, computational resources, services, and human involvement. The proficient interaction of these resources is critical for the operational efficacy of cyber-physical-social systems. CPSS exhibits resource constraints, openness, and uncertainty, resulting in high uncertainty in its services, including quality of service (QoS) provision and significant security risks. Consequently, an efficient and dependable service composition approach is crucial when dealing with complex service requirements. Furthermore, preference learning plays a pivotal role in enhancing user experiences. Trust is viewed as a barrier to the integration of social attributes among smart objects, which is essential for forming reliable social connections and delivering dependable services. This review offers an in-depth analysis of trustworthiness management within Cyber-Physical Social Systems (CPSS).*

Keywords: *CPSS, Trustworthiness, service management, Internet of things, Smart Systems*

1. Introduction

The extensive wave of computing, driven by the Internet, continues to reach its peak. We are now entering a new phase, characterized by the cyber-physical-social systems (CPSS). CPSSs consist of three fundamental elements: cyber space, physical space, and social space, as depicted in Figure 1, as well as advancements in mobile communication, cloud computing, Internet of things (IoT), and big data. The CPSS, which links physical objects to the digital world, is expected to be a catalyst for various innovative applications. In 2008, the US National Intelligence Council produced a report that identified IoT as one of six transformative civil technologies [1]. The utilization of sensors and actuators enables

*<b></b>**Corresponding Author**: Tamer Abdelkader

Information Systems Department, Faculty of Computer and Information Science, Ain Shams University, Cairo, Egypt

Email address: tammabde@cis.asu.edu.eg

remote locations' monitoring, and control of smart devices in the physical environment via the Internet. With mobile devices, users will have continuous access to the Internet and the interconnected smart devices, along with the cloud services essential for their operation. The combination of the Internet of Things (IoT) with cloud computing, mobile communication and computing, the semantic web, and social computing is set to foster the development of numerous innovative Cyber-Physical-Social Systems (CPSS). These systems will include applications such as smart cities, intelligent parking, smart traffic management, smart homes, healthcare innovations, transportation solutions, supply chain enhancements, smart manufacturing, product life cycle management, environmental monitoring, and government services, among others. Our future will be characterized by a unified cyber physical smart planet. Conversely, we will encounter larger and more complex challenges concerning security, privacy, and trust. Consequently, the engineering sector will experience a fundamental shift in the design, operation, and management of engineering systems.

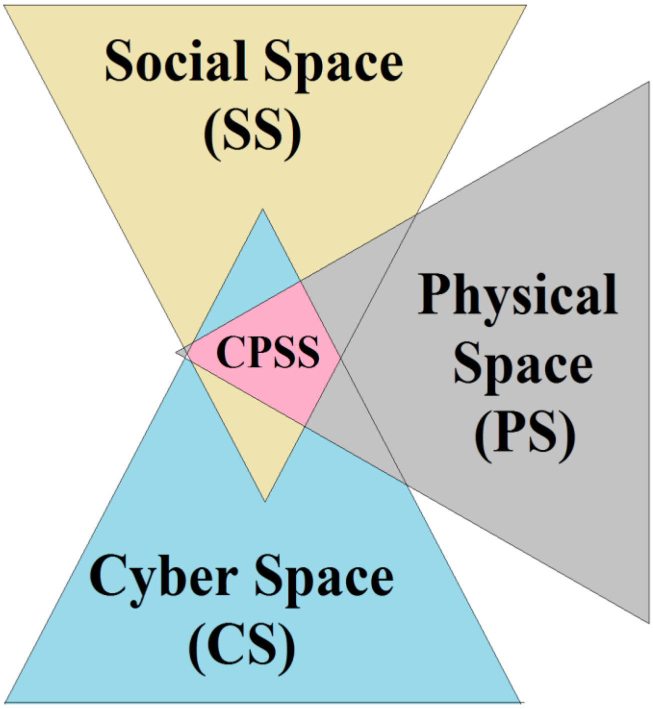


Figure. 1: Cyber Physical Social Systems (CPSS) Spaces

Technological progress, alongside shifts in society and global challenges such as globalization, urbanization, environmental sustainability, climate change, and demographic aging, is driving the emergence of new requirements for technologies, products, and services. These challenges create a rich environment for the evolution of innovative cyber-physical social systems that leverage the Internet of Things (IoT). The convergence of societal issues and technological advancements facilitated by IoT will lead to the development of new types of engineered systems, which will pose significant design, operational, and management challenges for systems engineers. Typically, these systems will consist of interconnected smart systems, such as smart cities, characterized by dynamic networks of devices, software, and human interactions, organized in a complex and decentralized manner to provide new system services, some of which will be of critical importance. The envisioned systems are distinguished by several novel characteristics. They integrate cyber, physical, and social elements, facilitating collaboration among sensors, applications, and users to deliver a unique service. Their diffuse nature leads to inquiries about the precise location of data when it is stored in the cloud. Additionally, these systems are capable of continuous reconfiguration, allowing nodes to join and leave the network seamlessly, much like the operation of Uber. Finally, they possess an intimate aspect, as demonstrated by devices such as Fitbit, which monitor heart rates and archive the data in the cloud.

The introduction of these new characteristics renders traditional qualities such as safety, reliability, and usability, which were previously focused on the technical system alone, inadequate. It is imperative to consider additional qualities that reflect the complex relationship between social and technical factors. Trust stands out as a primary quality in this context. Designers of Cyber Physical Social Systems must therefore address not only how to ensure the system's safety and reliability but also how to cultivate a perception of trustworthiness.

The importance of trust in a system is paramount, as a system perceived as untrustworthy may be either unused or misapplied, thus defeating its original purpose. For instance, if users are skeptical about the privacy of a health monitoring service, they might temporarily interfere with a sensor, leading to a misdiagnosis of a significant health condition by the system. In the rapidly developing integrated cyber-physical smart world, entities are heavily interconnected within a network, particularly concerning security, privacy, the integrity of data, and the reliability of services. The necessity for one entity to trust another can often lead to vulnerabilities. To effectively manage these vulnerabilities in the design, operation, and management of engineering systems, it is essential to formalize the concept of "trust" and to approach it with a methodical framework. This review aims to identify current trust management mechanisms and categorize them according to their primary technologies, thereby revealing the limitations inherent in each category. By analyzing critical aspects of trust, we underscore these limitations and highlight areas where further research is needed. Our mission is to provide a comprehensive analysis of the field while addressing the challenges that have been recognized. We aim to assist readers in navigating the extensive literature that exists within this domain. Additionally, we seek to guide readers in the creation of a strong trust management system, thereby enabling them to explore the literature based on the methods employed and the key attributes.

The rest of the paper is organized as follows. We discuss the related work in Section 2; In Section 3, we show the fundamental concepts of Trust and its features; In Section 4, we present trust management in Cyber-Physical-Social Systems (CPSS); finally, conclusions are drawn in Section 5.

2. Related work

Mon et al. [2] proposed a cluster-based framework that incorporates a central trust entity. A cluster is first established, and the master node is chosen according to its trust scores, which encompass both Quality of Service (QoS) and social trust attributes. The master node receives regular updates based on its trust value, utilizing clustering techniques grounded in regression models. Experiments were conducted to evaluate the effectiveness of this method, with results illustrated in several diagrams. A limitation of this system is the requirement for trust values to establish clusters, raising questions about the bootstrapping phase. Nonetheless, a key strength of this solution lies in its emphasis on data trust, which plays a vital role in identifying false messages, even from nodes that are generally considered reliable.

Bao et al. [3] proposed a dynamic trust management protocol for Internet of Things (IoT) systems. This protocol evaluates trust by incorporating both direct and indirect recommendations, as well as social factors. Moreover, the scalability concerning the storage of trust values is discussed. Malicious nodes are capable of executing BMA, SPA, and BSA attacks. The organization of nodes into communities allows for a trust evaluation process that considers social factors including honesty, cooperativeness, and the associated community. Experiments were performed to assess the impact of different weights in the trust evaluation and the protocol's ability to withstand trust-related attacks. In [4], a system is proposed in which nodes establish communities based on shared interests. This distributed protocol allows each node to assess the trustworthiness of other nodes within these communities. The system is designed to adapt to shifts in community interests by dynamically adjusting the trust parameters. To enhance scalability, the authors introduced a storage management strategy aimed at conserving memory, particularly given the resource limitations of IoT devices. Additionally, malicious nodes are capable of executing BMA, SPA, and BSA attacks. Experiments were conducted to evaluate the impact of varying certain weight values associated with the trust evaluation process, as well as the trust assessment under conditions of limited storage capacity.

Khajehasani et al. [5] analyze the extent of trust in the content shared on these social networks. This research is conducted through a survey, targeting a randomly selected group of 200 students from Sirjan University of Technology. The statistical outcomes suggest that there is no significant link between the time spent on virtual social networks and their daily engagement in terms of trust. Conversely, a consistent and significant relationship is identified between the type of membership in these networks and the trust that students have in them. In [6] introduce a deep learning model aimed at classifying the behavioral types found in the CICIDS2017 dataset through the application of three learning strategies. The dataset was divided among ten simulated nodes for the experiments. The centralized learning method yielded an F-Score of 98%, while the distributed learning approach resulted in an average F-Score of 78% across the ten nodes. In [7], an efficient automated system has been established to improve the quality of the organization’s operations, minimize time and resource expenditure, and enhances both accuracy and security. A comprehensive description of the system's hardware and software components was provided, followed by experiments aimed at assessing its performance. The findings indicated that the developed intelligent institutional system delivered precise and dependable measurements of multiple parameters. Additionally, the camera-based fire detection system successfully identified and notified users of potential fire hazards, as well as detected wall cracks that could jeopardize the institution's structural integrity, prompting necessary preventive actions.

S. helmy et al. [8] developed an advanced device for the continuous monitoring of cardiac patients, aimed at optimizing the time and effort required from both healthcare providers and patients. This design seeks to alleviate congestion in medical facilities while addressing the demands of a fast-paced lifestyle that necessitates regular health evaluations through remote monitoring. The prototype leverages IoT technology to track various health indicators, such as blood oxygen saturation, heart rate, and body temperature, all of which can be accessed and analyzed remotely. Utilizing a Bluetooth module, the device facilitates the collection of data and delivers real-time updates regarding the patient's condition. A comprehensive assessment was conducted on several individuals using diverse parameters. In summary, the Internet of Things (IoT) is proposed as an effective solution for the timely and efficient monitoring of cardiac patients within the healthcare system.

3. Trust as a Fundamental Concept and Features

The idea of managing trustworthiness is advancing swiftly and has been broadly utilized in a range of disciplines [9] along with their applications (e.g., Metaverse). It is vital to ascertain the most appropriate optimal parameters tailored to each specific CPSS ecosystem.

3.1 Trusts as a Fundamental Concept

Trust serves as a crucial element in human existence, facilitating the development of interpersonal relationships. With the rapid evolution of scientific advancements, especially in hardware and software, the notion of trust is becoming more integrated into diverse disciplines that require the examination of human behavior, such as sociology, psychology, economics, and computer science. [10].
The definition of trust is interpreted differently throughout various fields of study as shown in Table 1.

Table 1 Trust areas as a Fundamental Concept

Domains	Short Description
Sociology	A fundamental element of trust in sociological research is its capacity to cultivate reliable social relationships within a community, where trust is defined as the shared conviction held by all participants in the dialogue.
Psychology	Trust in psychology is conceptualized as the self-confidence that one individual places in another. This self-confidence can vary significantly based on different contexts, including the location, the criticality of the task, and the timing of the situation.
Economics	Trust can be described as a fundamental aspect of a business relationship that fosters reliance on both the partners involved and the transactions carried out with them.
Computer Science	Over thirty years ago, the preliminary versions of trust were characterized as a Unix computer program aimed at being free from Trojan horses, as discussed in a Turing Award lecture by Thompson.

Fundamentally, trust can be described as the confidence that one individual (the trustor) places in another individual (the trustee) [10], the idea encompasses several components, including the temporal aspect, human behavior, and environmental influences. This section offers a brief examination of trust in diverse areas.

- Trust in Sociology: Sociology examines the dynamics of human social relationships, the structure of societies, interpersonal interactions, and the processes that influence the transformation and continuity of these relationships and societal frameworks. The main objective of trust in sociological analysis is to delve into the development of dependable social relationships within a community, where trust is interpreted as the common belief that binds all participants in a discourse.
- Trust in Psychology: Psychology examines the attributes of the human mind, particularly within a defined context. In the field of psychology, trust is defined as an individual's confidence in another person, and this confidence can fluctuate based on various factors such as the environment, the significance of the task at hand, and the temporal context.
- Trust in Economics: Economics is a field within the social sciences that studies the production and distribution of goods and services. In this realm, trust is articulated as the confidence in commercial engagements, where one party maintains a belief in the reliability and credibility of the other party participating in the transaction.
- Trust in Computer Science: The primary objective is to develop a system that ensures security, meets its intended purpose, and can readily identify and efficiently recover from any unforeseen vulnerabilities. Current paradigms in computer science focus on data communication and processing, necessitating the implementation of secure and reliable management strategies.

3.2 Features of Trust

Trust may be measured in several ways by taking into account the following features.

- Subjective: From a social perspective, subjective trust can be described as the assessment of trust that is based on the importance of an object. This evaluation is influenced by the trustor's direct experiences, referred to as direct trust, and the opinions or feedback received from other individuals, which is termed indirect trust.
- Objective: The concept of objective trust is differentiated from subjective trust by its reliance on the collective evaluations provided by all components within the network. In this model, trust-related information for each component is made publicly available to all users. Additionally, the accessibility of this information is enhanced through the use of distributed hash tables, with its ongoing management being assured by social objects that have already been established as reliable.
- Localality: It represents the confidence developed through an object-object relationship, where one object evaluates the dependability of another by utilizing local information, which encompasses its observations and past experiences.
- Globality: Global trust, as opposed to local trust, is perceived as the reputation of an entity within the network. The trust score assigned to each entity is derived from the aggregation of local information provided by all other entities within the network.
- Context-Specific: The degree of trust that one object has in another is influenced by the context in which they exist. Typically, the relationship of trust between these objects is not static; it fluctuates based on various elements, including time, geographical location, and energy conditions.
- Asymmetric: Trust is characterized by its asymmetric nature; that is, when object A places its trust in object B, it does not ensure that B reciprocates that trust towards A.

4. Trust Management in Cyber-Physical-Social Systems (CPSS)

4.1 CPSS Architecture

Cyber Physical Social Systems (CPSS) can be characterized by their fundamental components such as cyber space, physical space, and social space.

- Cyber System (CS): The structure of a cyber system is formed by technical components such as computers, software, and networks, with human engagement occurring through the reading and writing of information, while not being considered a fundamental part of the system. A pertinent example is the information system found in healthcare institutions, which permits physicians, nurses, and patients to access medical information.
- Cyber-Physical Systems (CPS): integrate a cyber system, a physical system, and potentially human operators. The principal communication within CPS is established between the cyber and physical systems, with human interaction not being a critical component. The cyber system can collect, archive, and transmit data related to physical components, and it can employ actuators to affect the physical systems. An illustrative example of this is a CPS that tracks a diabetes patient's blood sugar levels and adjusts insulin delivery through an insulin pump.
- The Cyber-Physical-Social System (CPSS) is an integrated framework that includes a computational system, physical object, and social components that interact. These systems

consider the interplay between cybernetic and physical elements, along with the social interactions among the various social components. Healthcare is examples of these social relationships encompass physician-patient, nurse-patient, and physician-nurse interactions, among others.

4.2 Trust Management in CPSS

In the CPSS environment, recognizing malicious nodes is crucial. In our everyday interactions, we aim to connect and collaborate with reliable individuals, both in personal and professional contexts. Likewise, for CPSS devices to function optimally, they must engage with trustworthy nodes that deliver precise information. The foundation of trust relies on the accurate identification of CPSS devices. Each device must have a distinct identity to be acknowledged within the network. This distinct identity allows the device to link to the network and interact with other devices. Once authentication is successfully completed, access control mechanisms are tasked with regulating the actions and data that each device is allowed to access. It is imperative to maintain data integrity and confidentiality during both transmission and storage to defend against unauthorized access and manipulation. The dependability of devices is vital for ensuring the functionality and security of CPSS networks. This process includes evaluating device behavior, observing anomalies, and withdrawing trust when necessary. It commences with the collection of data from other nodes, which is subsequently utilized to assess the trust level, and this information is stored and applied accordingly. The established trust level determines whether a node can trust or interact with another node. Just as individuals would hesitate to finalize a transaction with someone they do not trust, the same concept is applicable to CPSS nodes within a network.

4.2.1 Trust Computation in CPSS

Trust metrics are defined as the characteristics selected and integrated to establish trust. These characteristics may be determined based on a node's social trust metrics and/or its quality of service (QoS) trust metrics.

- Social Metrics: The measurements of social trust demonstrate the social conduct of nodes, concentrating on the relationships between the owners of CPSS devices. This assessment takes into account multiple factors, including integrity, kindness, honesty, friendship, common interests, and selflessness [11].
- QoS Metrics: It illustrates the degree of confidence in a node's ability to ensure Quality of Service (QoS), which is quantified through reliability, effectiveness, data delivery ratio, throughput, and task completion rates.

Trust formation can occur through a singular dimension, focusing solely on either positive or negative Quality of Service (QoS), or it can be established through multiple dimensions, incorporating trust models that consider both QoS and social trust metrics.

- Single Trust: A single trust indicates that only one trust metric, such as the quality-of-service metric, is employed to evaluate the overall level of trust [12].
- Multi Trust: It utilizes the concept of trust as a multifaceted idea. For example, it integrates various elements, including social factors and Quality of Service (QoS) metrics, to create a comprehensive trust score [13].

Trust Aggregation: The system consists of techniques that synthesize trust observations to arrive at a singular trust score. Various aggregation techniques have been investigated in the body of research literature [14]; this includes, but is not restricted to, the method that utilizes a weighted sum [15], belief theory [16], Bayesian system [12], fuzzy logic [13], regression analysis [17], and machine learning [18]. Trust aggregation represents a crucial component of any trust computation model; thus, it is essential to examine the various trust aggregation techniques in a comparative context as shown in Figure 2.

- Weighted Sum: This method is acknowledged as one of the easiest and most prevalent aggregation techniques. It is referred to as the average weighted mean of each metric or value, where weights are assigned to each metric to calculate a comprehensive score [15].
- Belief Theory: known as Dempster-Shafer Theory (DST) or evidence theory, is designed to integrate diverse types of evidence, resulting in a degree of belief that ranges from 0 to 1. Within this framework, a value of 0 indicates no support, whereas a value of 1 signifies complete support for the evidence presented. DST provides an interval of uncertainty defined by belief (bel) and plausibility (pla), in contrast to traditional probability measures [16].
- A Bayesian system: Based on the principles established by Bayes' theorem, which integrates prior probability, posterior probability associated with the data, node, or interaction, along with the likelihood function [12].
- Machine learning: Depend on data aggregation, employing both clustering (unsupervised algorithms) and classification (supervised algorithms). When labeled data is unavailable, the aggregation process is divided into two phases: the first phase involves the use of unsupervised algorithms, including k-means clustering, agglomerative clustering, and spectral clustering, to label the data. The second phase employs supervised algorithms such as support vector machines, logistic regression, and random forests to classify the nodes or objects as either trustworthy or untrustworthy [18].
- Regression Analysis: This statistical technique utilizes the slope of lines to integrate multiple independent variables. There are two main categories of regression: i) Linear regression, which estimates a single dependent variable by utilizing data from one independent variable, and ii) multiple regression, which anticipates the result of a dependent variable based on information from several independent variables [17].
- Fuzzy Logic: Fuzzy logic differentiates itself from traditional Boolean logic by allowing for imprecise inputs rather than being limited to binary values of 0 or 1. This flexibility offers a reasoning framework that more closely mirrors human cognitive processes. As a result, fuzzy logic is particularly effective in addressing uncertainty and ambiguity, especially in matters of trust. Generally, a fuzzy aggregation process can be categorized into four essential stages: i) Fuzzy Controller – which transforms real values into fuzzy sets, ii) Fuzzy Logic Rules – which involve the formulation of fuzzy logic rules through techniques such as fuzzy intersection and fuzzy union, iii) Membership Function (Mapping Function) – which is tasked with converting fuzzy input sets into fuzzy output sets, and iv) Defuzzied Controller – which reverts fuzzy output sets back into real values. [13].

4.2.2 Trust Propagation in CPSS

Trust plays a crucial role in enhancing comprehension of its propagation within a network, which is typically classified into three main categories.

- Centralized: Centralized frameworks are based on a central authority that is chiefly tasked with (a) acquiring trust-related information to assess trust and (b) distributing this information across the network. The centralized control frameworks exhibit vulnerability to a singular point of failure, potentially resulting in the total failure of the network.
- Distributed: In distributed systems, entities are accountable for the computation and dissemination of trust throughout the network, operating without a central governing body. Although this scheme offers a remedy for the single point of failure, it is not without its challenges, including the necessity for honest trust computation, the management of computational resources, and ensuring unbiased trust propagation across the entire network.
- Hybrid: Hybrid schemes are typically employed to address the difficulties associated with both centralized and distributed systems. Additionally, these schemes categorize propagation into two primary types: locally distributed and globally centralized, as well as locally centralized and globally distributed.

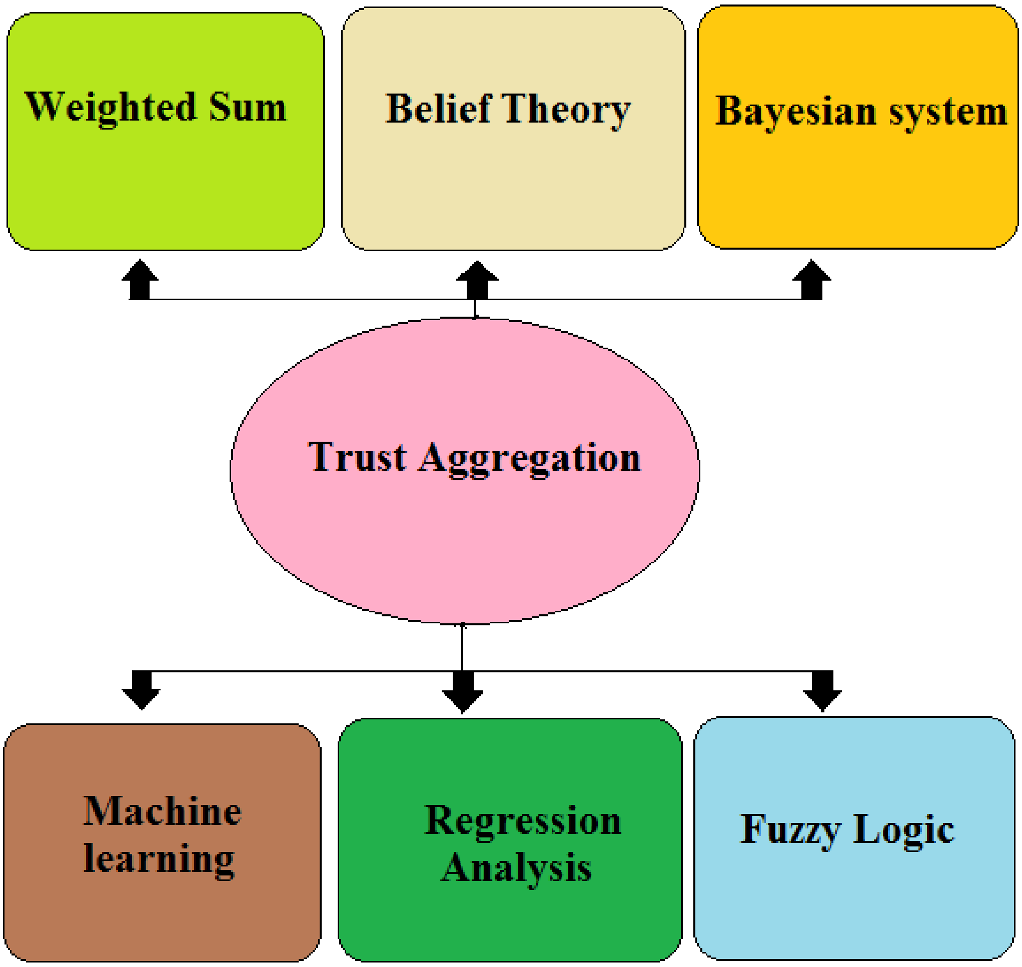


Figure. 2: Trust Aggregation Types

4.2.3 Trust Update in CPSS

At the termination of a transaction or at designated time intervals, the trust score assigned to a trustee is adjusted based on their performance. Therefore, the update can be executed in three different ways.

- Event-driven: This strategy entails updating trust after every transaction or when a particular event takes place. However, this kind of update results in higher traffic overhead in networks that experience more frequent transactions.
- Time-driven: Within a time-driven framework, trust is accumulated and revised periodically after specified time intervals. This strategy effectively resolves the difficulties inherent in event-driven approaches; however, the task of determining an appropriate time interval continues to be a challenge.
- Hybrid: Various research efforts investigate the dual approaches of event-driven and time-driven trust updates, indicating that trust can be modified periodically and/or in response to particular events occurring after an interaction.

4.2.4 Attacks Associated with Trust in CPSS

A node may engage in malicious activities to undermine the fundamental operations of the network and its services. Trust-related attacks can be classified into two categories, as illustrated in the accompanying Figure 3. Individual attacks and collusion-based attacks [19], [20].

Individual attacks pertain to assaults initiated by a single entity. Below, several prevalent types of individual attacks are succinctly examined:

- Self-Promoting Attacks (SPA): In this category of attacks, a node can bolster its significance by regularly issuing commendable recommendations for it, thus positioning itself as a preferred service provider. Upon being selected, the node may subsequently behave maliciously.
- Whitewashing Attacks (WA): A whitewashing attack allows a node to disconnect from the network or an application and later rejoin, thereby enabling it to rehabilitate its reputation and erase its unfavorable image.
- Discriminatory Attacks (DA): A node systematically attacks other nodes that do not have a diverse array of mutual friends, influenced by human intuition or a natural affinity for friends in Complex Peer-to-Peer Systems (CPSS). This type of attack is known as a selective behavior attack, wherein a node shows competence in relation to a particular service or node while being ineffective with others.
- Opportunistic Service Attacks (OSA): An object can effectively improve its reputation by offering exemplary service, particularly when its reputation has been tarnished by poor service. When an object maintains a high reputation, it is capable of collaborating with other objects to conduct collusion-based attacks.
- On-Off attacks (OOA): Although similar to OSA, in these forms of attacks, an object randomly switches between offering good and poor services to avoid being marked as a low-reputation node, thereby boosting its chances of being chosen as a service provider.

Collusion attacks are characterized by a collective action taken by a group of agents to influence the rating of a particular object, resulting in either an elevated or diminished assessment. The following are instances of collusion attacks.

- Bad Mouthing Attacks (BMA): Within the BMA system, a node has the potential to undermine the reputation of a reliable node by providing negative recommendations, which consequently diminishes its likelihood of being selected as a service provider.

- Ballot Stuffing Attacks (BSA): These types of attacks are carried out to elevate the reputation of malicious nodes in the network by issuing favorable reviews, consequently permitting the malicious node to be designated as a service provider.

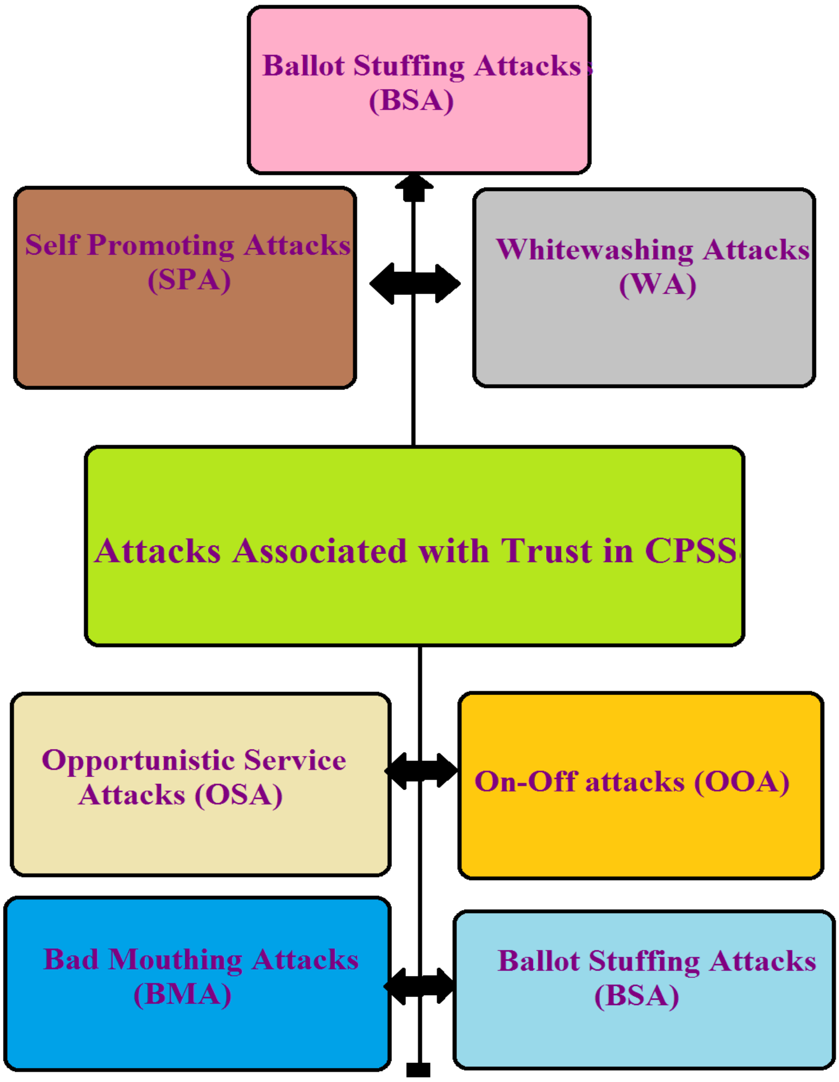

Ballot Stuffing Attacks (BSA)
Self Promoting Attacks (SPA)
Whitewashing Attacks (WA)
Attacks Associated with Trust in CPSS
Opportunistic Service Attacks (OSA)
On-Off attacks (OOA)
Bad Mouthing Attacks (BMA)
Ballot Stuffing Attacks (BSA)

Figure. 3: Trust Attacks in Cyber Physical Social Systems (CPSS)

4.2.5 Trust Decision in CPSS

The primary objective of developing a trust management system, following the calculation of a trustee's trust score, is to determine the trustworthiness of a node, utilizing one of the two techniques outlined below.

- Decision Based on Thresholds: Decision-making methods that are threshold-based rely on either a ranking function or a predetermined threshold value to guide their choices. Additionally, the threshold values can be modified to suit dynamic environments, whereas static values are employed for particular applications or services.

- Decision-Making Based on Context: This method establishes the guidelines utilized to determine and classify an object as malicious or benign by leveraging contextual information such as location, time factors, energy levels, and other relevant parameters.

5. Conclusion

Security and trust are essential components in Cyber-Physical Social Systems (CPSS), particularly as devices may be deployed in potentially hostile environments. Trust management techniques provide a viable method for assessing the reliability of a node. The past decade has witnessed a growing interest among researchers in the area of trust management within CPSS, resulting in a vast array of literature that can be complex to navigate. In light of this, our research has delved into several pertinent topics; we contend that our study can aid readers in determining the most suitable methods and technologies for a given CPSS trust management mechanism, while also highlighting the challenges that need to be taken into account in the system design process. Additionally, our work may provide valuable insights for researchers seeking to identify future research opportunities.

References

1. Strategic Business Insights (Firm) and National Intelligence Council (U.S.). “Disruptive Civil Technologies: Six Technologies with Potential Impacts on UHS Interests Out tHo 2025 : Biogeron technology, Energy Storage Materials, Biofuels and Bio-based Chemicals, Clean Coal Technologies, Service Robotics, the Internet of Things”, National Intelligence Council (2008).
2. F. Anish Mon, G. W. Sathianesan, and R. Ram, Trust model for iot using cluster analysis: A centralized approach, Wireless Personal Communications. 127(4) (2021) 715–736.
3. F. Bao and I. R. Chen, Dynamic trust management for internet of things applications, In Proceedings of the 2012 International Workshop on Self- Aware Internet of Things, Self-IoT ’ 12, New York, NY, USA, 2012, p. 1‑6.
4. F. Bao, I. R. Chen, and J. Guo, Scalable, adaptive and survivable trust management for community of interest based internet of things systems, In 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS), 2013, p. 1‑7.
5. S. Khajehasani, L. ehyadegari, The Study on the Optimism and the Amount of Trust in Social Media Content and the Level of their Ethical Health among the Students of Sirjan University of Technology, International Journal of Intelligent Computing and Information Sciences. 19(1) 2019 38-45.
6. O. Elnakib, E. Shaaban, Federated Learning Enabled IDS for Internet of Things on non-IID Data, International Journal of Intelligent Computing and Information Sciences. 24(1) 2024 13-28.
7. A. Atta, M. Esmat, Controlling and Security System Using IOT Infrastructure and Image Processing in Educational Institutions, International Journal of Intelligent Computing and Information Sciences. 23(4) 2023 128-141.
8. S. helmy, A. Amar, E. El-Horabty, Internet of Things (IoT) based smart device for cardiac patients monitoring using Blynk App, International Journal of Intelligent Computing and Information Sciences. 22(4) 2022 86-99.
9. B. R. Schlenker, B. Helm, and J. T. Tedeschi, The Effects of Personality and Situational Variables on Behavioral Trust, Journal of personality and social psychology. 25(3) (1973) 419-427.
10. W. Sherchan, S. Nepal, and C. Paris, A Survey of Trust in Social Networks, ACM Computing Survey. 45(4) (2013) 1‑33.

11. M. Nitti, R. Girau, L. Atzori, and S. Member, Trustworthiness Management in the Social Internet of Things, IEEE Transactions on Knowledge and Data Engineering. 26(5) (2014) 1253–1266.
12. I. Chen, J. Guo, and F. Bao, Trust Management for SOA-Based IoT and Its Application to Service Composition, IEEE Transactions on Services Computing. 9(3) (2016) 482–495.
13. H. Xia, F. Xiao, S. Zhang, C. Hu, and X. Cheng, Trustworthiness Inference Framework in the Social Internet of Things: A Context- Aware Approach, in proceeding of IEEE Conference on Computer Communications (INFOCOM), 2019, p. 838–846.
14. R. K. Chahal, N. Kumar, and S. Batra, Trust Management in Social Internet of Things: A Taxonomy, Open Issues, and Challenges, Computer Communications. 150(1) (2020) 13 – 46.
15. A. A. Adewuyi, H. Cheng, Q. Shi, J. Cao, A. MacDermott, and X. Wang, CTRUST: A Dynamic Trust Model for Collaborative Applications in the Internet of Things, IEEE Internet of Things Journal. 6(3) (2019) 5432–5445.
16. M. Beynon, B. Curry, and P. Morgan, The Dempster–Shafer Theory of Evidence: An Alternative Approach to Multicriteria Decision Modelling, Omega. 2(1) (2000) 37–50.
17. R. Venkataraman, M. Pushpalatha, and T. R. Rao, Regression-based Trust Model for Mobile Ad Hoc Networks, IET Information Security. 6(3) (2012) 131–140.
18. S. Sagar, A. Mahmood, J. Kumar, and Q. Z. Sheng, A Time-Aware Similarity-Based Trust Computational Model for Social Internet of Things, in IEEE Global Communications Conference (GlobeCom), 2020, p. 1–6.
19. R. M.S., S. Pattar, R. Buyya, V. K.R., S. Iyengar, and L. Patnaik, Social Internet of Things (SIoT): Foundations, Thrust Areas, Systematic Review and Future Directions, Computer Communications. 139(1) (2019) 32 – 57.
20. S. A. Siddiqui, A. Mahmood, Q. Z. Sheng, H. Suzuki, and W. Ni, A Survey of Trust Management in the Internet of Vehicles, Electronics. 10(18) (2021) 2223.