

Trust-Based Energy Optimization for Data Aggregation in Wireless Sensor Networks

Ayush Sharma¹ and Dr. Sunny Arora²

^{1,2}CSE Department, Guru Kashi University, Bathinda, India
Email: ayush.sharma468@gmail.com, sunnyaro@gmail.com

Abstract—A wireless sensor network is made up of several sensor nodes that can come and go from the network as they choose. Sensor networks are implemented in remote locations and are tiny in size. Energy consumption thus emerges as the primary concern of WSN. Because sensor nodes have limited energy, the data, which is collected from the targeted environment, is sent straight to the main station. The data sent by different sensor nodes is received by the sink node. By identifying and removing similarities between the data from various sensor nodes, the decision-making process is implemented. Additionally, the sink deploys the acquired data locally and sends it to the networks that are executing it.

Index Terms— IOT, WSN, CTNR, Routing, Multi-level Hierarchy.

I. INTRODUCTION

The Internet of Things (IoT) has piqued the curiosity of academics throughout the globe because of its diverse range of features and capabilities. The use of wireless sensor networks (WSNs) is a pretty well-known IoT innovation. IoT with WSN support is used to collect environmental data and pinpoint important real-world occurrences. It can greatly enhance people's life through various applications, including medical monitoring, battle tracking, and environmental monitoring [1]. The true worth of these IoT smart applications can be ascertained by analyzing the data that the devices placed on it offer. The 2020 conceptual framework states that the Internet of Things framework consists of four fundamental components, which are as follows:

$$\text{IoT} = \text{Services} + \text{Data} + \text{Networks} + \text{Sensors}$$

Sensors are the information sources that make up wireless sensor networks, or WSNs. They comprise the core components of the Internet of Things. The sensors are located using the bottom layer. This layer is responsible for the production and use of the data. The edge layer is also known as the fog layer. This layer uses edge devices for a significant amount of compute, storage, and information sharing to ensure that the data is suitable, dependable, and available for its customers. With the help of strong machines positioned there, the cloud layer does data mining.

Internet of Things applications provides services to people throughout the world [2].

A. Information Fusion Based on Trust

The absence of benchmarking methods makes smart apps unable to handle problems with the reliability of their data sources. Managing the dependability of data sources is the primary priority in order to fully benefit from smart applications.

For example, the data providers cause false or misleading information to be transmitted, rendering it unauthentic. In this instance, the conventional security techniques are not able to mitigate the problem. Contrary to security, trust is characterized by the attributes of the sensors, including their honesty, accuracy, and reputation. Forecasting and scenario evaluation are made possible by the information fusion process, which combines many, potentially conflicting bits of information from various sources [3]. Combining data from many diverse data sources to provide a clear, inclusive, and integrated evaluation of the situation is the main objective of this approach. As a source of information, sensors produce data. The sink node or nodes collect this data and then combine it. The information fusion process can involve changes, reductions, integration, and replacements. In the end, a product is produced that offers greater value than could be predicted from a single source of knowledge.

The information fusion process is where behavioural issues such as the accuracy, reliability, and integrity [4] of information sources are most challenging to address.

These challenges are many. First, an information source or sink node might not be reliable. This suggests that they might intentionally change aggregated or merged datasets. A dishonest information source may therefore purposefully fabricate information in order to further their own agenda. Furthermore, the difficult-to-define personal trust traits can affect the accuracy rates of information from trustworthy sources. Because nodes may evaluate the same situation differently, there are a variety of accuracy rates. Review-based systems can operate with imprecise metrics by design according to the accuracy principle. The reliability, accuracy, and integrity of the information sources and sink nodes must therefore be ensured before depending on the fused data [5].

Below is a discussion of each layer's data fusion perspective:

1) *Perception Layer:*

This layer contains a variety of technologies, such as RFID and sensors. While sensor nodes are used to locate and gather information on environmental conditions, RFID technology concentrates on tracking and detecting objects [6]. It is necessary to estimate the Data Perception Trust (DPT) in this layer. To detect any erroneous computations, each sensor must evaluate the precision of its own detected data.

The quality of sensed data may really be impacted by a variety of internal and external factors, including environmental conditions and resource constraint. Therefore, before communicating, each node must resolve these problems and assess the precision of its readings. Only the most reliable data must be sent over the network. DPT guarantee mainly makes it possible to detect unforeseen threats, which is necessary to preserve the sensor's reputation and maintain the same level of trust in it.

2) *Network Layer:*

This layer enables data broadcasting, analysis, and inspection [7]. This layer is usually composed of two sub-layers: the transport layer and the processing layer. To provide each sub-layer with convenient trust levels, the division is carried out

a) *Transport Layer:*

Data is continuously exchanged between nodes in this layer. It is necessary to evaluate the communication trust between objects in order to guarantee that data can move between nodes without being impacted or altered. The evaluation of communication trust among nodes frequently hinges on how they interact and communicate over time. Selfish and malevolent nodes that purposefully avoid connecting with neighboring nodes in an attempt to deceive the network can be identified using this trust level [8].

Communication trust includes both object trust and data trust. Current trust management stages typically center on the object trust. Current trust management plans usually show interest in the entity trust. People assume that if something is highly trusted, the information it conveys must also be trustworthy.

b) *Processing layer:*

Analysis and integration of the data gathered from this layer are the primary focus in order to produce an output that is reliable and trustworthy. The idea that the Data Fusion Trust decides whether or not the fusion approach has an effect on the information's credibility is taken into consideration. To ensure that the fusion produces high-quality results, a few requirements must be fulfilled. First, only trustworthy nodes should be selected to aggregate data. Second, only trusted nodes should take part in the fusion when DPT and CT are combined. Third, the data fusion process need to improve the quality of the data.

3) *Application Layer:*

This tier provides a variety of sophisticated services to the end users. Different information might be derived from the same detected data based on the needs of the consumers. Customers' demands must be accurately met by the required Internet of Things services at the right time and place [9]. The two main factors that determine service quality are the quality of the sensed data and the accuracy of the fusion result. These facilities may be

useful for a variety of industries, including public safety, healthcare, transportation, logistics management, location-based services, and the environment.

A level of trust assurance is insufficient to ensure the reliability of the information supplied. Since then, avoiding assessing trust at any level has an effect on the accuracy of the data.

B. IoT data fusion trust guarantee

Maintaining the accuracy of the data is necessary for Data Fusion Trust even while the guarantees of Data Perception Trust and CT are provided. The DFT is significantly impacted by the performance of the fusion node in terms of security, energy consumption, computation, and storage capacity. An overview of popular DFT systems used in Wireless Sensor Network-assisted IoT is provided below:

1) Witness-based approach:

This strategy assumes that the network includes sensor nodes and data aggregators in addition to witness nodes. A witness may function as a node in a data fusion network to validate or refute the data aggregator's result [10]. To verify the accuracy of the results, a data aggregator collects witness testimony. Every witness acts as a gauge for the Message Authentication Code (MAC) of the fusion result that was attained. The MAC is composed of the key, the fusion result, and the witness ID. Each witness trades a unique secret key with the sink node. The main objective is to stop the fusion node from creating the data whose aggregation is carried out since witnesses are unable to speak directly with sink nodes. This method then uses the n -out-of- $(m+1)$ methodology to validate the correctness.

2) Weighted-trust evaluation (WTE):

This indicates how each report influences the ultimate decision and represents a node's credibility. The IoT architecture is composed of three layers. The uppermost layer consists of sensor nodes [11]. The forwarding nodes in the next tier are in charge of calculating the outcomes of the fusion, updating the weights of every sensor node in the cluster, and transmitting the data to the next layer. Actually, if the fusion result does not match the data that the sensor node supplied, it will be penalized and have its WTE decreased. The penalty level is determined by the total number of sensor nodes in the same cluster and the number of nodes generating different reports.

If the WTE drops below a specified threshold, the participating entity will be classified as hostile. APs make up the final layer, which verifies the accuracy of the data received. The APs assign a weight to each forwarding node (FN) and subtract the newly obtained result before sending it to the wired network.

3) Double Cluster Heads Model (DCHM):

The operation of this framework requires MCH and VCH. The data is combined using these two objects, and the outliers are stored in two distinct indexes. In order to calculate the cluster head and vice-cluster head function perfection, this data will thereafter be sent to the base station for evaluation of the dissimilarity coefficient between two results. This model's primary objective is to select trustworthy CHs. This model is predicated on the notion that, if a CH or VCH's residual energy falls below a particular threshold, a re-selected message is transmitted within the cluster [12].

Therefore, the two people with the most trust and remaining energy will be appointed to the CH and VCH roles. Aggregation nodes are always responsible for a number of tasks. However, it must first assess the reliability of the fusion result. This framework employs a Bayesian data fusion technique to estimate the accuracy and reliability of the fusion output in accordance with the previous allocations.

II. LITERATURE SURVEY

A thorough assessment of TMs (trust models) based on a number of crucial factors, including scalability, overhead, and resilience, was proposed by I. Souissi et al. (2019) [13]. These frameworks failed to meet the requirements of all the aforementioned criteria and integrate the Data Perception Trust, CT (Communication Trust), and DFT (Data Fusion Trust) methodologies. Furthermore, the main emphasis was on proposing new systems that incorporated the methodologies mentioned above to enhance the process of making trust-based decisions for merging data in the Internet of Things. Additionally, an adaptive trust management model, or TMM, was proposed. The recommended method did a good job of modifying the object's resources in relation to the requirements of Internet of Things applications.

A block chain-based STMS (semi-centralized trust management system) paradigm was created by Y. Liu et al. in 2022 for both single and multiple domains [14]. The Internet of Things (IoT) devices were centralized and arranged through the use of cloud servers. In order to construct the proposed rotation-based consensus protocol in a decentralized manner to allow the cross-domain data interchange, these servers helped maintain a rating data

ledger in each domain. When direct and indirect trust data were combined to assess the trust value of dynamic harmful devices, a computational trust system was created. Ultimately, experiments were conducted to simulate the model under investigation under various conditions. According to the testing results, the model under investigation was able to identify malicious devices and lessen their effects.

A new CAT (context-aware trust) paradigm for lightweight IoT (Internet of Things) devices was introduced by N. Li et al. in 2019 [15]. A trustworthy summary of a service provider that did not have historical behaviour records was provided. It was possible for a trust or to determine the significance of context items. As a result, the unique decisions were made using the same record of reliability. Various attacks were initiated to calculate the model that was presented. The outcomes confirmed that the model was resistant to a variety of attacks, including on-off and negative mouthing attacks. Additionally, the significance of a few key measures was also established. A new framework called CTRUST was presented by A. A. Adewuyi et al. in 2019 [16]. Using this approach, the trust was precisely parameterized, and belief functions were used to calculate the recommendations. The effect of trust maturity and decay on the trust evaluation process was investigated. Each trust aspect was modeled using the appropriate mathematical functions. Accuracy, convergence, and resilience of the resulting utility are evaluated in order to replicate the introduced framework in a collaborative download application. The outcomes showed that the proposed framework worked well in terms of security and efficacy.

A safe and long-lasting trust system was proposed by A. Kavitha et al. in 2022 [17]. This approach was helpful in identifying the malicious nodes and improving mote cooperation. Both direct and indirect trust are used to separate the malicious nodes from the legitimate ones. To assess the direct trust, a node's packet-forwarding behaviour was taken into account. To observe the packet forwarding behaviour of neighbours, a new two-hop model was proposed. When the recommendations were combined, the indirect trust was assessed with the aid of the weighted D-S theory. According to this hypothesis, a novel similarity approach was used to measure the weight of the recommendations made by various neighbours.

The dynamic weight computation is counted using a variety of interactions. The findings demonstrated that the proposed mechanism was effective and robust against the NS-2 simulator's packet drop/modification attacks, bad-mouthing, on-off attacks, and collusion attacks.

A MATW (multi-layer adaptive and trust-based weighting) method was used by B. Shala et al. (2020) to create an efficient trust framework [18]. Additionally, many trust measurements and associated mathematical models were used to assess the trust. After that, a novel method for carrying out incentive processes in the IoT market was proposed. Smart contracts and control loops were used for this. The main goal was to motivate the individuals to keep improving their behaviour. Ultimately, the created framework's dependability was demonstrated. The experimental results showed that, when compared to the conventional approaches in different situations, the created framework was resilient to certain attacks.

A ML (machine learning) enabled TE (trust evaluation) technique was created by W. Ma et al. in 2021 [19]. An ADL (deep learning) technique is used to aggregate network QoS (quality of service) trust attributes in order to build a behavioural framework for a specific IoT (Internet of Things) device. The behavioural framework forecasted the resemblance between actual network behaviour and network behaviour, which was then calculated to gauge trust. Trust values aided in the decision-making process by providing an illustration of a device's trust status. Finally, the experimentation quantified the designed technique. According to the findings, the method was effective.

A block chain-based trust system for Wireless Sensor Internet of Things (WSIoTs) was suggested by N. Javaid et al. in 2022 [20]. Furthermore, the Dijkstra algorithm was used to recommend a routing protocol that would effectively connect network nodes and prevent incorrect gaps between standard sensor nodes and base stations. Additionally, the network's transparency was provided by the block chain's immutable record of node transactions. The consensus mechanism known as PoA (Proof of Authority) was introduced and used to add and validate transactions in the blocks. An interplanetary file system, a distributed platform, was used to store the data in a reliable and economical manner. The results of the simulation demonstrated that, in comparison to previous algorithms, the provided technique improved the system by up to 13%. Furthermore, the suggested framework was shown to be reliable in terms of energy consumption, node status, gas consumption, and throughput.

A Block chain DIT (Decentralised Interoperable Trust) paradigm for IoT (Internet of Things) zones was developed by E. M. Abou-Nassar et al. in 2020 [21]. An ITIS (Indirect Trust Inference System) helped to mitigate the semantic gaps and improve TF (trustworthy factor) estimation utilizing the network nodes and edges, while a smart contract guaranteed the authenticity of the budgets. An encrypted block chain ripple chain is used to establish trustworthy communication. In order to address the fusion and integration problems, the nodes were verified based on their interoperable structure to implement regulated communication.

Additionally, Ethereum and the ripple block chain are taken into consideration for linking and combining requests across trustworthy zones. Compared to alternative approaches, the developed model was more scalable, interoperable, mutually authentic, dependable, and protected the privacy and security of the data. A L/W-HMT (Light-weight Hidden Markov Model) was proposed by G. Joshi et al. (2021) to assess trust in order to reduce the impact of compromised nodes and to limit the storing of redundant data in order to reduce overhead, memory, and energy usage [22]. A dependable and compromised state of a two-state Hidden Markov Model (HMM) was introduced. The number of packets that were transmitted, dropped, modified, and received determined how the state was changed. The forward likelihood function, or FLF, was used to calculate the node's trust value. The MATLAB simulation results validated the superiority of the proposed method, which improved detection rate (DR) by 6%, packet delivery rate (PDR) by 8%, and energy usage by about 70%. A DSTM (decentralized service-oriented trust management) algorithm was developed by M. Ebrahimi et al. in 2022 for the Internet of Things (IoT) in healthcare [23]. The evidence distance is used to punish the malicious units and supply healthcare information providers. To estimate trust based on recommenders' direct experiences and indirect input, a context-aware framework was used. To estimate the level of confidence in a source or service, indirect trust values and the combinatorial laws of evidence theory were taken into consideration. In terms of dynamic metrics, the established algorithm's security against on-off, good-mouthing, and bad-mouthing attacks was demonstrated. The outcomes showed that the developed algorithm was reliable and effective. Before negotiating a service level agreement (SLA), F. Li et al. (2022) proposed a trust model for identifying the reliable service providers in a dynamic Internet of Things (IoT) environment [24]. Using historical data from previous negotiations and the system's observed run-time effectiveness, this model concentrated on creating a trust credit to show the SLA's fulfilment and potential negotiation success rate. The Rough Set hypothesis was used to predict the success rate of negotiations. Based on the monitored data, BI (Bayesian Inference) was used to assume the possibility of SLA breach. The results of the simulation demonstrated the viability and effectiveness of the proposed approach.

III. RESEARCH METHODOLOGY

One of the most important requirements for clustered wireless sensor networks is the random distribution of nodes. In order to generate the cluster heads (CHs), the sensor nodes (SNs) are distributed at random. As a result, several problems arise. Because of the incidence of energy usage issues, avoiding the CH's disposability becomes crucial. Preventing long-distance communication in CH and placing the nodes beneath them is the next main emphasis. The nodes that are chosen are referred to as CH, and the inefficient suggested standards are unable to pick the nodes. The nodes' conditions make their existence in the network and in remote areas more complicated. As a result, inappropriate nodes are produced.

The nodes are regarded as CHs when the intra-cluster energy is maximized. Authentic motes use less energy than the receiver and SNs. Synchronous broad spectrum production on the system reduces the nodes' battery energy consumption.

Choosing the parent node for each CH in order to separate the actions is the main focus. Maximum productivity is then achieved. The implementation of two value functions by each SN helps them choose the CH. The functions are created taking into account the nodes' degree, and the potential of neighbour motes is calculated by calculating their distance from the sink. In order to generate the CH, nodes with a higher degree must form. In order to avoid expensive communications, the higher degreed CH can encompass a vast number of nodes. Thus, after reducing the energy used by the nodes, the network's lifespan is extended. Sending a Hello message with identity is the main focus of the first stage. When calculating the distance between each mote and the sink, the SS is taken into account. Additionally, its primary objective is to send an INTIAL-MSG with an ID and distance between each node and sink. Additionally, the distance between a node and its neighbours is calculated. The node uses the calculation method provided in eq. (1) to measure the CH as follows:

$$R_{CH} = R_{min} * [1 + (\frac{d_{BS} - d_{BSmin}}{d_{BSmax} - d_{BSmin}})] \quad (1)$$

This indicates the minimum cluster size that can be used as a protocol metric. The distance between the nearest node and the sink is represented by, while the distance between the farthest node and the sink is shown by. In order to offer the node with appropriateness and choose it as CH, the value function is run to calculate a value for every mote.

$$F_{CH-value} = \alpha * N_{deg} + \frac{\beta}{MSD_{deg}} + \frac{\gamma}{d_{BS}} \quad (2)$$

α , β , and γ stand for the constant weights, and their values fall between 0 and 1. Every node in the networks is given the same, modifiable values. The mean square distance between the neighbouring nodes is indicated by, while the radius of the number of neighbouring nodes is given by. The parameter is used to show how far each node is from the sink. The values of total CHs at a given time are calculated using the expected values. The improved value produced for each mote is therefore F(CH-value). In order to attain the improved values that fall between 0 and 1, each node seeks to observe other nodes. Additionally, each node is used to generate a random number between 0 and 1. When the value is less than that, the node is considered a candidate and chosen as the cluster leader.

Once the nodes have been chosen as CH, they are compared using the radius and residual energy. A node is regarded as a CH if it has RE. This node provides the broadcast code and ID. All of the motes in the network are aware of CH's stature.

Using the signal intensity as a guide, a non-CH mote assists in locating the closest CH. The energy cluster's intra-cluster communication is determined by the relevant components, like the cluster. The cluster's communication has been very expensive, as has the energy used for node radio and distance. The intra-cluster power increases as a result.

Additionally, centrality is defined in this study as a significant tactic. In order to reduce the intra-cluster energy, the second power average is reduced the closer the receiver node is to the central cluster. The energy is influenced by many factors. According to the suggested criteria, cache nodes cannot choose nodes in challenging circumstances. In order to choose any node as a volunteer node, the main goal is to calculate the value of each step for each non-CH node.

$$Access\ Time = H * T_c + (1 - H)(T_c + T_m) \quad (3)$$

IV. CONCLUSION

An energy-efficient routing method with the potential to extend WSN's lifespan is the CTNR. Gateway nodes are used in this study to improve the CTNR protocol. The suggested protocol will use location-based clustering to partition the entire network into clusters. In each cluster, CH is chosen based on energy and distance. The sensor node with the greatest energy and the shortest sink distance will be chosen to be the cluster head. Based on energy, the nodes that cannot be chosen as cluster heads will be chosen as leader nodes. The network's gateway nodes will be installed last. Information from the sensor nodes is sent to the cluster head, who then forwards it to the leader nodes, who in turn forward it to the gateway node. Information is sent to the sink via the gateway node. The proposed method is simulated using MATLAB, and the number of live nodes, dead nodes, and packets sent over the network are taken into account when analyzing the results. When compared to the current strategy, the findings show that the proposed method is effective in reducing the number of dead nodes, increasing the number of alive nodes, and transmitting packets.

REFERENCES

- [1] G. Fortino, L. Fotia, F. Messina, D. Rosaci and G. M. L. Sarné, "Trust and Reputation in the Internet of Things: State-of-the-Art and Research Challenges," in IEEE Access, vol. 8, pp. 60117-60125, 2020
- [2] R. Rani, S. Kumar and U. Dohare, "Trust Evaluation for Light Weight Security in Sensor Enabled Internet of Things: Game Theory Oriented Approach," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8421-8432, Oct. 2019,
- [3] E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O. -Y. Song, A. K. Bashir and A. A. A. El-Latif, "DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems," in IEEE Access, vol. 8, pp. 111223-111238, 2020
- [4] M. Bahutair, A. Bouguettaya and A. G. Neiat, "Multi-Perspective Trust Management Framework for Crowdsourced IoT Services," in IEEE Transactions on Services Computing, vol. 15, no. 4, pp. 2396-2409, 1 July-Aug. 2022
- [5] S. V. Shankhpal and S. H. Brahmananda, "Design and Development of trust management scheme for the internet of things based on the optimization algorithm," 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), Gwalior, India, 2020, pp. 207-211
- [6] A. Salunke and S. Bhambar, "Comparative Study of Trust and Reputation Security Models in IoT Networks," 2019 International Conference on Intelligent Computing and Control Systems (ICCS), Madurai, India, 2019, pp. 830-835
- [7] Y. Liu, C. Zhang, Y. Yan, X. Zhou, Z. Tian and J. Zhang, "A Semi-centralized Trust Management Model Based on Blockchain for Data Exchange in IoT System," in IEEE Transactions on Services Computing

- [8] S. Asiri and A. Miri, "A Sybil Resistant IoT Trust Model Using Blockchains," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1017-1026
- [9] K. M. Sadique, R. Rahmani and P. Johannesson, "Trust in Internet of Things: An architecture for the future IoT network," 2018 International Conference on Innovation in Engineering and Technology (ICIET), Dhaka, Bangladesh, 2018, pp. 1-5
- [10] C. V. L. Mendoza and J. H. Kleinschmidt, "Defense for selective attacks in the IoT with a distributed trust management scheme," 2016 IEEE International Symposium on Consumer Electronics (ISCE), Sao Paulo, Brazil, 2016, pp. 53-54
- [11] Z. Lin and L. Dong, "Clarifying Trust in Social Internet of Things," in IEEE Transactions on Knowledge and Data Engineering, vol. 30, no. 2, pp. 234-248, 1 Feb. 2018
- [12] C. Lewis, N. Li and V. Varadharajan, "Targeted Context based Attacks on Trust Management Systems in IoT," 2023 in IEEE Internet of Things Journal
- [13] I. Souissi, N. B. Azzouna and L. B. Said, "A multi-level study of information trust models in WSN-assisted IoT", Computer Networks, vol. 151, pp. 12-30, 14 March 2019
- [14] Y. Liu, C. Zhang, Y. Yan, X. Zhou, Z. Tian and J. Zhang, "A Semi-centralized Trust Management Model Based on Blockchain for Data Exchange in IoT System," in IEEE Transactions on Services Computing, vol. 24, no. 3, pp. 782-794, 2022
- [15] N. Li, V. Varadharajan and S. Nepal, "Context-Aware Trust Management System for IoT Applications with Multiple Domains," 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 2019, pp. 1138-1148
- [16] A. A. Adewuyi, H. Cheng, Q. Shi, J. Cao, Á. MacDermott and X. Wang, "CTRUST: A Dynamic Trust Model for Collaborative Applications in the Internet of Things," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5432-5445, June 2019
- [17] A. Kavitha et al., "Security in IoT Mesh Networks Based on Trust Similarity," in IEEE Access, vol. 10, pp. 121712-121724, 2022
- [18] B. Shala, U. Trick, A. Lehmann, B. Ghita and S. Shiaele, "Blockchain and Trust for Secure, End-User-Based and Decentralized IoT Service Provision," in IEEE Access, vol. 8, pp. 119961-119979, 2020
- [19] W. Ma, X. Wang, M. Hu and Q. Zhou, "Machine Learning Empowered Trust Evaluation Method for IoT Devices," in IEEE Access, vol. 9, pp. 65066-65077, 2021
- [20] N. Javaid, "A Secure and Efficient Trust Model for Wireless Sensor IoTs Using Blockchain," in IEEE Access, vol. 10, pp. 4568-4579, 2022
- [21] E. M. Abou-Nassar, A. M. Ilyasu, P. M. El-Kafrawy, O. -Y. Song, A. K. Bashir and A. A. A. El-Latif, "DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems," in IEEE Access, vol. 8, pp. 111223-111238, 2020
- [22] G. Joshi and V. Sharma, "Light-Weight Hidden Markov Trust Evaluation Model for IoT network," 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2021, pp. 142-149
- [23] M. Ebrahimi, M. S. Haghighi, A. Jolfaei, N. Shamaeian and M. H. Tadayon, "A Secure and Decentralized Trust Management Scheme for Smart Health Systems," in IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 5, pp. 1961-1968, May 2022
- [24] F. Li, G. White and S. Clarke, "A Trust Model for SLA Negotiation Candidates Selection in a Dynamic IoT Environment," in IEEE Transactions on Services Computing, vol. 15, no. 5, pp. 2565-2578, 1 Sept.-Oct. 2022