Transport Layer Security Techniques for Internet of Things Device: A Review

Dr. T. V. V. Satyanarayana

Professor, Department of ECE,
Mohan Babu University, Tirupati, Andhra Pradesh, 517102, India.
satya.tvv@gmail.com

Abstract: To safeguard data, guarantee device authenticity and comply with regulatory compliance standards, IoT devices must employ Transport Layer Security (TLS) protocols. It maintains the safety and confidentiality of data exchanged by IoT devices and helps defend the IoT ecosystem against a variety of security risks. In this review paper, basics of IoT structure is mentioned with popular protocols. TCP may be utilised in IoT, depending on the specific requirements of the application. If data security, reliability, and integrity are important with minimal latency, TCP could be a viable choice. The widely used protocols such as REST (Representational State Transfer), DDS (Data Distribution Service), CoAP (Constrained Application Protocol), MQTT (Message Queuing Telemetry Transport), XMPP (Extensible Messaging and Presence Protocol) and HTTP (Hypertext Transfer Protocol) are discussed in detail. To help new researchers, a discussion of several energy-efficient TLS protocols and an explanation of the transport layer's difficulties is offered. The discussion of various prospects and successful future directions will help the researchers in the long term.

Keywords: Transport Layer Security (TLS), Internet of Things (IoT), Data-Local Reconstruction Layer (DLRL), Handshake Optimizations, Object Management Group (OMG), Representational State Transfer (REST).

1. Introduction

Technology today offers significant advantages over security communication difficulties [1]. Over the past ten years, there has been a major increase in computer communication including online purchases and payments in return for goods and services. The TLS protocol is one of the protocols that is frequently used to protect these transactions through authentication and encryption [2]. Encryption is employed in this protocol to stop the monitoring of sensitive data like account passwords and credit card numbers. For various applications, end-to-end secure communication is provided by the cryptographic protocol TLS [3]. It is one of the best popular protocol for connecting a client and a server. The Record Protocol and the Handshake Protocol are the two essential components [4]. The Record Protocol uses the keys established by the Handshake Protocol to encrypt data. The handshake protocol, which is a component of TLS, also permits authentication of the presumptive identity [5] [6]. The Record Protocol provides the maintenance of an encrypted path for the delivery of data. Additionally, the TLS protocol has a unique data framing and authentication mechanism [7].

An encryption mechanism called TLS is used to authenticate the server's identity in a client-server communication and to encrypt client-server interactions [8]. Mutual TLS (mTLS) represents a mutual (two-way) verification technique that verifies that the individuals at either end of a web connection are both in possession of the proper private key [9]. mTLS is a component in zero-trust security models, because it ensures multiple authentications among the client as well as server for servers, devices, users, application programming interfaces (APIs), etc [10]. Certificates are used by mTLS to verify clients and servers. It may also be utilised by applications for the Internet of Things (IoT). Given that the mTLS connection between the user's device and the web server is point-to-point with certificate-based authentication, it is difficult to send a message from the host to several clients [11].

Since mTLS connections among clients and servers are point-to-point with certificate-based authentication, there is no simple way to send a message from a server to several clients [12] [13]. Multicasting is more challenging if endpoints are dispersed globally and have different network rates and bandwidth. In some cases, time-sensitive communications must go through mTLS channels to the operator; as a result, out-of-band communications must use different channels while preserving identical mTLS security control [14] [15].

The IoT is becoming more and more important in every aspect of day-to-day life [16]. It has been employed in a variety of application areas, including smart cities and homes, healthcare and factory automation. Naturally, sensitive data is collected, and it can be transferred across an unreliable network infrastructure, like Internet [17]. Because of this, end-to-end communication security is a crucial requirement for various Internet of Things application scenarios. Standard-based solutions are currently available for IoT security [18]. Among these are the datagram-oriented version of the TLS protocols. The de-facto protocol supporting IoT security of communication

is the Datagram TLS (DTLS) protocol. The most recent TLS version 1.3, offers significant performance improvements and lower message dimensions that can push the security of IoT connectivity even further [19].

Despite the fact that standardised Internet security protocols have significant benefits for deployment and compatibility. Both public-key certificates and symmetric pre-shared keys (PSKs) are supported for authentication by the TLS protocol [20]. PSK-based authentication uses a minimal amount of bandwidth and processing resources. In order to provide security when generating the PSK, there must also be enough entropy, which is typically not guaranteed in practise.

2. Review Objectives

The IoT uses a variety of services, hardware and communication protocols. IoT variety can be seen as a two-edged sword that benefits users but also increases the risk of security risks and assaults. A physical perception layer, a network and protocol layer, an application layer, a transport layer and a data and cloud services layer are all components of the IoT architecture. Transport protocols are demonstrated, and the safety risks they face are explored while offering standard fixes. It includes the absence of widely accepted lightweight encryption techniques, the difficulties associated with using machine learning algorithms to improve security and the usage of blockchain to address security issues in the Internet of Things. However, a comparison of various methods is provided below.

- Various protocol in IoT transport layer and Energy-Efficient Transport Layer Security for the Internet of Things.
- Different techniques are used to secure the transport layer for Internet of Things devices.
- Challenges faced on transport layer security in Internet of Things.
- The most important application of transport layer security solutions.

3. Basics of IoT architecture

TCP/IP protocol is now used by the internet to facilitate communication between network hosts. With the introduction of IoT, that connect many objects with the Internet, traffic over the Internet will significantly increase and there will be an increase in the need for more data storage. Security and privacy difficulties will arise as a result of such a large network. As a result, the proposed IoT design must solve a number of issues, including scalability, dependability and quality of service. Therefore, the design of various prospective apps and underlying business models as well as advances in technology, play a significant role in the development of the Internet of Things. The IoT model essentially consists of five layers.

- ***Perception layer:***

This layer consists of both physical things and sensing technology. Depending on the technique used to identify the object, these sensors could involve RFID tags, barcodes or infrared sensors. This data may include details about the object's location, humidity, motion orientation, orientation, etc., depending on the type of sensor. Once gathered, this data is forwarded to the network layer so that it can be sent safely to the processing unit. Figure 1 shows the IoT architecture.

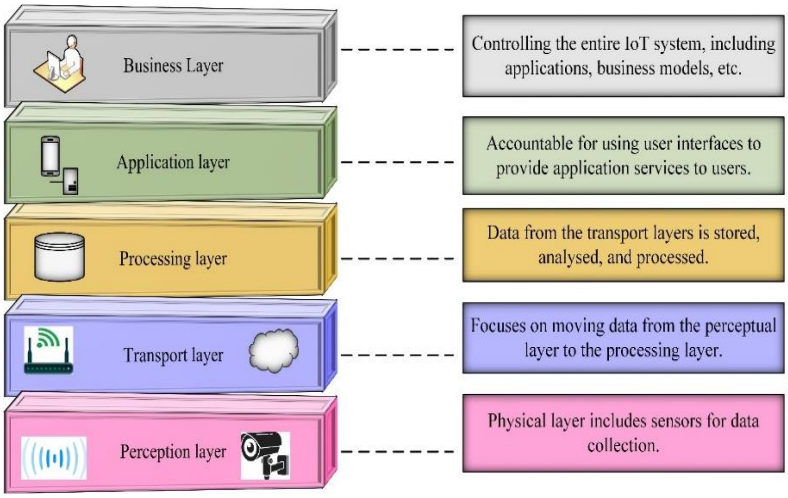

Figure 1. IoT architecture

- ***Transport layer***:

This layer's primary duty is to convey data collected from sensing devices to the system's processing unit in a secure manner. This data can be transmitted wirelessly or across wired networks. Depending on the sensor devices, the technology which can be utilised can include infrared, WiFi, 3G, Bluetooth, etc.

- ***Processing layer***:

Various services are implemented by IoT objects and devices. It can also exchange information with the database. This layer does extensive computations and information processing. Finally, it makes decisions on its own by examining the results.

- ***Application layer***:

This layer is in charge of giving overall programme administration based on the information from the item that was examined at the processing layer. IoT can be used for a variety of applications, including smart manufacturing, smart health, intelligent transportation, smart housing, and more.

- ***Business layer***:

The business layer works together with the larger Internet of Things system, which is made up of several apps and services. This layer produces graphs, flowcharts, and business models using the information obtained from the Application layer.

4. Popular Protocols in IoT Transport Layer

IoT application layers contain many popular protocols: REST, MQTT, CoAP, XMPP and DDS.

- ***REST***

The term "REST" [21] [22] refers to an architectural design approach for network systems in R.T. It is an architecture for designing network applications that is independent of the operating system and programming language being used to link devices. To put it another way, REST is an architectural approach that makes use of industry standards like HTTP, the Uniform Resource Locator (URL) and XML. Data communication utilising the client-server model and the HTTP protocol is made feasible by a web-oriented architectural style called REST. For message transmission in the REST architecture, HTTP is employed in the request-response system. The client sends the message via HTTP as a request, and the server responds using HTTP on the client's behalf. The Get, Put, Post and Delete techniques for HTTP requests are suggested by the REST architecture. Figure 2 shows the workflow of REST architecture.

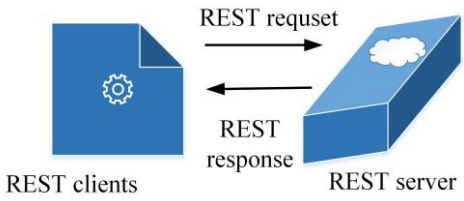

Figure 2. Workflow of REST architecture

- ***MQTT***

As opposed to the HTTP request/response framework, the Message Queue Telemetry Transport (MQTT) [23] [24] builds on the TCP/IP network protocol and employs a publish/subscribe design. The central hub responsible for relaying every message among recipients and senders is known as a MQTT broker. The publish/subscribe architecture of MQTT enables clients to both post messages with subjects and subscribe to topics in an event-driven manner. A client subscribes to a topic, and the broker then sends that client all messages with the corresponding subject. The topic provides routing data for the broker. Any hierarchical structure can have topics organised into a name space. Clients can interact over the topic of their choice alone without needing to know each other thanks to MQTT's extremely scalable and adaptable solutions. An open TCP link to the broker is maintained by each MQTT client. The MQTT broker can hold every message in the event that this connection is broken, and when it comes back up, it will transmit them to the user. Figure 3 shows the MQTT messaging structure.

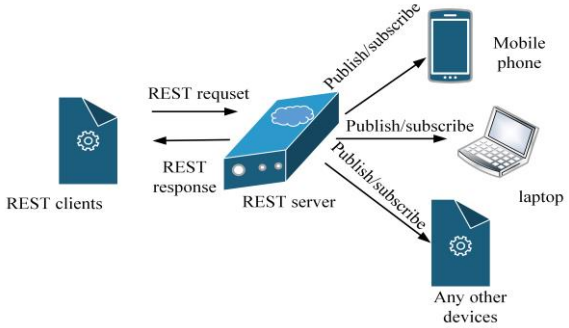

Figure 3. MQTT messaging structure

➢ ***CoAP***

In a wireless sensor network (WSN) and Internet of Things (IoT), the confined Application Protocol (CoAP) [25] [26] functions as a specialised web transfer protocol for usage with confined nodes and limited networks. CoAP is built on the REST Model, which supports the request/response as well as resource/observe paradigms to HTTP. In place of TCP as well as Datagram Transport Layer Security (DTLS), CoAP uses UDP as its transport protocol. Similar to HTTP, CoAP is built on a client/server architecture. Data is requested from a server by a client using the GET, POST, PUT or DELETE methods and codes. Confirmable (CON), Acknowledgement (ACK), Reset (RST) and Non-confirmable (NON-CON) are the four message types included in CoAP.

➢ ***XMPP***

With XMPP, users can send instantaneous messages across the Internet to anyone using any operating system. Numerous instant messaging apps have employed XMPP [27] [28] in the context of IoT due to its various possibilities. XMPP uses an XML stanza, which is a piece of code made up of three sections: message, presence and IQ, used to connect the server and client. Figure 4 shows the architecture of XMPP communication.

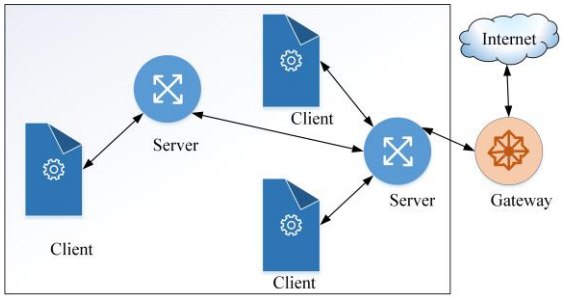

Figure 4. Architecture of XMPP communication

➢ ***DDS***

The Object Management Group (OMG) has standardised DDS [29] [30], publish-subscribe middleware that is data-centric and designed for highly dynamic distributed networks. Without using a central server that may become a single point of failure, the network architecture is dynamically identified and connections between nodes are made peer-to-peer. DDS is frequently used in industrial contexts due to the extensive range of Quality of Service (QoS) policies that it offers. The DDS architecture is defined by two levels: Data-Local Reconstruction Layer (DLRL) and Data Centric Publish Subscribe (DCPS).

➢ ***HTTP***

The Hypertext Transfer Protocol (HTTP) [31] [32], a dependable TCP application protocol for collaborative and distributed ecosystems, is said to be the cornerstone of data exchange on the internet. The client/server computing model of HTTP also offers REST and URI techniques, including PUT, DELETE, GET and POST, to access the many server-hosted resources.

Table 1: Details of various TCP protocols

Protocol	Communication mode	UFP/TCP	Size	Header size	Security and QoS	Security mechanism	REST
HTTP	Half Duplex	TCP	Heavy weight	Server dependent	Both	SSL/TLS	Yes
CoAP	Half Duplex	UDP	Light weight	4	QoS	DTLS	Yes
MQTT	Full Duplex	TCP	Light weight	2	Both	SASL/TLS	No
XMPP	Full Duplex	TCP	-	-	Security	SASL/TLS	Yes
DDS	Full Duplex	Both	Light weight	-	QoS	-	No

5. Energy-Efficient Transport Layer Security for the Internet of Things

To guarantee the optimal operation of IoT (Internet of Things) devices while preserving confidentiality and reliability, energy-efficient and secure transport layers are essential. It takes careful evaluation of many elements as well as the application of proper procedures and strategies to achieve this equilibrium. In the recent past, a number of authors have presented specific approaches which discussed below:

In order to reduce energy usage and improve data transfer to medical specialists, Saba et al. [33] suggested an energy-saving and secure architecture for e-healthcare utilising IoMT. Using the Kruskal algorithm, the next-

hop is chosen depending on a number of characteristics to produce an optimum and low-cost routing path. The structure, which is based upon the Kruskal algorithm, cleverly separates the subgraph from the whole graph and lowers the overall communication cost. Furthermore, patient data is sent and exchanged with confidentiality, posing a threat to data privacy as it travels over the public Internet through many unprotected access points. In this study, SEF-IoMT uses cypher block chaining to transmit the data in the form of chains, enhancing its security level against hostile traffic. In addition, the digital authentications based on private-public key are included in data transfer together with the cypher block chaining algorithm to guarantee its validity and integrity.

Kumar et al. [34] describe a safe and power-effective smart building architecture using developing IoT technologies. Each device has a distinct address that identifies it and the Constrained Application mechanism (CoAP) is a crucial web transmission mechanism. It is an application layer protocol, which means that data transit does not occur over secured channels. Datagram TLS (DTLS) was the security protocol that includes automatic authentication, data integrity, key management and secrecy. The performance of all technical systems is managed by a smart building design, which was developed to ensure energy efficiency.

Subashini et al. [35] suggest an encrypted Energy Efficient Framework (SEEF) as a better way to address a number of issues relating to the transmission and upkeep of encrypted data. Various self-modules are incorporated into SEEF to provide increased efficiency in terms of decreased energy consumption and improved QoS for data maintenance and transmission. Performance data shows an improvement in throughput of up to 96% and a packet delivery ratio (PDR) increase of 0.57 MB/s, respectively. The overall time delay and energy consumption are each reduced to 0.69 seconds and 0.076 joules, respectively.

According to a threshold value, Roshini et al. [36] proposed Hierarchical Energy Efficient Secure Routing protocol (HEESR) divides deployed body networks into relay nodes and direct nodes. In contrast with various traditional protocols, cluster head selection depends on the the traffic priority data and level of energy, such as non-critical and critical data. The information is then compressed using the Huffman encoding method and encrypted using an asymmetric cryptographic algorithm to ensure safe data transfer before being sent over the chosen path. Data prioritisation is the main method used by this protocol to add security and routing effectiveness in a hierarchical pattern. It achieved confidentiality of 93%, energy usage of 6% and throughput of 92%, which significantly reduced the packet loss rate and delivered the data on time.

The Host Identity Protocol (HIP), one of the current security protocols, was the main topic of Kauch et al. [33] work. A number of optimisation opportunities was found based on the examination of comparable research and some of them have been merged into the suggested E-HIP optimised protocol. It has been implemented as a modified version of the open-source OpenHIP library and used to communicate among real hardware devices for verification purposes. The secure interaction was effective. Experimental evaluation has determined that the suggested optimisation has a net consequence of a 20% increase in energy efficiency.

6. Techniques used to secure transport layer for Internet of Things devices

Communication between all layers is the primary importance of transport layer, which deals features like congestion avoidance, reliability, and the guarantee that packets is transported in the similar sequence as initially sent. Some networking protocols that are often used in the Internet of Things as integrated into the transport layers. Ahmad et al. [38] introduced to the devices connected to Internet of Things (IoT) produce and consume information, which necessitates data communication and forth between numerous devices. In terms of IoT, ensuring data security is a significant difficulty. A Intrusion Detection Scheme is often used to find and stop malicious containers for entering the system because IoT device is fundamentally low-power and don't need a lot of computing resources. Using features for the UNSW-NB15 data set, to recommend feature clusters based on message queuing telemetry transport (MQTT), and transmission control protocol (TCP). To fix issues through the data set like imbalance, dimensionality's grumble, and over-fitting. Since health data are extremely sensitive, end-to-end security solutions are required to protect and manage the health data was introduced by Kumar et al. [39]. The sensitive data that is gathered via wearable Internet of Things (IoT) devices is generally protected by a variation of authentication and authorisation systems.

The transport layer security (TLS) protocol is made to convey information more reliably for source to end. A user can get around the no missing or modified messages issue by using this protocol. Tolerating unreliability is where TLS presents its biggest challenge. The Datagram Transport Layer Security (DTLS) protocol is developed in order to address this problem in low-power wireless restricted networks. A handshake protocol, base protocol, record layer, alert protocol and Change CipherSpec comprise DTLS protocol. The difficult problem with the DTLS protocol is that a server could get a lot of ClientHello responses from an attacker. A denial-of-service (DOS) attack would be launched beside the server in this case. This denial-of-service attack establishes a new connection with the server, increases attacker bandwidth, and allots resources to each Client. The suggested a smart gateway-based authorization and authentication approach as a solution to this problem in order to stop and keep more complex physiological information from an malicious users and attackers.

In order to allow a wide range of applications and facilities, the Internet of Things (IoT), a novel era of computing in digital world, aims for the formation of numerous smart gadgets was suggested by Gupta et.al [40].

The devices is limited resources, and services would offer a demand particular constraints, with security being the most important one. Consequently, it is essential to clarify the IoT's central structure and its associated features in order to understand and observe with these norms. This extensive survey focuses on the security architecture of IoT and deals a detailed taxonomy of the area's most demanding issues as well as the key technologies like Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSN), which are permitting features in the development of IoT.

Internet of Things (IoT) usage is increased, and it has newly involved more attention because of the wide range of devices and applications, it is used for, containing sensitive home devices, medical devices, wireless sensors, and further associated IoT gadgets was presented by Lombardi et.al [41]. Since it proceeds time to aspect into each potential susceptibilities, security consideration is sometimes overlooked in the flash to quickly transport new IoT properties on market place. Security concerns is raised as IoT devices are internet-based contain sensitive and secret data. A central program referred to the "SDN Controller" is presented through the software-defined networking (SDN) technology, an intriguing development in computer system design that permits complete network device. Consequently, utilizing SDN is a strong method to improve IoT interacting efficiency and report current issues.

The Internet of Things (IoT) resource boundaries and widespread usage present a serious problem for IoT application security was introduced by Diroet al. [42]. Due to the present classical internet safety design, high resource supplies and lack of endwise security mechanisms, the need for effective and ultra-light security design and protocols. In the resource-constrained IoT setting, symmetric-key load encryption has also been utilized to reduce message communication overhead. The analysis demonstrates that, while maintaining similar authenticated end-to-end connectivity across communicating IoT nodes, the proposed technique overtakes Transport Layer Security (TLS) in terms of resource use. In comparison to current TLS-based security schemes, the proposed complete security scheme uses less overhead and conserves more communication capacity. The suggested approach, in particular, uses less handshakes and decreases the amount of transmitted messages of each handshake. Various method used to secure transport layer for Internet of Things devices is illustrates in Table 2.

Table 2. Summary of various method used to secure transport layer for Internet of Things devices

Author	Methods	Advantages	Limitations
Ahmad et al. [38]	MQTT, TCP	It offers reliable interaction among a network's communicating servers.	To fix issues with the data set such as imbalance, dimensionality's grumble, and over-fitting.
Kumar et al. [39]	DTLS	However, DTLS also benefits from the lower overhead and decreased latency of data packet protocols.	Less security
Gupta et al. [40]	RFID	Instead of needing to count every single item, RFID devices provide a quick and accurate method of tracking them.	Limited storage
Lombardi et al.[41]	SDN	For large, complicated networks that demand high uptime, SDN is a fantastic alternative.	The network must be completely reconfigured. This cost is greater as an effect of reconfiguration.
Diro et al. [42]	TLS	TLS offers a more secure way to handle authentication and message exchange.	More latency than other robust security techniques**.**

7. Challenges of transport layer security in Internet of Things

The key difficulties in creating a transport layer protocol are: Dynamic Topology, Power and Bandwidth constraints.

- ***Dynamic Topology***

The efficiency of the transportation layer is affected by the daily changes in technology, which will also have a small impact on it. A tool in Blender's sculpt mode is called dynamic topology. The mesh is automatically divided so that we can sculpt with more detail without having to consider the topology. Traditionally, when creating a 3D model, the shape as well as topology are both addressed simultaneously. Figure 5 shows the model diagram of dynamic topology

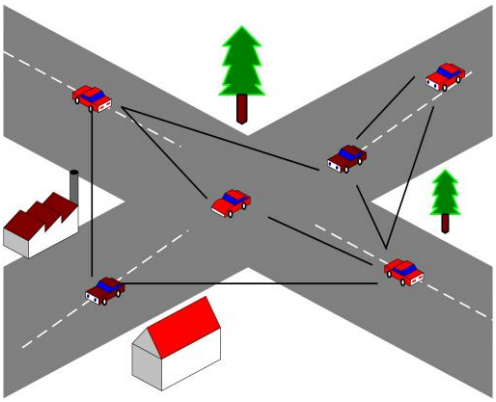

Figure 5. Model diagram of dynamic topology

- ***Power and Bandwidth constraints***

Government restrictions on transmission bandwidth as well as the weak power output of wireless systems are the main causes of their limits. Due to the restricted wireless resources, operators are looking for methods to increase channel capacity. But each methodology or approach used has its own difficulties.

- ***Unsecured data transmission***

Unsecured data transmission is the act of transferring data without the necessary security through a network or the Internet. This may expose the data to malicious entities who might intercept, alter, or steal. Data transfer across an unencrypted network link or the usage of insecure protocols can result in unsafe data transmission. It's critical to employ safe protocols such as VPN or TLS/SSL and to encrypt records before transferring it if you want to safeguard sensitive data through transmission. The data is accessed while being transmitted, this can help to maintain its integrity and confidentiality. IoT strategies regularly send sensitive data, which could be compromised if it is not adequately secured.

- ***Lack of encryption***

Even though encryption is an excellent method to prevent attackers from acquiring data, it presents one of the largest security concerns for IoT. These drives are used for a normal computer's storage and processing power.

8. Applications of transport layer security solutions

Using the cryptographic technology known as Transport Layer Security (TLS), data transmission across a computer network is made safe. It guarantees authentication, data integrity, and privacy for data between two interacting apps. TLS is widely used in many different industries, including:

- ***Location Sensing and Information Sharing:***

The location data contains of either relative or absolute position information from objects as well as environmental position data attained from CellID, GPS, RFID, and various sources. Some of the application used for information sharing is:

- *Tracking mobile assets*: Utilising the positioning sensor and communication feature already installed on the commodity, this programme can track and keep track of its state.
- *Fleet administration*: Based on the needs of the business and the current position data gathered by the vehicles, the fleet manager can plan the vehicles and drivers.
- *Information system for traffic*: By tracking the location data of numerous vehicles, this application can obtain traffic information including road traffic situations as well as congested areas.

- ***Virtual private networks***

Virtual private networks, or VPNs is to protect the confidentiality and safety of users when using the worldwide web, many VPN providers employ TLS to encrypt the communication among the user's device and the VPN server.

- ***Environment Sensing:***

Through locally or widely dispersed terminals, the IoT system can gather and procedure a variety of chemical or physical eco-friendly parameters. Temperature, noise, humidity, visibility, spectrum, pollution, light intensity, radiation, pictures, and bodily indicators are examples of common environmental information. Some of the application used here are:

- Environmental recognition: IoT systems provide disaster monitoring, factory monitoring, and environmental and ecological monitoring for things like forests and glaciers. All of them have automatic alarm systems that gather environmental data from several sensors.
- Remote medical observation: IoT can examine the recurrent indicator data gathered from the patient's body via the device and offer the users health trends and suggestions.

❖ ***Chat and Instant Messaging Programmes***

TLS is frequently used by well-known messaging applications to safeguard text, phone, and video communication, safeguarding user confidentiality and message content.

❖ ***Ad Hoc Networking:***

IoT devices is able to quickly form their own systems and integrate with the service/network layer to transport associated facilities. In vehicle network, the system connecting vehicles and roadways can rapidly self-organize in order to transport the data.

❖ ***Web Services (APIs)***

A large number of internet-based APIs (Application Programming Interfaces) secure data transfer among mobile devices and internet servers using TLS, preserving the privacy and reliability of API requests and responses.

❖ ***Secure Web Services (SOAP, REST)***

TLS is frequently used in the context of web services to safeguard interaction among the server and the client, preserving the confidentiality and authenticity of data sent over SOAP or REST APIs.

❖ ***Secure Communication:***

Depending on the needs of service, IoT systems is also offer a secure data transfer network from the application and IoT terminals.

❖ ***Transferring Files***

To safeguard files while they are being sent, TLS is frequently used with secure data transfer methods as SFTP (SSH File Transfer Protocol), secure SCP (Secure Copy Protocol) and FTPS (FTP Secure).

9. Effective Future Directions

The implementation of IoT is regard to a wide range of research is necessary in a number of different areas. Some issue are highlighted in this section: massive scaling, big data, robustness, human-in-the-loop, privacy and security. Figure 6 shows Effective Future Directions of IoT.

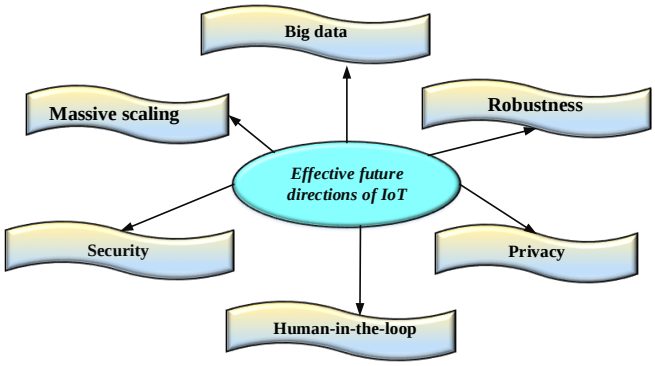

Figure 6. Effective Future Directions

➢ ***Massive scaling***

As IoT (Internet of Things) devices often contain a large amount of devices and can generate vast amounts of data, scalability is a crucial factor to take into account. Here are some important variables that can affect the IoT systems' ability to scale:

- *Network capacity:* It's critical to have sufficient network capacity to manage the rising demand as the number of devices and data traffic grows. This can necessitate updating the network infrastructure, such as by installing mesh networks, adding more access points, or boosting bandwidth.

- *Data processing:* It can be difficult to collect and analyze that data quickly and effectively as the quantity of data produced by IoT devices rises. Using edge computing is one strategy since it enables data processing to take place closer to the source, lowering latency and network traffic. Large amounts of data can be processed via cloud computing.

- *Device management:* The management and maintenance of several devices might become challenging. This necessitates the use of a scalable device management system with capabilities like automatic supply, remote control, and updates via the air.

➢ ***Big data***

Big Data is a sizable amount of data, then organizations similar social media systems and additional businesses collect the information. Which is utilized for a multiplicity of projects including predictive analytics

and machine learning. It is handled by Big Data analytics-supporting tools. Volume, Velocity, Variety, and Veracity are the four that data researchers use to help us learn Big Data.

- *Volume:* Volume, as you might have guessed, refers to the size of the data sets. These are typically several gigabytes in size, if not more. Due to its pure quantity, this enormous volume of data requires much specialised processing and analysis. This data cannot be stored using conventional storage methods. This means that a typical CPU cannot handle big data collections.
- *Velocity:* The term "velocity" describes the way quickly the records is produced, while High-speed data handling entails specialized approaches. As an illustration, social media is overwhelmed with a shocking size of posts each day. To expose data that can be useful in the future, extraordinary volume, high velocity, and variety data must be estimated and handled utilizing cutting-edge approaches.
- *Variety:* Big Data is an extraordinarily wide range of miscellaneous organisations, for online data such as social media posts and web pages to extra predictably accessible personal information, such addresses and phone records. Big Data typically comes from sources that fit into one of three categories: structured, semi-structured, or unstructured data. This diversity in data formats frequently necessitates specialized algorithms and various processing needs.
- *Veracity:* Data quality is referred to as veracity. "High veracity data" are records that are useful to evaluate because they are crucial to the final outcomes. However, a large portion of low-utility or useless data often makes up low-veracity data. This implies that in order to extract anything useful, it must first be sorted processed.

➢ ***Robustness***

A key aspect of IoT big data that has drawn a lot of attention from both researchers and business is the robustness of data processing. Robustness has a number of interpretations in many contexts. In this article, it will primarily concentrate on one common IoT scenarios that could potentially involve noisy data.

- *Noisy data:* The data that IoT devices collect typically contains some noise. There are various causes for this. IoT devices must operate in the presence of radio frequency noise due to their widespread deployment. Additionally, IoT device noise might be introduced by data gathering issues and anomalous behaviour. Another important element that can contribute to the noisy nature of the gathered data is future, incorrect measurement validation.

➢ ***Privacy***

IoT widespread use and interactions will offer people numerous conveniences and practical services, but it will also present numerous opportunities to violate people's privacy. The privacy regulations for every domain are required to set in order to address the privacy issue brought on by future IoT applications. Once specified, privacy must be enforced by the specific IoT infrastructure and IoT application.

➢ ***Human-in-the-loop***

Applications for the Internet of Things will multiply and advance over time. Since humans and things will work together in many of these new applications, most of them will directly involve people. A wide range of uses, such healthcare, energy management and automobile systems can benefit from the exciting possibilities provided by human in-the-loop devices. For instance, it is proposed that employing models of behaviours associated with daily life in home healthcare might improve illnesses of elderly people and keep them safe, and that expressly adding human-in-the-loop simulations for driving can increase safety. Although including humans in the process has obvious benefits, modelling people behaviours is quite difficult due to the intricate psychological, behavioural and physiological characteristics of people.

➢ ***Security***

The dealing with security assaults is a fundamental issue that is common in the Internet today and must be faced. Because of the low storage capacity of the items being used, the physical location of the sensors, objects, actuators, and openness of schemes, especially including the fact as the majority of devices will interact wirelessly, security assaults are a concern for the IoT. IoT security solutions are a significant research challenge because the majority of mainframe security solutions used today have complex computing and memory requirements. Given that many IoTs operate in real-time, a runtime self-healing manner with countermeasures, real-time detection and repairs is ideal for speedy responses.

TLS will continue to strive for higher levels of usability, performance and security in the future. TLS will adapt as cyber-security threats change to meet new difficulties while preserving its position as the key building block of secure internet communication. The advancement of these trends will depend heavily on cooperation between standards bodies, security community and the industry specialists.

10. Conclusion

Basic IoT structure and well-known protocols are described in this review article. TCP may be utilised in IoT, depending on the specific requirements of the application. If data security, reliability and integrity are important with minimal latency, TCP could be a viable choice. The widely used protocols such as REST, MQTT, CoAP, XMPP, DDS and HTTP are discussed in detail. To help new researchers, a discussion of several energy-efficient

TLS protocols and an explanation of the transport layer's difficulties is offered. The discussion of various prospects and successful future directions will help the researchers in the long term.

11. References

[1] Sarker IH, Khan AI, Abushark YB, Alsolami F (2023) Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. Mobile Networks and Applications vol. 28, no. 1, pp. 296-312.

[2] Khan NA, Khan AS, Kar HA, Ahmad Z, Tarmizi S, Julaihi AA (2022) Employing public key infrastructure to encapsulate messages during transport layer security handshake procedure. In2022 Applied Informatics International Conference (AiIC), pp. 126-130. IEEE.

[3] Kim H, Kim M, Ha J, Roh H (2022) Revisiting TLS-encrypted traffic fingerprinting methods for malware family classification. In2022 13th International Conference on Information and Communication Technology Convergence (ICTC), pp. 1273-1278. IEEE.

[4] Chen J, Cheng G, Mei H (2023) F-ACCUMUL: A Protocol fingerprint and accumulative payload length sample-based tor-snowflake traffic-identifying framework. Applied Sciences vol. 13, no. 1, pp. 622.

[5] Malik M, Dutta M, Granjal J (2023) L-ecqv: Lightweight ecqv implicit certificates for authentication in the internet of things. IEEE Access vol. 11, pp. 35517-40.

[6] Şeker Ö, Dalkılıç G, Çabuk UC (2023) MARAS: Mutual authentication and role-based authorization scheme for lightweight Internet of Things applications. Sensors vol. 23, no. 12, pp. 5674.

[7] Krähenbühl C, Legner M, Bitterli S, Perrig A (2021) Pervasive Internet-wide low-latency authentication. In2021 International Conference on Computer Communications and Networks (ICCCN), pp. 1-9. IEEE.

[8] Ohwo OB, Ayankoya FY, Ajayi OF, Alao DO (2023) Advancing DNS Performance Through an Adaptive Transport Layer Security Model (ad-TLSM). Ingénierie des Systèmes d'Information vol. 28, no. 3.

[9] Soni M, Singh DK (2023) Blockchain-based group authentication scheme for 6G communication network. Physical Communication vol. 57, pp. 102005.

[10] Chen B, Qiao S, Zhao J, Liu D, Shi X, Lyu M, Chen H, Lu H, Zhai Y (2020) A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. IEEE internet of things journal vol. 8, no. 13, pp. 10248-63.

[11] Wichary T, Mongay Batalla J, Mavromoustakis CX, Żurek J, Mastorakis G (2022) Network slicing security controls and assurance for verticals. Electronics vol. 11, no. 2, pp. 222.

[12] Wichary T, Mongay Batalla J, Mavromoustakis CX, Żurek J, Mastorakis G (2022) Network slicing security controls and assurance for verticals. Electronics vol. 11, no. 2, pp. 222.

[13] Sabanci K. Exploring Post-Quantum Cryptographic Schemes for TLS in 5G Nb-IoT: Feasibility and Recommendations (Master's thesis, Marquette University).

[14] Primbs J, Ilg W, Thierfelder A, Severitt B, Hohnecker CS, Alt AK, Pascher A, Wörz U, Lautenbacher H, Hollmann K, Barth GM (2022) The SSTeP-KiZ System—Secure Real-Time Communication Based on Open Web Standards for Multimodal Sensor-Assisted Tele-Psychotherapy. Sensors vol. 22, no. 24, pp. 9589.

[15] Jagannath A, Kane Z, Jagannath J (2022) RF fingerprinting needs attention: Multi-task approach for real-world WiFi and Bluetooth. InGLOBECOM 2022-2022 IEEE Global Communications Conference, pp. 4607-4612. IEEE.

[16] Bansal M, Nanda M, Husain MN (2021) Security and privacy aspects for Internet of Things (IoT). In2021 6th international conference on inventive computation technologies (ICICT), pp. 199-204. IEEE.

[17] Zhou Z, Chen X, Li E, Zeng L, Luo K, Zhang J (2019) Edge intelligence: Paving the last mile of artificial intelligence with edge computing. Proceedings of the IEEE vol. 107, no. 8, pp. 1738-62.

[18] Cirillo F, Solmaz G, Berz EL, Bauer M, Cheng B, Kovacs E (2019) A standard-based open source IoT platform: FIWARE. IEEE Internet of Things Magazine vol. 2, no. 3, pp. 12-8.

[19] Gonzalez R, Wiggers T (2022) KEMTLS vs. post-quantum TLS: Performance on embedded systems. InInternational Conference on Security, Privacy, and Applied Cryptography Engineering, pp. 99-117. Cham: Springer Nature Switzerland.

[20] Cardamone N, Dalena V, Mauro A, Settembre M, Vecchia G, Vitaliti A, Dondossola G, Bartalesi D, Garrone F, Terruggia R (2022) Blockchain-Based Public Key Authentication of IoT Devices for Electrical Energy Systems. In2022 AEIT International Annual Conference (AEIT), pp. 1-6. IEEE.

[21] Triawan A, Alipudin W (2021) Penerapan Representational State Transfer (REST) Pada Push Notification Whatsapp Untuk Layanan Informasi Akademik. Teknois: Jurnal Ilmiah Teknologi Informasi dan Sains vol. 11, no. 1, pp. 59-66.

[22] Sud K, Sud K (2020) Understanding REST APIs. Practical hapi: Build Your Own hapi Apps and Learn from Industry Case Studies, pp. 1-1.

[23] Sanjuan EB, Cardiel IA, Cerrada JA, Cerrada C (2020) Message queuing telemetry transport (MQTT) security: A cryptographic smart card approach. IEEE Access vol. 8, pp. 115051-62.

[24] De Rango F, Potrino G, Tropea M, Fazio P (2020) Energy-aware dynamic Internet of Things security system based on Elliptic Curve Cryptography and Message Queue Telemetry Transport protocol for mitigating Replay attacks. Pervasive and Mobile Computing vol. 61, pp. 101105.

[25] Majumder S, Ray S, Sadhukhan D, Khan MK, Dasgupta M (2021) ECC-CoAP: Elliptic curve cryptography based constraint application protocol for internet of things. Wireless Personal Communications vol. 116, no. 3, pp. 1867-96.

[26] Yassein MB, Hmeidi I, Meqdadi O, Alghazo F, Odat B, AlZoubi O, Smairat A (2020) Challenges and techniques of constrained application protocol (CoAP) for efficient energy consumption. In2020 11th International Conference on Information and Communication Systems (ICICS), pp. 373-377. IEEE.

[27] Bansal M (2020) Application layer protocols for internet of healthcare things (IoHT). In2020 fourth international conference on inventive systems and control (ICISC), pp. 369-376. IEEE.
[28] Ustun TS, Hussain SS (2020) IEC 61850 Modeling of UPFC and XMPP communication for power management in microgrids. IEEE Access vol. 8, pp. 141696-704.
[29] Michaud MJ, Dean T, Leblanc SP (2018) Attacking OMG data distribution service (DDS) based real-time mission critical distributed systems. In2018 13th International conference on malicious and unwanted software (MALWARE), pp. 68-77. IEEE.
[30] An K, Kuroda T, Gokhale A, Tambe S, Sorbini A (2013) Model-driven generative framework for automated omg dds performance testing in the cloud. ACM Sigplan Notices vol. 49, no. 3, pp. 179-82.
[31] Ho MH, Yen HC, Lai MY, Liu YT (2021) Implementation of dds cloud platform for real-time data acquisition of sensors. In2021 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), pp. 1-2. IEEE.
[32] White R, Caiazza G, Jiang C, Ou X, Yang Z, Cortesi A, Christensen H (2019) Network reconnaissance and vulnerability excavation of secure DDS systems. In2019 IEEE European symposium on security and privacy workshops (EUROS&PW), pp. 57-66. IEEE.
[33] Shah R, Correia S (2021) Encryption of data over HTTP (hypertext transfer protocol)/HTTPS (hypertext transfer protocol secure) requests for secure data transfers over the internet. In2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), pp. 587-590. IEEE.
[34] da Cruz MA, Rodrigues JJ, Lorenz P, Solic P, Al-Muhtadi J, Albuquerque VH (2019) A proposal for bridging application layer protocols to HTTP on IoT solutions. Future Generation Computer Systems vol. 97, pp. 145-52.
[35] Saba T, Haseeb K, Ahmed I, Rehman A (2020) Secure and energy-efficient framework using Internet of Medical Things for e-healthcare. Journal of Infection and Public Health vol. 13, no. 10, pp. 1567-75.
[36] Kumar A, Sharma S, Goyal N, Singh A, Cheng X, Singh P (2021) Secure and energy-efficient smart building architecture with emerging technology IoT. Computer Communications vol. 176, pp. 207-17.
[37] Subashini S, Mathiyalagan P (2020) A cross layer design and flower pollination optimization algorithm for secured energy efficient framework in wireless sensor network. Wireless Personal Communications vol. 112, no. 3, pp. 1601-28.
[38] Roshini A, Kiran KV (2023) Hierarchical energy efficient secure routing protocol for optimal route selection in wireless body area networks. International Journal of Intelligent Networks vol. 4, pp. 19-28.
[39] Kaňuch P, Macko D (2019) E-hip: An energy-efficient openhip-based security in internet of things networks. Sensors vol. 19, no. 22, pp. 4921.
[40] Ahmad M, Riaz Q, Zeeshan M, Tahir H, Haider SA, Khan MS (2021) Intrusion detection in internet of things using supervised machine learning based on application and transport layer features using UNSW-NB15 data-set. EURASIP Journal on Wireless Communications and Networking vol. 2021, pp. 1-23.
[41] Kumar PM, Gandhi UD (2020) Enhanced DTLS with CoAP-based authentication scheme for the internet of things in healthcare application. The Journal of Supercomputing vol. 76, no. 6, pp. 3963-83.
[42] Gupta BB, Quamara M (2020) An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. Concurrency and Computation: Practice and Experience vol. 32, no. 21, pp. e4946.
[43] Lombardi M, Pascale F, Santaniello D (2021) Internet of things: A general overview between architectures, protocols and applications. Information vol. 12, no. 2, pp. 87.
[44] Diro A, Reda H, Chilamkurti N, Mahmood A, Zaman N, Nam Y (2020) Lightweight authenticated-encryption scheme for internet of things based on publish-subscribe communication. IEEE Access vol. 8, pp. 60539-51.

Author Profile

Dr. T. V. V. Satyanarayana is currently working as Professor in the Department of ECE, Mohan Babu University, Tirupati. He completed his Graduation and Post Graduation in Electronic Science from Acharya Nagarjuna University in 2002 and 2004 respectively. He obtained M.Tech in Communications and Radar Systems from Acharya Nagarjuna University in 2007. His research interests include IoT, Machine Learning and allied fields. Currently he is the reviewer of various International Journals. He has 45 International publications and 4 patents to his credit.