International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Recent Trust Management Models for Secure IoT Ecosystem

Kajol Rana[1], Dr.Ajay Vikram Singh[2], Dr. P.Vijaya[3]

Submitted: 06/06/2022 **Accepted:** 10/09/2022

Abstract: The emotional component of trust is crucial in the rapidly evolving world of computers. With a focus on distributed Trust Management systems, a variety of Trust Management frameworks and models have recently been developed for the Internet of Things (IoT). IoT systems may offer considerable advantages across a wide range of application sectors. These fields span everything from smart grid technology to home automation, environmental monitoring, and healthcare. However, there are numerous security concerns with the IoT, including challenges with trust management, key management, identification, and availability. The Internet of Things offers a realistic solution for threat management called "security by trust" (IoT). For symbiotic applications on the IoT stage, there is currently no clear-cut trust management framework. A framework's nodes' dependability should be evaluated in order to estimate the trust using the proper bounds. The parametrization of trust is not explicitly spelled out in existing models. Likewise, most existing models do not adequately depict trust erosion. Furthermore, trust recommendations are frequently given incorrect weights based on past trust, which increases the impact of poor recommendations. In this review paper, we'll cover about various trust models and how they affect Internet of Things security.

Keywords**:** *Iot, Security framework, Trust Management, Classification of Models.*

1. Introduction

IoT is a phenomenon that all physical objects are linked to the Internet, 3G, or WIFI networks and interact in real time. The IoT concept can be implemented with a wide range of wireless technologies, including RFID tags, sensors, actuators, and mobile phones. Computing & communication systems are smoothly integrated in these technologies[1]. IoT offers a variety of new, advanced, and intelligent applications and services for human life, including healthcare, home automation, smart grid, automated mobility, environmental monitoring, as well as smart cities. Nonetheless, the diversity and dynamism of IoT applications, along with the paucity of available resources, provide a substantial security risk that must be addressed [2].

Therefore, it is unlikely that IoT applications will acquire widespread adoption until they have robust security foundations that avoid the emergence of dangerous models, or at least reduce their impact [3]. The Internet of Things (IoT) is a network of "things" that can connect to and share data with other internet-connected devices and systems. These "things" are equipped with sensors, software, and other technologies. They range from commonplace objects to state-of-the-art industrial machinery. There are five criteria that are crucial to the operation of every IoT device:

Presence: IoT devices, like vehicles, exist in the real world, but their presence is only possible thanks to factors that are readily apparent, such the connection component.

Feeling: Every IoT device has a personality, whether that personality is overt or subtle. For instance, a car has a licence plate number. Articles can deal with both data and a specific option.

Connectivity: The two objects may be able to access the assistance or data as a result of an IoT object's ability to connect with another object.

Interaction: An IoT item can communicate with various entities, including people, machines, and tangible objects. A vast variety of management can be created and consumed by two persons.

Dynamicity: IoT devices are capable of interacting at any time, anywhere, and in any position. They are not restricted to a remote area and are free to enter and exit the neighbourhood anytime they need to. [17].

[1] *Research Scholar, PhD*
Amity University, Noida, India
kajolrana27@gmail.com
[2] *Professor*
Amity University, Noida, India
avsingh1@amity.edu
[3] *HOD – CSE*
Waljat College of Applied Sciences, Oman
vijaya@waljat.net

Experts predict that by 2025, 30.10 billion IoT gadget will be linked to the network due to advancements in the sector and the vast number of uses it has. Therefore, IoT security advances are urgently needed. [18]

IoT application performance is significantly impacted by IoT security. When an IoT object requires to interconnect with other objects for data and information security reasons, assurance that the object is trustworthy is needed [19]. Trust management offers study of organisational behaviour based on both recent and historical behaviour. Concerns like identity management, improved user privacy, & data security can be resolved with the usage of trusted management. On the IoT platform, a number of proposed trust management systems are currently available. Many analysts really run into difficulties when attempting to assess the trust values of the nodes inside an IoT system, including the following:

- To retain a suitable level of trust, and secure data flow between IoT components,
- IoT technology related to data integrity issue
- setting up free from any and all harm correspondence with various part at the edge organization
- How to conserve energy using dependable intelligent devices and infrastructure [20].

Developers and researchers suggest many trust models as a solution to these issues, including

- ✓ Dependable gateway system
- ✓ Providing IoT Trust for Energy Efficient Homes and Smart Homes
- ✓ Evaluation of Military IoT Networks, Information Quality as an Indicator of Trust in the IoT
- ✓ Two-way Trust Recommendation in the AI Enabled IoT Systems,
- ✓ Automated
- ✓ Trust Computation in IoT

1.1 Problems in IoT

There are numerous unresolved problems as well as difficulties in the IoT internet world because there are so many connected devices. The first difficulty is standardising all the technologies utilised in IoT platforms in order to provide a unified approach [21].

- **Active and Passive Attacks:** These assaults have the ability to retrieve important data while interfering with network communication. IoT systems are vulnerable to threats from both internal and external system elements.
- A network's inability to access resources at that moment causes a delay in the provision of services.
- Devices with outdated hardware and software are far more vulnerable to attacks and are not updated.
- IoT does not have any preventative mechanisms to safeguard user data privacy.
- The use of traditional encryption techniques and key management does not protect data.
- An effective traffic management approach is required since the task of transferring packets over the network is shared by multiple devices. To prevent any loss or collision, traffic analysis aids in the establishment of unique rules for data transmission and reception.
- Data mining is a different problem. It enables other users to see the sensitive info.
- Management of authentication and identification. Identity management must provide an effective method for preventing devices from replicating their identities.
- Trust management and integration policies present another difficulty. There is no objective agreement in trust management. In this network, granting access control to the proper resources is a significant problem [7].
- The system cannot be protected from malicious attacks by a single networking protocol. The network protocol seeks to fully satisfy the user's expectations, so its fresh invention is not a simple one. The proper topology selection is another another problem [8].
- There should be a way to facilitate flawless interoperability operations between the systems. Because of the large number of linked devices' varied features and file formats, which creates data overhead.
- Scalability is the ability for a system to expand its feature set in response to a changing environment. The major problem is that as external conditions change, humans are unable to adapt a system [8].
- **Preservation:** The system can be easily hacked by others.
- Another obstacle to internet of things trust is infrastructure. The overwhelming quantity of gadgets makes it more challenging for one system to locate and communicate with another system.

According to Yan et al. [22], trust, security, and protection are significant challenges that are intricately intertwined in the developing field of data innovation known as the Internet of Things. In this section, we'll go over the meaning of trust as well as a trademark that several scientists recently used. The alternative definition comes from [23], which describes trust as a degree of faith in certain things based on preexisting beliefs. This degree of confidence can be applied as a notion for making decisions while establishing trust for IoT devices.

1.1 Trust Properties

A holistic trust model's capacity to achieve improved trust accuracy depends on the selection of the right trust attributes. The trust properties are categorised below in order to illustrate the trust relationship between various participating individuals and entities [11].

Objective Properties: The values of these qualities can be assessed and tracked as part of the computational trust. Similar to how requester nodes' reputation, predictability, ability, and strength are measuring units, provider nodes' policies, criteria, and security groups can be quantified [12].

Subjective Properties: The values of these attributes are not evaluable but can be tracked as part of social trust. Non-measuring units include the provider nodes' willingness, belief, and security reliance, as well as the requester nodes' kindness, benevolence, and honesty.

Context Properties: The trust relationship between the grantor and the trustee is contingent on the context-specific criteria. Depending on the circumstances, the findings of a trust evaluation will vary. This property is directly associated with the results of the trust for the grantor and trustee.

2. Literature Review

Several distributions are introduced to cover a variety of IoT-dependent subjects. Sicari et al. [24] introduced the study challenge and available programmes in the IoT security sector, which includes eight classes: authentication, segregation, access control, protection, trust, strategic requirement, middleware, and varied security.

They presented the available information and proposed a path for future exploration. Guo et al. advocate the compilation of a trust framework based on the following five categories: a.) trust integration, b) Trust building, c) Trust value, d) Trust development, & e.) Trust review. In fact, they cover the research gaps and issues in every discipline [25].

After reviewing the most recent publications, Ammar et al. [26] hypothesised that the existing IoT framework is fragmented. Current research initiatives are categorized based on element structure, programming language, hardware and software dependencies, hardware compatibility, authorized communication protocol, and security characteristics.

Ruan and Durresi [33] proposed a social IoT system to assess the value of trust. to create an IoT trust paradigm that could withstand difficulties and hostile attacks. The social IoT paradigm communicates only trustworthy relationships and concentrates on each node inside an IoT network. This may promote trust between two dissimilar nodes. After that, only a reliable authority will be able to access data and communications. The architecture of trust management is influenced by various security concerns in various requirements. This approach focuses mostly on separating the trust. Systems can simplify the use of the authentication procedures for devices to join the network through identity management.

Mendoza & Kleinschmidt [34] conducted IoT, or the internet of things Even though it can be difficult to build trust between devices, distributed trust management focuses on how devices act directly and indirectly. Instead than using a central node to determine trust for other nodes, each node uses this approach to assess the behaviour of its nearby nodes. Based on comparing trust values with the threshold, it demonstrates how to defend against various harmful assaults on a single device. During the first phase of distributed trust management, nodes begin communicating with one another and with all other nodes. This will reveal how many neighbour nodes there are. The node will now ask the neighbours for service after discovering the neighbour list. The first trust value will be determined based on direct interactions, and a trust table with adjacent nodes' trust values will be prepared. Later, neighbouring nodes will share this table. By combining the initial trust value and neighbour recommendations, the actual trust value will then be updated.

Saied et al. [35] suggested a multi-service, context-sensitive design for an IoT trust management system. In this system, a novel approach is put forth whereby the majority of IoT networks are interconnected with various devices, but the reliability is based solely on a single function. A novel technique to create a multiservice for various functions is provided by the TMS in this scenario where several devices are connected in an IoT but we are unable to acquire trustworthiness from the devices. The aforementioned work is carried out by grouping and combining the individual functions. The suggested trust management system demonstrates how several devices might work together to perform a particular task. The techniques in the new approach are recommended for the nodes interacting with other nodes to receive services in order to obtain trustworthiness from the nodes that are now available. Information is first gathered from several nodes in order to determine the requirements. Before receiving a trust value from other systems, systems in a trusted environment are working together. The node may determine the behaviour of other nodes and determine whether they act inappropriately or engage in any attacks focused on the +ve & -ve values. Despite fact that the systems are spread across many locations, only one message was transmitted, and the network was being monitored locally. While the client node receives service from its aiding nodes, the evaluation of the process reviews the transaction, which might be good or negative. With the aid of a context-aware idea, many devices are able to deliver multiple services with confidence.

Wosowei J. et.al. [21] examined IoT, social networking, and the social networks of networked smart devices were combined to create the Social Internet of Things. This occurrence has enhanced both perspectives and given rise to new environment. The Human to Thing and Thing To Thing interconnection model of the IoT are expanded upon by the SIoT. The Internet of Things has made it possible to create "social devices" with social intelligence (IoT). Such social objects (SOs) can locate and communicate with other SOs nearby thanks to their social features. They search social networks for relevant content to find beneficial services and information. Prior to this study, little research has been conducted on the concept of trust & trustworthiness in the IoT. Let's start by reviewing the fundamentals of SIoT and comparing it to the IoT in refers of trust. Second, we classify & evaluate every SIoT trust management solution that has been discussed in the literature over the last six years. Comparative analysis is used, we investigate the most recent cutting-edge SIoT trust management strategies.

Pourghebleh et.al [15] investigated The majority of previous research used both direct & indirect trust to gather the data for the aggregate component. In contrast to direct trust, indirect trust may result in a number of issues, including inaccurate suggestions, a need for a large computing power and a lengthy process to assign trust values. Additionally, because most research has focused on static elements for aggregation, it's possible that this is incompatible with the dynamic of the Internet of Things. The studies focused on the dynamics of the aggregation process as well as manually distributing weights, as is the case in fuzzy logic, which is fully reliant on human experience and talent, in order to develop machine learning tactics that may improve aggregation processes. In order to increase data accuracy and efficiency, dynamic aggregation with dynamic weight assignment is used.

3. Trust Management in Iot

In practical applications, the security of IoT networks is crucial. In reality, there has been a lot of research done on security issues in the communications & networking area. Since trust may be included into communication and network protocol designs, trust management is given considerable consideration. Additionally, the improvement of trust relationships, which control the availability, reliability, as well as secure operation of the network, depends on the cooperation and collaboration of participating nodes.

Actually, a variety of computer, communication, & information systems sectors have tackled trust management challenges, like as social networking, WSNs, and more recently, the IoT. The majority of research considers IoT items to be little more than wireless sensors. As a result, this is a summary of many trust management strategies applied in WSNs.

There are two types of trust methods (TMs) for WSNs: OTM & CBTM. The two divisions of OTMs [38]. The models are categorised as centralised or distributed in the first subcategory, which is called Node TMs. In centralised arrangements, a single base station calculates the trust values of each node. These versions, meanwhile, consume a lot of energy and aren't suitable for the majority of WSNs. In distributed models, the nodes independently determine the trust levels. The latter, however, have a high memory and compute complexity. The data TMs make up the second subgroup. These models use data discrepancies or improper data processing to determine a node's trust value. Data TMs are not used to protect data, though. a group-based TM for the CTMs which blends decentralized and centralized computation and gives a set of nodes a single trust value [39]. This strategy guards against selfish and malevolent nodes. This is not, yet, protected against TMs attacks and is based on an irrational assumption. a hybrid TM that uses monitoring to keep tabs on how the various nodes behave and spot erroneous information coming from faulty and compromised nodes. The cluster head in this model is a weakness because it is open to malicious attacks.

A hierarchical framework for managing trust focused on both social and QoS trust traits, like as intimacy and honesty. These multiple measures used formation, reputation (aggregation), & updating models to evaluate a node's trustworthiness [40]. The protocol makes use of both direct observations based on nodes' knowledge and indirect suggestions from network nodes in order to update trust values. This approach manages a big number of heterogeneous sensor nodes using a clustering methodology. For robustness and intrusion tolerance, it also manages selfish and evil sensor nodes. However, the energy is a parameter that is needed to build the different metrics employed in this protocol. A normal node will use more energy and may even lose its trustworthiness if it is surrounded by selfish nodes. Moreover, because a protocol employs indirect suggestions, it is susceptible to good and negative mouthing attacks.

IoT Trust Management study according to IoT architectural levels. There are in fact a variety of IoT architectural proposal possibilities available. The three-layer design with a sensor layer, network (core) layer, as well as application layer is the most prevalent[41]. RFID, sensors, as well as actuators are examples of the physical components that make up the sensor layer. The IoT market's most widely used standard for this tier is IEEE 802.15.4. This standard lays the groundwork for the development of IoT communication. It specifies a Physical Layer (PHY) and a Medium Access Control (MAC) sublayer for low-rate wireless local area networks (LR-WPAN). This layer takes data and information, processes it, and then transmits it wirelessly to a base station. The network layer acts as a connecting layer between the sensor layer and the application layer by using wired & wireless communication networks including WiFi, ZigBee, LTE, and GPRS. This layer contains data handling and transmission methods such as IPv6 Over Low-Power Wireless Area Networks and Routing Protocol for Low-Power and Lossy Networks.

The sensor as well as network layers are hosted on constrained Internet of Things devices with limited power. In order to offer end users the services they want, the application layer combines and analyzes data obtained from the network layer. Strong hardware is required for this layer because to its extensive and complex computing needs. Fundamental technologies like the Constrained Application Protocol are handled at this layer.

The three IoT tiers are vulnerable to a variety of unique threats and assaults.Since developing a trust mechanism for the entire IoT is difficult, trust mechanisms can be developed for each of the three aforementioned IoT layers. According to each layer's specific function, this system provides self-organizing sensors for the sensor layer, effective and secure routing of data packets & control messages for the network layer, and multi-services for the application layer, as illustrated in Figure 1.

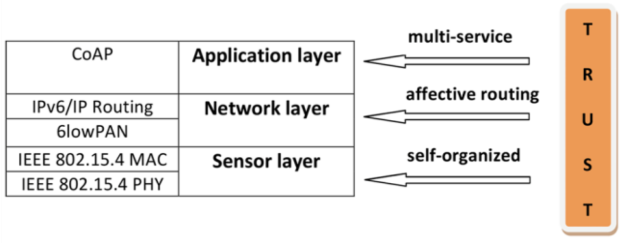

Figure 1- Layered Trust for IoT

Different research projects have been carried out to categorize IoT trust management models. Trust models are categorized using the objective & subjective traits of the trust & beneficiaries [42]. The authors contend that a range of IoT systems should widely adopt trust management. Additionally, by combining decision and analysis models with different security considerations, trust should be assured across all IoT layers vertically. Accordingly, the global model should include the evaluation of entity trust at all stages, system and entity durability as well as availability, privacy & key management, trust routing, including QIoTS.

According to authors, trust is a multifaceted concept with multiple context-specific meanings [43]. They divided trust models into 4 approaches: social networking approaches, fuzzy method approaches, cooperative approach approaches, and identity-based method approaches.

4. Trust Frameworks

IoT progress is hampered by security concerns. Before the security breach, decisions may have improved the performance of IoT apps. We will concentrate more on redesigning IoT security mechanisms in this section.

- **Trustworthy Gateway System for Smart Home IoT Trust Domain**

The development of a gateway framework that establishes a secure IoT environment and protects IoT from dangerous threats. Additionally, a trustworthy corridor framework can protect IoT without making changes to IP-based devices by converting the IP addresses of the home appliances and the appliance control server into recognizable identifiers (Identities) that can be used to pass through an untrusted online organization. Because it can be used to smart home assistants, smart offices, and smart automobiles utilizing an IoT trust method concept called trust space, it can establish a new trust network administration biological system and a new trust network plan of operation environment.

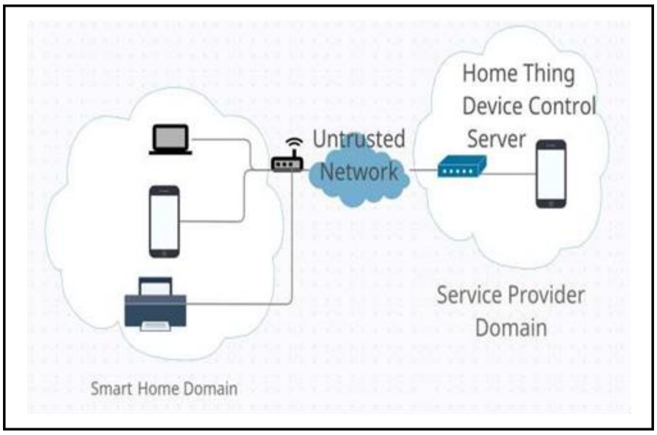

Figure 2-Trustworthy gateway system

- **Efficiency of Trust Assessment in Military IoT Networks**

Cost- and energy-efficient security should be given in IoT military organisations. This research provides a suggested, step-by-step evaluation technique that gradually implements a process of trustworthiness by questioning and restricting trust testing. The purpose of imitation is to demonstrate that the proposed scheme offers the same level of security yet consuming significantly less energy than the existing scheme.

Using trust values, secure communication channels are constructed in a trust-based method. The literary activity discussed the calculation of trust's value. Existing programs are categorized as distributed or centralized based on whether individual values are evaluated by network nodes or by the central BS [37].

In the suggested part, methods for directing the tree structure are implemented. Each hub only considers the conduct of other hubs' children. When the hub is analysing the suspicious behaviour of its children's hubs, it begins by requesting that its parents' hub determine whether the suspect hub has been included in the boycott. If the suspicious hub is not located in the rundown, the question is referred to the highest-level parent hub, which is renamed until the investigation begins with the root hub. The root hub or hub that examines the suspect hub in the rundown generates a response and transmits it to the hub where the comparison inquiry is presented initially. The response signals that the suspicious hub is now marked as vulnerable, or that a neighbourly trust cycle should commence.

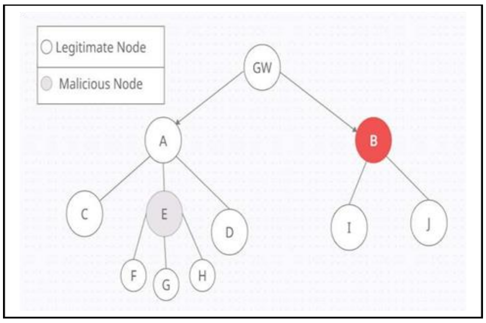

Figure 3. Energy Efficient Trust

- **Information Quality as a Trust Indicator for Internet of Things**

  Introduces a framework that employs a trust-based framework that complies with actual QoI DQ criteria and demonstrates how QoI testing and Trust testing are executed in a highly assured IoT environment.

  A trust monitoring system that examines the relationship between users and service providers' trust can use this dimension to offer concrete statistics based on specific information, or reference ontology. Regarding DQ concerns in a particular usage context, we consider QoI to refer to a specific degree of data that matches or complements the type of usage. The focus of this study is the creation and evaluation of the QoI module. To classify QoI rules, we essentially followed the definition of QoI in [13, 14, 15]. Then, it offers ways to incorporate these ideals into a school. To analyse the reliability of IoT services and applications, the suggested Reputation-Experience-Information (REK) model of dependability is used to evaluate the results utilising these points as an important dependable indication [16, 12].

  The decision to approve the construction is being looked into. The job is examined and approved using a system called self-versatile recommender (SAR), which has been created and installed at the testbeds for the Wise-IoT project. The SAR design offers the flexibility needed to schedule experiments and gather the information streams needed to analyze the system's results.

In terms of the examination of work, the paper suggests a few directions for future research, such as the use of QoI evaluation and trust in a range of IoT administrations and the development of a model for measuring trust that takes into account other relevant data besides QoI.

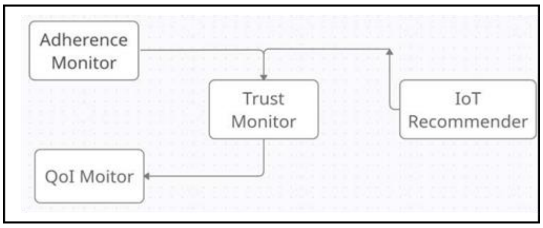

Figure 4. Quality of Information as indicator of Trust

- **Subjective Logic and Multiple Attributes for Automated Trust Computation in the IoT**

  To computerised trust calculation mechanism for IoT is presented. It provides a method for determining the trustworthiness of nodes focused on EBSL & MADM. Approach takes into account trust assessment weaknesses by combining FT & RT components into a trust organization. The structure's mechanism for measuring trust scores and translating them into feelings for use in a TN is a noteworthy contribution. Using the MADM methodology, the trust ratings can represent different context-based and specialised factors that influence both FT and RT. It approves the suggested trust evaluation instrument that employs testing using authentic data. The outcomes show that the trust system can distinguish between compromised and faulty hubs by accurately capturing the conduct and boundaries of hubs. It is also apparent that hubs' trust would be affected by their organisational neighbours. We emphasize that the MADM attributes we can think of are planning possibilities that can change based on the framework or application. As a result, one new area of future research could be the examination of additional features in MADM describing for trust calculation in application-specific IoT organizations. However, because it takes into account different trait types, our suggested solution can be seen as a rule-based model.

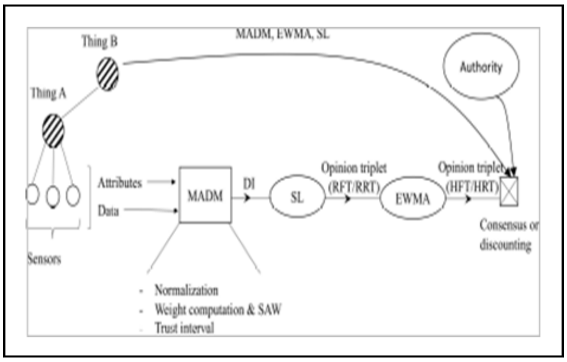

Figure 5 Automated trust computation

- **An IoT Trust Management model**

  It refers to the Internet of Objects (IoT) growth, which is a strategy for actual gadgets, home appliances, and other things to be outfitted with hardware, software, sensors, actuators, & availability, allowing them to cooperate and exchange data. We also discussed security protection, the potential for IoT attacks, and the trust the chiefs concept.

There isn't a single, universal IoT design that researchers and people throughout the world agree upon. Numerous architectural designs have been developed by scholars. Some scholars assert that the IoT architecture consists of three layers, while others suggest for a four-layer design. IoT innovations hinder the three-layer architecture from achieving application requirements.

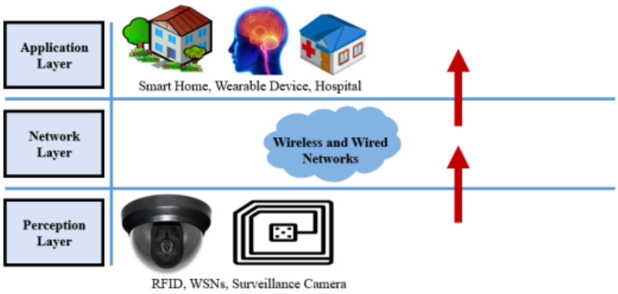
Application Layer
Smart Home, Wearable Device, Hospital
Network Layer
Wireless and Wired Networks
Perception Layer
RFID, WSNs, Surveillance Camera

Figure 6. The IoT's three-layer design.

✓ **Perception Layer:** It is frequently called the sensor layer. It functions like the human eyes, hearing, and nose. It is responsible for identifying objects and extracting information from them. There are numerous types of information-collecting sensors attached to items, including RFID, 2-D barcode, and sensors. The sensors are selected based on the needs of the applications. The data collected by these sensors may pertain to location, air quality, the surroundings, motion, vibration, etc. However, they are the primary target of attackers seeking to replace the sensor with their own. Consequently, the bulk of risks involve sensors [35–37]. The following are typical perception layer security threats:

- ✧ Eaves - dropping
- ✧ Node - Capture
- ✧ Fake Node & Malicious
- ✧ Replay - Attack
- ✧ Timing - Attack

✓ **Application Layer:** A application layer explains all apps which utilise IoT technology or have been deployed using IoT. Examples of IoT applications include smart homes, smart cities, smart health, and animal tracking. It is accountable for providing services to the applications. Depending on the information collected by sensors, the services provided for each application may differ. The application layer has many difficulties, with security being the main issue. IoT provides several internal and external hazards as well as vulnerabilities, especially when used to build a smart home. The devices used in smart homes, like ZigBee, have limited processing capacity and storage, which is one of the main challenges to establishing robust security in an IoT-based smart home. The following are typical application layer security issues and worries:

- ◆ Cross Site Scripting
- ◆ Malicious Code Attack
- ◆ The capacity to manage Mass Data

✓ **Network Layer:** The transmission layer is also known as the network layer. It serves as a link between the perception layer and the application layer. It moves and sends information collected by sensors from actual items. It is possible to employ a wired or wireless transmission method. Additionally, it is in charge of connecting networks, network devices, and intelligent objects. It is therefore particularly vulnerable to attack from the enemy's perspective. It creates significant security concerns regarding the authenticity as well as integrity of information being transmitted along the network. Common network layer security issues and challenges include the following:

- ❖ DoS - Attack
- ❖ MiTM - Attack
- ❖ Storage - Attack
- ❖ Exploit - Attack

A survey obtained a selection of open systems and platforms for developing IoT applications based on current technology. To lead everything to cover the IoT model in an organisation, trust qualities that effect vision have been examined, and the TMM should encompass all social events related with the IoT model in diverse contexts. The elements that offer intelligent IoT applications based on trust in the board model are also combined in a new TMM structure that is proposed. The components inside the layers, particularly the cross-layer, are additionally consolidated by this structure.

5. Evaluation and Classification of Previous Trust Models

Trust assessment model inside IoT is now in its infancy, with few conclusive works in circulation, likely due to limited IoT stage and experimentation experiences. Table 1 details the stream flow and research involved in the trust calculation model.

For information and data security concerns, when an IoT device must connect with other objects, it must be guaranteed that the object is trusted [39].

Numerous analysts still face different difficulties on the subject of IoT research, including

- ➢ guaranteeing a sufficient degree of secure information trade and trust between IoT part
- ➢ IoT advancements identified with information secrecy concern
- ➢ setting up free from any and all harm correspondence with various part at the edge organization,
- ➢ how to save energy utilizing dependable shrewd gadget and framework [39].

In Table 1, several security structures are analysed so that a superior organisation of the systems and their content may be established. It is clear that each structure serves a different purpose. Specific attacks such as intrusion identification and defence are addressed in nearly every system depicted.

Table 1: Comparison of Trust Management Methods

Security Framework	**Attributes**	**Facilities/Drawbacks**
Dependable system offering IoT Smart home trust sphere	● Gateway Framework ● IP to ID	Prevents malicious activities
Energy Efficient Trust Evaluation In Millitary IoT Networks	● Local Trust Evaluation Process ● Routing Path method	● Low Power Consumption ● Collaborative Observation
Information Quality as a Measure of IoT Trust	● Reputation ● Experiencing ● Knowledge ● Self adaptive recommender ● Middle ware	● Hard to deploy practically ● Under Supervision
Subjective Logic and Multiple Attributes for Automated Trust Computation in the Internet of Things	● EBSL ● MADM	● Direct and Indirect Trust Computation
An IoT Trust Management model	● Cross-layers ● Middlewarre ● AMI	● Multi Platform ● Flexible

6. Iot Trust Management Principle and Terminology

Introduces the fundamental components of developing a model for trust management. These modules are used to evaluate and analyze entity characteristics such as honesty, integrity, and dependability in order to determine the value of trust [25]. The five elements are shown in Figure 7, and are discussed in the sections which are follow.

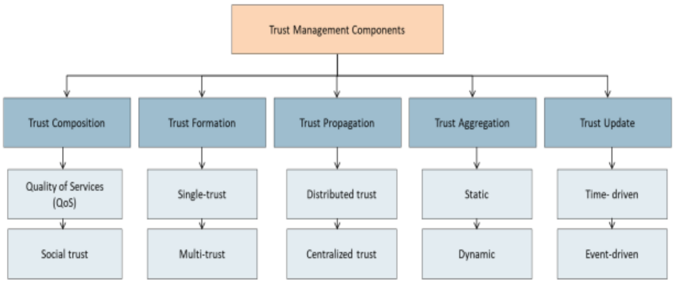

Figure 7. Trust Management model components.

1. **Trust Composition:** It consists of two basic modules: QoS trust & social trust [25]. This refers to the factors considered during trust computation.
   - ● QoS is the idea which an IoT entity will provide higher-quality functionality. To evaluate the value of trust, QoS trust incorporates a variety of trust criteria, including competence, dependability, job completion ability, and cooperation [26].
   - ● Social trust is the social relationship between the owners of Internet of Things (IoT) assets. Social relationship trust is used to evaluate the trustworthiness of an Internet of Things entity. In fact, social trust quantifies trust values using trust attributes like honesty, centrality, closeness, privacy, and connection[26].
2. **Trust Formation:** This indicate to whether trust computation is predicated on a single property (singletrust) or numerous qualities (multitrust). Moreover, these elements are primarily disturbed with how QoS and social trust traits are weighted [6].
3. **Trust Propagation:** The technique of communicating trustworthiness to other entities is known as trust propagation. This sort of transmission distinguishes two primary strategies [25]:
   - ● Distributed relates to Internet of Things (IoT) entities that automatically communicate trust and observations to other IoT units with which they interact or come into contact [25].
   - ● The presence of centralised entities is required for centralised trust. It can be implemented by IoT devices as a physical cloud or as a virtual trust service.
4. **Trust Aggregation:** This is the most effective way to gather trust data, which is subsequently assessed either directly by the entity (direct assessment) or indirectly by other entities (indirect evaluation) [33]. Information is combined by this component using either static or dynamic weights. Based on the properties of the entity, the static is calculated. Based on each communication party's unique trust qualities, the initial trust is established between them. Trust

management must give weights to every property based on context information in order to make suitable dynamic trust judgments [34]. In the literature, many models of trust aggregation are discussed, including regression analysis, fuzzy logic, belief theory, and Bayesian inference.

5. **Trust Update:** This element specifies when the values of trust should be updated. The trust information is periodically (time-driven) updated by utilizing a trust aggregate or after a QoS-affecting transaction or event (event-driven).

Conclusion

After comparing the operation of the aforementioned security frameworks, it is likely that Trust-based strategies are providing increasingly capable and secure components for IoT. As an outcome, it has been observed that cryptographic systems are most commonly employed to ensure a minimum level of security. When contemplating the IoT and billions of devices, security requirements must go beyond confirmation, confirmation, convention, and standard threats. We may conclude from the aforementioned research that there is a need for enhanced security measures that can provide shared security or device-to-device security, so that the entire IoT can be configured to prevent assaults such as on-off, CandyJar, Mirai Botnet, and Slandering. The Internet of Things (IoT) is a unique concept that intends to enhance quality of life through the networking of intelligent objects, technologies, and applications. It is fast gaining prominence in contemporary culture. In principle, the IoT would permit the automation of our immediate surroundings. This paper summarized the fundamental idea and uses of this approach. We have highlighted numerous studies pertaining to the Internet of Things' layered architectures and suggested security attacks based on the IoT's layers that can damage its performance.

As an outcome, it is reasonable to conclude that, when calculating trust, one cannot rely solely on a single technique; rather, one must consider all aspects that may affect the value of trust in a certain manner, such as quality of service, reputation, honesty, information entropy, feedback, etc. Additionally, a method for energy conservation is required, as IoT devices are battery-powered and cannot consume the necessary energy to function at peak efficiency.

References

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

[2]. Shafique, K.; Khawaja, B.A.; Sabir, F.; Qazi, S.; Mustaqim, M. Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios. IEEE Access 2020, 8, 23022–23040.

[3]. C. Sobin, “A survey on architecture, protocols and challenges in IoT,” Wireless Pers. Commun., vol. 112, pp. 1383–1429, Jan. 2020

[4]. Sharma, A., Pilli, E. S., Mazumdar, A. P., & Gera, P. (2020). Towards trustworthy Internet of Things: A survey on Trust Management applications and schemes. Computer Communications, 160, 475-493.

[5]. N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, D. I. Kim, and Z. Han. Data collection and wireless communication in internet of things (IoT) using economic analysis and pricing models: A survey. IEEE Communications Surveys Tutorials, 18(4):2546– 2590, Fourth quarter 2019. ISSN 1553-877X. doi: 10.1109/COMST.2016.2582841

[6]. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. IEEE Access 2019, 7, 82721–82743.

[7]. Ahmed, A.I.A.; Ab Hamid, S.H.; Gani, A.; Khan, S.; Khan, M.K. Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open research challenges. J. Netw. Comput. Appl. 2019, 145, 102409

[8]. Jayasinghe, U.; Lee, G.M.; Um, T.-W.; Shi, Q. Machine Learning Based Trust Computational Model for IoT Services. IEEE Trans. Sustain. Comput. 2019, 4, 39–52.

[9]. Chen, I. R., Guo, J., & Bao, F. (2019). 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

[10]. Kim, B.-S., Hassan, S., & Khan, M. K. (2018). Trust management techniques for the Social Internet of Things: A survey. IEEE Access, 7, 29763-29787. https://doi.org/10.1109/ACCESS.2018.2880838

[11]. M. Frustaci, P. Pace, G. Aloi, and G. Fortino. Evaluating critical security issues of the IoT world: Present and future challenges. IEEE Internet of Things Journal, 5(4):2483–2495, Aug 2018. ISSN 2327-4662. Doi: 10.1109/JIOT.2017.2767291.

[12]. Djedjig, N.; Tandjaoui, D.; Romdhani, I.; Medjek, F. Trust management in the internet of things. In Security and Privacy in Smart Sensor Networks; IGI Global: Hershey, PA, USA, 2018; pp. 122–146.

[13]. V. Gazis. A survey of standards for machine-to-machine and the internet of things. IEEE Communications Surveys Tutorials, 19(1):482–511, first quarter 2017. ISSN 1553-877X. Doi: 10.1109/COMST.2016.2592948.

[14]. U. Raza, P. Kulkarni, and M. Sooriyabandara. Low power wide area networks: An overview. IEEE Communications Surveys Tutorials, 19(2):855–873, second quarter 2017. ISSN 1553-877X. Doi: 10.1109/COMST.990 2017.2652320.

[15]. Pourghebleh, B.; Navimipour, N.J. Data aggregation mechanisms in the Internet of things: A systematic review of the literature and recommendations for

future research. J. Netw. Comput. Appl. 2017, 97, 23–34

[16]. A. Arabsorkhi, M. Sayad Haghighi, and R. Ghorbanloo. A conceptual trust model for the internet of things interactions. In 2016 8th International Symposium on Telecommunications (IST), pages 89–93, Sept 2016.doi: 10.1109/ISTEL.2016.7881789.

[17]. Goar, . V. K. ., and N. S. . Yadav. "Business Decision Making by Big Data Analytics". International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 5, May 2022, pp. 22-35, doi:10.17762/ijritcc.v10i5.5550.

[18]. Roman, R., P. Najera, and J. Lopez. (2011) "Securing the Internet of Things," Computer (Long. Beach. Calif) 44 (9): 51–58.

[19]. https://www.statista.com/statistics/1101442/iot-number-of- connected-devices-worldwide/#:~:text=The%20total%20installed%20base%20o f,that%20are%20expected%20in%202021.

[20]. Chen, I. R., J. Guo, and F. Bao. (2016) "Trust Management for SOA-Based IoT and Its Application to Service Composition." IEEE Trans. Serv. Comput. 9 (3): 482–495.

[21]. Albishi, S., B. Soh, A. Ullah, and F. Algarni. (2017) "Challenges and Solutions for Applications and Technologies in the Internet of Things." Procedia Comput. Sci. 124: 608– 614.

[22]. Yan, Z., P. Zhang, and A. V. Vasilakos. (2014) "A Survey on Trust Management for Internet of Things." J. Netw. Comput. Appl. 42: 120– 134.

[23]. Jiang, J., G. Han, F. Wang, L. Shu, and M. Guizani (2015) "An Efficient Distributed Trust Model for Wireless Sensor Networks." IEEE Trans. Parallel Distrib. Syst. 26 (5): 1228– 1237.

[24]. Sicari, S., A. Rizzardi, L. A. Grieco, and A. Coen-Porisini. (2015) "Security, Privacy and Trust in Internet of Things: The Road Ahead."

[25]. Guo, J., I. R. Chen, and J. J. P. Tsai. (2017) "A Survey of Trust Computation Models for Service Management in Internet of Things Systems." Comput. Commun. 97: 1–14.

[26]. Ammar, M., G. Russello, and B. Crispo. (2018) "Internet of Things: A survey on the security of IoT frameworks." J. Information Security Appl. 38: 8–27.

[27]. N. Marchang and R. Datta, "Light-weight trust-based routing protocol for mobile ad hoc networks," IET Information security, vol. 6, no. 2, pp. 77–83, 2012.

[28]. A. Tajeddine, A. Kayssi, A. Chehab, I. Elhajj, and W. Itani, "Centera: a centralized trust-based efficient routing protocol with authentication for wireless sensor networks," Sensors, vol. 15, no. 2, pp. 3299–3333, 2015.

[29]. N. Truong, H. Lee, B. Askwith and G. Lee, "Toward a Trust Evaluation Mechanism in the Social Internet of Things," SENSORS, vol. 17, no. 6, 2017

[30]. M. Ge and M. Helfert, "Data and information quality assessment in information manufacturing system," in International Conference on Business Information Systems, 2008.

[31]. N. Askham, D. Cook, M. Doyle, H. Fereday, M. Gibson, U. Landbeck, R. .. Lee, C. Maynard, G. Palmer and J. Schwarzenbach, "The six primary dimensions for data quality assessment," DAMA UK Working Group, United Kingdom, 2013.

[32]. N. Laranjeiro, S. Soydemir and J. Bernardino, "A survey on data quality: classifying poor data," in IEEE 21st Pacific Rim International Symposium on Dependable Computing (PRDC), 2015

[33]. Gupta, D. J. . (2022). A Study on Various Cloud Computing Technologies, Implementation Process, Categories and Application Use in Organisation. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(1), 09–12. https://doi.org/10.17762/ijfrcsce.v8i1.2064

[34]. N. B. Truong, T. Um, B. Zhou and G. M. Lee, "Frompersonal experience to global reputation for trust evaluation in the social internet of things," in IEEE Global Communications Conference (GLOBECOM), Singapore, 2017.

[35]. Chen, I. R., J. Guo, and F. Bao. (2016) "Trust Management for SOA-Based IoT and Its Application to Service Composition." IEEE Trans. Serv. Comput. 9 (3): 482–495.

[36]. Albishi, S., B. Soh, A. Ullah, and F. Algarni. (2017) "Challenges and Solutions for Applications and Technologies in the Internet of Things." Procedia Comput. Sci. 124: 608– 614.

[37]. Kabisha, M. S., Rahim, K. A., Khaliluzzaman, M., & Khan, S. I. (2022). Face and Hand Gesture Recognition Based Person Identification System using Convolutional Neural Network. International Journal of Intelligent Systems and Applications in Engineering, 10(1), 105–115. https://doi.org/10.18201/ijisae.2022.273

[38]. Mendoza, C. V., & Kleinschmidt, J. H. (2015). Mitigating on-off attacks in the internet of things using a distributed trust management scheme. International Journal of Distributed Sensor Networks, 11(11), 859731.

[39]. Saied, Y. B., Olivereau, A., Zeghlache, D., & Laurent, M. (2013). Trust management system design for the Internet of Things: A context-aware and multi-service approach. Computers & Security, 39, 351-365.

[40]. Wosowei, J., & Shastry, C. Novel Research on Challenges and Directions for Trust Management in Social Internet of Things (SIOT).

[41]. Han, G., Jiang, J., Shu, L., Niu, J., & Chao, H. C. (2014). Management and applications of trust in Wireless Sensor Networks: A survey. Journal of Computer and System Sciences, 80(3), 602-617.

[42]. N. A. Libre. (2021). A Discussion Platform for Enhancing Students Interaction in the Online Education. Journal of Online Engineering Education, 12(2), 07–12. Retrieved from http://onlineengineeringeducation.com/index.php/joee/article/view/49

[43]. Shaikh, R. A., Jameel, H., d'Auriol, B. J., Lee, H., Lee, S., & Song, Y. J. (2009). Group-based trust management scheme for clustered wireless sensor

networks.IEEE transactions on parallel and distributed systems, 20(11), 1698-1712

[44]. Bao, F., Chen, R., Chang, M., & Cho, J. H. (2012). Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection.IEEE transactions on network and service management, 9(2), 169-183.

[45]. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

[46]. Yan, Z., Zhang, P., &Vasilakos, A. V. (2014). A survey on trust management for Internet of Things.Journal of network and computer applications, 42, 120-134.

[47]. Sicari, S., Rizzardi, A., Grieco, L. A., &Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146-164.

[48]. Ali, B.; Awad, A.I. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. Sensors 2018, 18, 817