**Securing the Internet of Things: A Comprehensive Survey on IoT Security Challenges and Solutions**

**Abstract**

Because it connects multiple sensors and items to interact with one another without the intervention of human involvement, the The Internet of Things (IoT) has recently gained popularity. A hot study issues. The requirements for large-scale IoT deployment are fast expanding, and security is a big concern. By performing an exhaustive survey of previous work in the domain of IoT security, this research focuses on the most recent IoT security risks and vulnerabilities. The current danger taxonomy is provided in the application, architecture, and communication contexts. This research also compares potential IoT security concerns. The IoT security scenario is discussed, along with an examination of potential attacks. There are also open research topics Considering the challenges of IoT security implementation discussed. This research seeks to serve as a valuable guide to existing security risks and weaknesses in the IoT heterogeneous environment, as well as potential solutions for strengthening IoT security architecture.

**1 Introduction**

The Internet of Things (IoT) is a network of connected devices. and items that can communicate with each other without the need for human involvement. Sensor devices, for example, are physical devices, that monitor and gather various forms of data about machines and human social life are included in the "things" in the IoT. People, things, sensors, and services are all constantly connected thanks to the Internet of Things. The Internet of Things' main goal is to create a network infrastructure with communication protocols and applications that are interoperable that allows Personal computers (PCs), smart devices, cars, and goods are all examples of physical/virtual sensors. like refrigerators, dishwashers, microwave ovens, food, and medicines to be connected and integrated at any time and on any network. Because of advancements in smartphone technology, a wide range of things can now to be a part of the Internet of Things via various smartphone sensors. The requirements for large-scale IoT implementation, on the other hand, are fast expanding, posing a serious security problem.

The major obstacles in an IoT context are privacy, authorization, verification, access control, and system are all terms that can be used to describe how a system works. setup, information storage, and management. Smartphone and embedded devices are examples of IoT applications, for example, contribute to the creation of a digital environment that promotes global connectivity makes life easier sensitivity, adaptability, and responsiveness to human needs requirements. Security, on the other hand, cannot be assured. When a user's signal is interrupted or intercepted, their privacy may be jeopardized, and information about them may be disclosed. This issue should be addressed to ensure For the IoT to be extensively adopted, users must have confidence in terms of privacy and control over personal information. Addressing security concerns is critical to the IoT's development.

The focus of this survey report is on security risks and weaknesses with the context of IoT security, as well as present IoT security. We look at a variety of existing studies in the subject of Internet of Things (IoT) security that employ various strategies. Based on current security concerns in the settings of application, architecture, and communication, we provide an IoT security taxonomy. The IoT's potential security threats and vulnerabilities are also compared. We present a novel security scenario for the IoT architecture and analyze potential threats and assaults on the IoT environment.

This research seeks to serve as a valuable guide to existing security risks and weaknesses in the IoT heterogeneous environment, as well as potential solutions for strengthening IoT security architecture. State-of-the-art IoT security threats and vulnerabilities have been investigated in terms of application deployments such as smart environment, intelligent transportation, smart grid, and healthcare system.

The security of the Internet of Things, particularly Authentication and permission have also been examined as part of the Internet of Things architecture.

The most important work is a safe Internet of Things architecture for smart cities based on Chakrabarty and Engels' black SDN proposal (2016). However, due to the restricted nature of IoT nodes, the proposed architecture does not provide a full SDN implementation, making IoT nodes subject to new sorts of risks and assaults, such as node capturing, eavesdropping, and manipulation. The architecture also reduces network efficiency and makes routing more difficult. The current research proposes a comprehensive solution to the security challenge based on the flaws and limits of existing methodologies.

Abdmeziem and Tandjaoui's end-to-end (E2E) For e-health applications, a secure key-management protocol is required. is another similar study (2015). The security protocol is restricted to offloading computationally intensive third-party cryptographic primitives and does not define the necessary trade-off between the cost of communication and the quantity of third parties. Flauza, Gonzalaz, and Nulot (2015) do not specify cryptographic primitives and do not disclose them to third parties. suggested a border controller-based SDN-based security architecture for the IoT. Border controllers, on the other hand, have several disadvantages, including securing business security and both wanted and unwanted traffic. The authors did not address any of these issues. Herndez-Rams et al. (2018) focused on a restricted smart object authentication and authorization system. Nonetheless, the proposed architecture for authentication and authorization was not incorporated into the restricted IoT contexts.

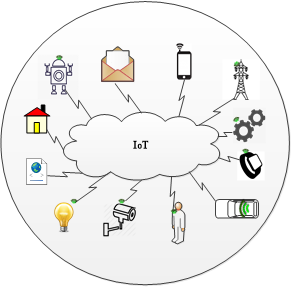
The rest of this paper is laid out as follows. Section 2 gives an overview of the Internet of Things (IoT) and the differences between IoT and traditional wireless network security. The Internet of Things (IoT) is classified under Section 3. The risks and weaknesses of the Internet of Things are discussed in Section 4. The IoT security taxonomy is described in Section 5. A scenario for IoT security is presented in Section 6. The examination of prospective assaults offered by threats and vulnerabilities on the IoT is presented in Section 7. Section 8. discusses potential future directions. Finally, Section 9 brings the research to a close.

**2 Overview of IoT**

The Internet of Things (IoT) has recently gained popularity and gotten a lot of attention due to the growing number of Internet-connected products. The Internet of Things (IoT) is the linking of massive diverse communication patterns in heterogeneous network architectures and systems, such as human-to-human, human-to-thing, and thing-to-thing. Furthermore, the Internet of Things (IoT) is a domain in which physical objects are continually connected to build an information network with the purpose of providing sophisticated and intelligent services to users. The connected "things" (sensors or mobile devices, for example) monitor and collect a wide range of environmental data. They make it possible to collect real-time data on properties, people, plants, and animals.

Sensor-equipped devices in the IoT model understand how to move light data around the physical world, allowing cloud-based resources for data extraction and decision-making based on the extracted data utilizing devices with actuators, which improves communication between nodes. IoT applications have been improved using various methodologies, strategies, and models generated from device-driven-embedded frameworks as the degree and number of IoT components has increased. The Internet of Things (IoT) is necessary to handle issues such as real-time communication, the presence of both a sensor and an actuator, as well as the IoT's distributed heterogeneous nature. Securing a wireless sensor network is approached in this way (WSN (Wireless Sensor Network)), which is a key component for constructing restricted devices in the IoT, has been researched by many research groups.

WSNs (Wireless Sensor Network) are wireless ad hoc networks that serve as the foundation for IoT devices. They are used to collect data from their surroundings and deliver it to users, as well as to remotely access linked IoT devices. They are made from many small nodes that are capable of detecting, computing, and communicating with other devices (Bi, Wang, and Xu, 2016 and Frizzo-barker et al., 2016). Secrecy, trustworthiness, verification, and non-revocation are all requirements for communication between the Internet and sensor nodes. In terms of deployment and technology, IoT privacy and security challenges differ from those in traditional and other wireless networks (Yinbiao et al., 2014). Low-power, lossy networks are used to deploy IoT networks (LLN (Low power and Lossy Networks) (Low power and Lossy Networks)). LLNs (Low power and Lossy Networks) are networks with energy, memory, and computing power constraints. As a result, IoT environments are secured using lightweight encryption technology, which incorporates a lightweight cryptographic method. For traditional and other wireless networks, these aspects have not been studied.



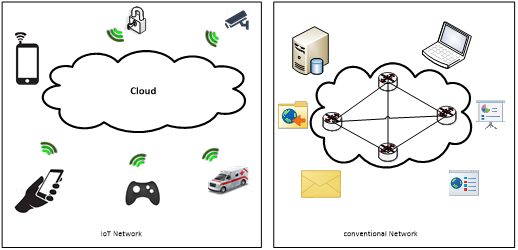
**2.1 Internet of Things Security vs. Traditional Security**

In terms of security and privacy, there are some fundamental distinctions between IoT and traditional wireless networks. The implementation of the Internet of Things, for example, is unlike that of the traditional Internet. LLNs are used by some IoT devices, whereas others have highly dynamic topologies that are dependent on the application. Dynamism, memory, and processing power all put a strain on LLNs (Lu, 2014). These factors are not considered on the regular Internet. Due to node impersonation, LLNs suffer significant data losses. For example, if an attacker can access the network under any guise during data transmission, the attacker can be assumed to be a legitimate node.

Both IoT and traditional network devices have various security characteristics and requirements. Sensor nodes have limited processing power and storage capacity in the IoT perception layer, making frequency hopping communication and public key encryption to protect IoT devices difficult. IoT devices use lightweight encryption technology, which comprises a lightweight cryptographic algorithm. The network layer of the IoT network has security challenges, Man-in-the-middle and counterfeit attacks are examples of such assaults. Both attacks can capture and send false information to network communicating nodes (Zhao, 2013). Unauthorized nodes are prevented using identity authentication and data secrecy mechanisms. Data sharing is the most essential element in the application layer. Data sharing causes issues with data privacy, access control, and information disclosure (Zhang, 2015). Authentication, key agreement, and user privacy protection over diverse networks are all s for the application layer, there are security needs.

Furthermore, both networks use different communication protocols. Each network layer has its own set of communication protocols. In the IoT perception/physical layer, for example, IPv6 is used through low-power wireless personal area networks, but in traditional networks, wireless fidelity is employed in the physical layer. Datagram Transport Layer Security (DTLS) is utilized as a communication protocol at the IoT network layer, whereas a transmission control protocol is employed in traditional networks (TCP (Transmission Control Protocol)). In the IoT application layer, the Constrained Application Protocol (CoAP) is utilized for communication, whereas in traditional networks, the Hypertext Transport Protocol (HTTP) is employed (Milbourn, 2016).

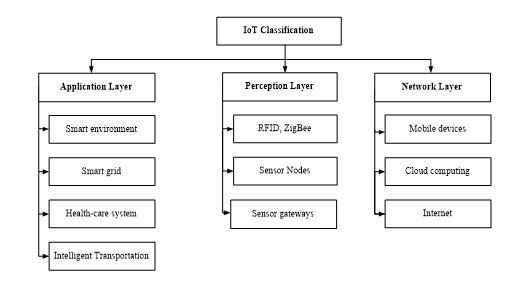
In conclusion, traditional security architecture is created from the standpoint of people and is unsuitable for machine-to-machine communication. Although the security concerns in both networks are similar, the methodologies and strategies employed to address each network security issue are different (Kai, 2016). The security threats and vulnerabilities highlighted in this survey are particular to IoT devices.



*Figure 2: Traditional Network vs. IoT Network*

**3 IoT Classification**

The Internet of Things can be separated into three layers: application, perception, and network protocol (Zhao and Ge, 2013).

Figure 3: Internet of Things (IoT) categorization

**3.1 Application Layer**

There is presently no single standard for designing the IoT application layer (Zhao and Ge, 2013). Depending on the service it provides, the application layer can be organized in several diverse ways. The application layer is the topmost and most visible layer to the user.

This layer contains Smart grid, smart city, healthcare system, and intelligent transportation protocols are examples of applications. An application layer protocol is dispersed across several end systems, with one end system's application using the protocol to exchange data packets with another end system's application. An application layer typically includes middleware, a machine-to-machine (M2M) communication protocol, cloud computing, and a service support platform. Depending on the sector and surrounding conditions, different security challenges arise (Valmohammadi, 2016).

**3.1.1 Intelligent Environment**

Smart environments, such as smart cities, can be imagined thanks to the integration of IoT applications. A smart environment integrates the services of several shareholders and scales to support many users in a reliable and distributed manner. They should be able to work in both wired and wireless system environments, as well as deal with constraints such as restricted data access and an untrustworthy network. In an IoT smart environment, context awareness is associated with a variety of methods, methodologies, models, features, frameworks, applications, and middleware solutions (Ning and Liu 2015). As a result, M2M communication between IoT devices is less demanding and gives more relevant data that aids in the recognition of a scenario or data. Smart city devices, on the other hand, are vulnerable to a variety of threats and attacks, including smart city DoS attacks, data manipulation, fake seismic detection, and fake flood detection.

**Smart Grid 3.1.2**

Smart meters, smart appliances, renewable energy sources, and energy-efficient resources are all part of a smart grid. Due to the increased need for alternative energy sources, the traditional electrical distribution infrastructure has been modernized, which is advantageous to energy distribution. A smart grid is an electrical distribution system that encompasses a wide range of electrical power functions, such as smart meters, smart gadgets, sustainable energy resources, and effective energy qualities, and distributes energy flows in a bidirectional manner from manufacturers to consumers. Smart grids are essential components of energy management for a healthy environment. Smart grids are dependable, reduce costs and increase energy independence. Customer security, physical security, traditional power equipment trust, device endpoints, and malicious attacks are all threats to the smart grid.

**3.1.3 System of Healthcare**

The rising expense of health maintenance and the prevalence of long-term disorders around the world necessitate a transformation of healthcare services from a doctor-centered framework to an individual-centered environment, with an emphasis on disease control and patient health (Moosavi et al., 2015). The framework is built on radio frequency technology, which provides basic networking capabilities. The interconnection of micro nodes built using sensing (detecting) and actuating (activating) capabilities placed inside or outside the human body underpins e-health (Abdmeziem and Tandjaoui, 2015). The apps are connection-aware, active, and tailored, and they communicate with connected devices over trusted channels. The rapid growth of IoT services has necessitated the development of new techniques to deal with heterogeneous devices, changing availability, and data-generating behavior (Abdmeziem and Tandjaoui, 2015 and Aazam et al., 2016). Smart healthcare entails the usage of smart health cards that safeguard patients' confidentiality and privacy. Smart health cards, on the other hand, are prone to theft, loss, insider misuse, unintended activities, hacking, internal attack, and cyber-attack (Aman and Snekkenes, 2016).

**Intelligent Transportation 3.1.4**

Information technology, vehicle manufacturers, and industries are all contributing to the Internet of Things revolution by developing new products and systems that incorporate a variety of technologies and communication solutions, such as radio frequency identification (RFID) tags, sensors, and actuators (Kanuparthi, Karri, and Addepalli, 2013). The introduction of detection advancements in passive RFID tags will enable completely new functionalities in the IoT application space, especially in terms of tracking locations and movement and temperature monitoring (Atzori, Iera, and Morabito, 2010). RSUs (Roadside Unit) and On-Board Units (OBUs) with transceivers and transponders make up the Dedicated Short-Range Communication (DSRC) system. It operates between the radio frequencies of 5.725 MHz and 5.875 MHz and is mostly used for frequent data transfer between automobiles and roadside infrastructure, such as toll collecting. Furthermore, with the Electronic Fee Collecting (EFC) program for toll collection, DSRC supports intelligent transportation systems. EFC is mostly utilized in the United States and countries of the European Union, such as Switzerland, Germany, and Austria (Bansal, Kenney and Rohrs, 2013).

In Europe, EFC deployment is based on the European DSRC 5.8 GHz technology, a standard produced by the Comité Européen de Normalization (CEN) and based on the European Telecommunications Standards Institute (ETSI), with IEEE 1609.2 as the security standard. However, these systems are currently incompatible in terms of technology, security, and billing mechanisms. The tariff concept is one of the most common sources of incompatibility in the classification parameters used and how the cost is calculated (i.e., whether it is based on network, distance, or zone/congestion). In terms of security, for example, several security procedures are employed to ensure the integrity of data stored in OBU.

Large-scale WSNs are used in intelligent transportation to track trip time online (from point A to point B), Decisions about routing, wait lengths, air pollutants, traffic congestion, and noise emissions are all factors to consider. Intelligent transportation includes traffic control, parking, and public transportation. Its simplicity allows diverse personnel to be well-informed, as well as the safe, organized, and smooth operation of intelligent transportation systems. Intelligent transportation, on the other hand, is vulnerable to a variety of risks and attacks, including denial of service (DoS), incorrect configurations, insecure transmission channels, congestion control, security, and spectrum sharing.

**3.2 Perception Layer**

Data collection is a function of the perception layer. This layer consists of two parts: the perception node (sensors, controllers, and so on) and the perception network (which connects the network layer). The perception node acquires and controls data, whereas the perception network layer executes control instructions for transferring and regulating data. All forms of sensors, including RFID, ZigBee, sensor nodes, and sensor gateways, are included in perception layer technologies.

**Radio Frequency Identification**

Radio Frequency Identification technology is the most significant advancement in the embedded communication model, as it allows microprocessors to be configured for wireless communication. There are two types of RFID tags: active and passive. RFID tags that are active have a power source. In terms of processing capability and storage, they are identical to the lower end nodes of WSNs. These tags send signals to readers no matter how far away they are, and their power supply allows for rapid connection. The lifespan of active RFID devices is limited. Passive RFID tags, on the other hand, are not powered by a battery.

They establish communication between the tag and the RFID reader by harnessing the power of the reader's query signal. They are utilized in a variety of applications, including bank cards and toll tags. Passive RFID tags are small and have an almost limitless lifespan. RFID tags have two main characteristics: auto identification and unique identity, which involves the quick interchange of data between tags and readers via wireless links. Tracking, DoS, repudiation, spoofing, eavesdropping, data newness, accessibility, self-organization, time management, secure localization, tractability, robustness, survival, and counterfeiting are all threats and attacks on RFID.

**Sensor Nodes**

A sensor node can collect and interpret sensory data as well as communicate with other network nodes. The following components are found in sensor nodes: I a controller that performs (ii) a transceiver that transmits and receives radio frequencies, and (iii) a data processor that regulates the functioning of other pieces in the node, (iii) a program memory for programming the device, (iv) a power source for the nodes, and (v) hardware for collecting data from the environment The essential components of a sensor node are the sensors and actuators that are used for sensing and activating devices based on commands delivered by the nodes. The sensor node has a long connection delay and is flexible. Sensor nodes are vulnerable to threats and attacks such as node subversion, node failure, node outage, passive information collecting, false node message corruption, exhaustion, unfairness, Sybil, jamming, tampering, and collisions.

**Sensor Gateways**

Sensor gateways manage wireless networks and aggregate data from multiple distant WSN nodes. A 2.4 GHz IEEE 802.15.4 radio is included in every gateway for communication. WSN entails the use of a network of dedicated transducers and a communication framework to monitor and record the status of any sensor device at various places. Temperature, humidity, pressure, wind direction and speed, light strength, vibration strength, sound strength, power-line voltage, chemical concentrations, pollution levels, and dynamic physiological functions are all monitored on a regular basis. For data exchange between two or more devices, the wireless communication channel entails radio communication, transmitters, and receivers. User access, network expansion, mobility, and cooperation are all aided by this route. Nonetheless, misconfiguration, hacking, signal loss, DoS, war dialing, protocol tunneling, man-in-the-middle assault, interruption interception, and alteration fabrication are all threats and attacks on this channel (Liu et al., 2016).

**Network Layer**

The perception layer, which is responsible for data transmission and storage awareness, receives network transmission and information security from the network layer, as well as a constantly accessible atmosphere The network layer includes mobile devices, cloud computing, and the Internet.

**Mobile Device**

A mobile device (such as a tablet or laptop) is a computer that runs an operating system (OS) that enables it to run business, enterprise resource planning, and finance applications. Most portable gadgets include Wi-Fi, Bluetooth, Near-Field Communication (NFC), and the Global Positioning System (GPS) built in, allowing them to connect to the Internet and other devices. Mobile devices can also deliver location-based services. Smartphones and personal digital assistants are ideal for people who want to take advantage of some of the benefits of a traditional PC (Personal computers) without having to move one. By integrating data capture devices such as barcodes, RFID, and smart card readers, digital business partners can further expand the available components for business users. Despite this, mobile devices are prone to threats and assaults such as tracking, eavesdropping, denial of service (DoS), bluesnarfing, bluejacking, bluebugging, data corruption, and deletion.

**Cloud Computing**

Cloud computing is a type of distributed computing that uses the Internet to provide common data processing for a variety of devices based on a set of criteria. This distributed computing approach enables ubiquitous, appropriate on-demand network access to a growing pool of computing properties (e.g., servers, systems, storages, functions, and utilities). On the Internet of Things, cloud computing technology has made it easier to process enormous volumes of data created by communicating devices and provides IoT devices with on-demand resources. High computational power, low-cost services, high performance, adaptability, and openness for device accessibility are all features of this technology (Botta et al., 2016). Cloud computing is a distributed computing that makes use of the Internet to provide standardized data processing for a variety of devices based on a set of criteria. This distributed computing technique offers on-demand network access to a growing pool of computing properties from anywhere in the world (e.g., servers, systems, storages, functions, and utilities). On the Internet of Things, cloud computing technology has made it easier to process enormous volumes of data created by communicating devices and provides IoT devices with on-demand resources. High computational power, low-cost services, high performance, adaptability, and openness for device accessibility are all features of this technology (Botta et al., 2016).

**Internet**

The Internet is a worldwide network of interconnected computers that connects billions of devices using the conventional Internet protocol (IP) suite (TCP/IP). A network of networks, such as private, public, academic, business, and government networks, make up this configuration, that are linked together via a variety of electronic, wireless, and optical networking technologies and span a local to a global scale. The Internet provides a wide range of information and services, connecting hypertext files to the World Wide Web application, e-mail, communication, and distributed document sharing systems are just a few examples. The hardware and software layers that make up the Internet communication architecture regulate many aspects of the system. Millions of restricted devices are connected to the Internet to communicate and share resources. Confidentiality, encryption, infections, cyberbullying, hacking, identity theft, reliability, integrity, and consent are all frequent security and privacy concerns over the Internet.

**4 Threats and Vulnerabilities of the IoT**

The several types of existing security solutions for the IoT are described in this section, which includes related works that focus on the risks and weaknesses of the IoT. Security solutions for threats and vulnerabilities in IoT architecture and applications were the focus of the associated works.

In the literature, several specific solutions for IoT architecture and applications have been offered (Granjal, Monteiro, and Silva, 2015 and Guo, Chen, and Tsai, 2017). Chakrabarty, Engels, and Member (2016) and Haroon et al. (2016) suggested a secure IoT architecture for smart cities that solves the vulnerabilities in traditional IoT systems (2016). Black networks and a Key Management System (KMS) make up the architecture, which ensures confidentiality, integrity, privacy, and efficient key distribution. The goal was to provide security services that minimize IoT network vulnerabilities at the link and network layers, with a focus on mission-critical data. The disadvantages of this strategy include the lack of a privacy solution for specifying device location, as well as additional routing issues for IoT nodes that are sleeping, resulting in data loss.

Valdivieso et al. (2014) and Akhundzada et al. (2016) presented an SDN architecture for developing IoT applications to overcome traditional networks' inflexible security. A SDN architecture was chosen as the foundation for constructing a secure network operating system that gives administrators a global view of potential risks and attacks on the IoT network, as well as the ability to control the network against those threats. SDNs, on the other hand, have some downsides in terms of security, scalability, and reliability. The separation of an SDN's control and data planes produces poor packet processing performance, which leads to serious issues including packet delay or loss, as well as distributed DoS (DDoS) attacks.

Flauzac, Gonzalez, and Nolot developed a unique SDN-based security architecture for the IoT, commonly known as the SDN domain employing border controllers (2015). The authors explained how SDN might be used to connect heterogeneous IoT devices, how each domain's security could be improved, and how security rules could be spread without jeopardizing any domain's security. However, the authors were unable to handle the challenges of securing both wanted and unwanted traffic, as well as corporate protection, which are two of the most significant disadvantages of deploying border controllers.

A unique lightweight key management mechanism was proposed by Abdmeziem and Tandjaoui (2015). To establish a safe and protected communication channel for limited nodes and wireless devices, the protocol relies on the collaboration of various IoT security components. The protocol ensures data confidentiality and restricted node authentication during data transfer throughout the channel. The security protocol, on the other hand, is restricted to dumping heavyweight cryptographic primitives to uninvited third parties and does not describe the essential tradeoff between communication overhead and the number of third parties.

For restricted smart objects, Hernández-Ramos et al. (2015) focused on a lightweight validation and authorization security architecture. The suggested security framework's objects/devices are compliant with the EU FP7 IoT-A Project's recent IoT Architectural Reference Model project. Following that, the framework plans to propose a general security strategy for designing unique lightweight security protocols for the Internet of Things. The authors did not, however, integrate the suggested framework into limited IoT contexts for authentication, authorization, or developing alternate processes to evaluate its accuracy.

SecKit, a security toolkit for integrating a management framework for IoT devices, was proposed by Neisse et al. (2015). The security toolkit seeks to aggregate meta-models and serve as a foundation for developing IoT security engineering tools, add-ons, runtime components, and extensions to solve security, data protection, trust, and privacy concerns in the limited IoT context. Cross-domain security configuration and interoperability are also enabled and improved by the framework. One disadvantage of this method is that it does not include a design study for deploying security and privacy solutions for devices in a dynamic environment. Another disadvantage is that data security is not guaranteed, as hostile attackers might simply take control of IoT actuators and send erroneous data, causing the data transmission process between linked devices to be disrupted.

Several solutions to the dangers and vulnerabilities of IoT architecture and applications are investigated and discussed in this review. Rather than creating separate solutions for various architecture and application scenarios, we believe that IoT applications may be secured by implementing a universal IoT security architecture that considers in this survey's proposed IoT security solutions. To our knowledge, none of the currently available security approaches have the following characteristics of IoT architecture:

1. A privacy approach for specifying node positions and coping with new routing challenges caused by header encryption for IoT nodes that are sleeping.
2. For offloading, a simple symmetric cryptography solution to third parties at restricted nodes.
3. Managing poor packet processing performance due to the SDN's control and data plane separation.
4. Allowing limited nodes to create a shared key with any wireless devices with whom they have no prior shared information.
5. Apart from the limited nodes and wireless items, ensuring an E2E code in which no entity has knowledge of the exchanged secret.

In fact, building a generic security solution for a wide range of IoT applications that is backward compatible with existing systems is safer.

In the following part, we present and discuss our newly constructed IoT security taxonomy, which includes application, architecture, communication, and user.

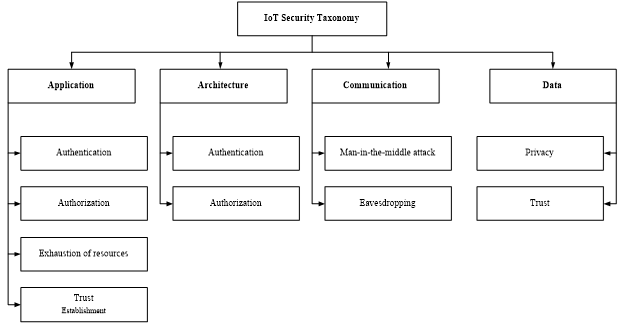
**5 Security Taxonomy for IoT**

The current state of IoT security methodologies outlined in Section 3 points to the need for a new security taxonomy to categorize types of security risks and vulnerabilities in each IoT application area that is simple and more specific. As a result, we detail the functionality and performance of each domain in relation to various threats and vulnerabilities, as well as how security countermeasures might help to improve security in every IoT application domain.

As a result of new security threats posed to IoT devices, the security information profile of the devices is constantly changing. Although technology solutions may be implemented in response to IoT risks and vulnerabilities, IoT security remains a big management issue. To effectively manage IoT dangers, a rigorous and thorough study is required to reduce identified threats in the IoT environment (Covington, 2013). The IoT security taxonomy must give a full study of the security mechanisms, including services and threats, as well as how all their components work, to provide system developers and analysts with the information they need to design and analyze secure systems.

The suggested taxonomy aids in the development of an IoT security framework in a diverse context. The IoT security taxonomy will aid in the examination of IoT security, which is an important topic (Mahalle, Babar, Prasad, and Prasad, 2010 and Babar et al., 2015). The proposed taxonomy will be utilized as a framework to study certain new unknown vulnerabilities and attacks in IoT networks in a methodical manner. This taxonomy will aid security developers in the creation of security models for limited devices, as well as serve as a useful resource for security analysts.

Building a new classification of the application domain, architectural domain, communication channel, and data domain for the IoT is the first stage in establishing our taxonomy. Then, for IoT security, we develop a new matrix taxonomy that links each classification to its proper components. Finally, as indicated in Figure 4, we discuss and analyze each security component, assess its impact, and link it to one or more security countermeasures.



*Figure 4: Taxonomy of IoT Security*

**5 Apps**

The Internet of Things will have an impact on a wide range of applications. The scope, scale, heterogeneity, repeatability, and user participation of applications are all considered when categorizing them (Gubbi, Buyya, Marusic, and Palaniswami, 2013). As indicated in the IoT security taxonomy, there are a variety of security techniques available. Authentication, (ii) Authorization, (iii) Resource Exhaustion, and (iv) Trust Establishment are the most often utilized security strategies that are examined with the use cases in this application domain.

**Authentication**

Authentication permits the integration of numerous IoT devices and their deployment in diverse smart environments, such as smart cities, in the IoT application domain. (Martn-Fernández, Caballero-Gil, and Caballero-Gil, 2016). A smart environment can incorporate a variety of services provided by multiple businesses, as well as scaled to support many users in a secure and distributed manner. Before exchanging route information, routing peers of connected IoT devices must validate each other (known as peer authentication), ensuring that the source of the route data is the connected peer devices (known as data origin authentication). This validation contributes to the enhancement of M2M communication, which is a key component of the IoT goal (Perera et al., 2014). Framework responsiveness in the IoT refers to a wide range of methodologies and middleware solutions that make M2M communication simple.

Gubbi et al. (2013) worked on a standard authentication mechanism for the Internet of Things (IoT) that would work across multiple levels and terminal nodes. Hashing and element extraction are used in the scheme. To avoid jamming attacks, the extracted element is shared with the hash function. This approach provides a secure authentication solution for IoT devices. The extraction technique includes various lightweight irreversibility properties that ensure the security of linked items in the IoT realm. The system focuses on the authentication process between distinct IoT layers that provide data to terminal nodes, rather than the other way around. The assertion that the method would improve data security was based entirely on theory, with no practical evidence to back it up.

For the Internet of Things, Ndibanje et al. (2014) presented a security study as well as authentication and access control improvements. Their research focused on deconstructing current authentication and access control systems and proposing a workable protocol for the Internet of Things. To improve device A key establishment technique based on Elliptical Curve Cryptography (ECC) was used for authentication. It was simple, efficient, and secure. Role-Based Access Control (RBAC) was also established for the access control policy for applications associated with the IoT network.. Nonetheless, because the communication cost for IoT sensor nodes was significant, practical trials on the suggested security valuation, no tests were performed.

Abdull gazil. (2016) proposed a security study, while Ye et al. (2014) presented an effective authentication and access control method. Their approach was founded on a thorough grasp of the IoT perception layer's security problems. This method generates an ECC-based session key, which improves mutual authentication between the user and sensor nodes. This solution, however, only addresses the authentication difficulties in the IoT perception layer, not the device access control policy based on attributes.

Ndibanje et al. (2014) provided a security analysis, and Ye et al. (2014) presented a reliable authentication and access control mechanism. Their strategy was founded on a thorough grasp of the security issues that exist at the IoT perception layer. This method creates an ECC-based session key that enhances mutual authentication between the user and sensor nodes. However, this method only tackles the authentication issues at the IoT perception layer, not the attribute-based device access control policy.

* The ECC-Diffie–Hellman technique is used to generate a secret key during the key generation phase.
* Establishment phase: After generating the secret key, this phase entails establishing the device's identity. Either a one-way or mutual authentication mechanism is used to establish identity.
* The third phase, implementation, gives authenticated devices permission to communicate with one another.

Although the concept does not eliminate DoS attacks, it does lessen the risk by granting resource access to only one ID at a time.

To secure RFID tags, Al-turjman and Gunay (2016) proposed a lightweight authentication protocol. Devices such as RFID and sensors are used in the IoT's perception layer. The computing capability of these devices is limited due to their constraints. These qualities make it difficult to apply any cryptographic techniques to ensure the security of IoT networks. When RFID is unsecured, an attacker can quickly get network access by sniffing and reprogramming the victim's electronic product code tag. By using an authentication mechanism on the tags, this attack can be averted. With minimal processing overhead on the devices, the authentication protocol ensures integrated authentication between RFID readers and tagged products.

**Authorization**

Authorization refers to the process of defining access rights to resources, such as medical devices, in terms of information security and access control. The interconnection of micro nodes built using sensing (detecting) and actuating (activating) capabilities placed inside or outside the human body underpins e-health. E-health apps are connection-aware, dynamic, personal, and trust-based.

Only authorized users should have access to the information. Humans, machines, services, internal objects (i.e., devices within the network), and external objects can all be users in the IoT. (i.e., devices outside the network). Sensors, for example, should not reveal acquired data to an unauthorized nearby node (Abdmeziem and Tandjaoui, 2015 and Aazam et al., 2016). How data is managed and controlled in a heterogeneous IoT context is another authorization issue that must be addressed. Users of the Internet of Things should be aware of the data management techniques that will be used, as well as the procedure or administration, and ensure that the data is protected throughout the process (Moosavi et al., 2015).

ID authentication at IoT sensor nodes was proposed by Gaur et al. (2015). The method used was a one-time encrypted request–reply scheme. When many parties are communicating, the technique employs a pre-shared matrix and a dynamic variable cipher. The communication parties generate a random coordinate that will be used as the key (or password) coordinate. Every message (communication) between parties is encrypted with a key and node ID, as well as a timestamp. The communicating parties authenticate each other's timestamps, and they can also use the timestamp to end a session. However, because the key can be rehashed for other locations, this strategy is only effective in an IoT area where safeguarding items is not extremely delicate and important. If the password is updated on a regular basis, the security of that IoT framework may be improved. For this work to be deployed in many IoT devices, the formation of the pre-shared matrix must be secure.

**Exhaustion of Resources**

The rising demand for ubiquitous resources such as energy sources can add to present system resources and have a significant impact on the performance of various applications, resulting in resource leakages and overloading in the IoT. (Borgia, 2014). According to Bekara (2014), resource-exhaustion vulnerability is a form of flaw that causes the undefined or wasteful consumption or allocation of resources, or the inability to release them when they are no longer required, resulting in their depletion.

By establishing routing loops and lengthening the path during packet transmission, resource depletion attacks sap the energy of target IoT nodes. Resource depletion attacks are a threat to routing protocols (Raju, 2014).

Resource exhaustion can also occur when an attacker sends out copious amounts of packets from one or more attack nodes on a regular basis. All sensor nodes within the transmission range of the assault nodes are potential targets in this situation, and their batteries are intentionally depleted. If the attackers' packets elicit a transmitted response time from the target nodes, battery depletion is hastened. When the destination nodes opt to transmit the packet to other nodes in the WSN, for example, this deterioration occurs. Because more sensor nodes become unavailable at the same time and the nodes may be separated into sub-networks that cannot communicate with one another, resource exhaustion attacks are more severe than other DoS assaults (Botta et al., 2016).

**Trust Establishment**

To build trust between IoT physical items and events, such as networked WSNs, RFID-based devices, and mobile phones, a credible trust mechanism must be offered (Akhunzada et al., 2016). The application server can be hacked, exposing sensitive user information, and allowing for the forgery of authentic user credentials on the network. There are mechanisms in place to check network devices. However, there are no plausible ways for building confidence in network application verification. As a result, establishing trust is critical for proper device interoperability. The preservation of user privacy, such as personal user data, by policy and prospect of IoT users in a flexible manner is what trust entails What trust entails is the protection of user privacy, such as personal user data, through policy and the prospect of IoT users in a flexible manner. Because IoT devices are portable and movable in nature, they can be physically moved from one owner to another. As a result, trust must be created between both parties for the devices to travel smoothly in terms of access monitoring and permission. By constructing an item-level access-control architecture, Atzori et al. (2010) established a paradigm of mutual trust in system security in the IoT. During data transfer, the framework creates trust among linked IoT devices. In this architecture, the authors employed key creations and tokens as techniques for creating trust. By providing creation keys and tokens to IoT devices during data transfer, the processes ensured that communicating devices were authorized.

**Architecture**

There is currently not widely approved IoT architecture (Chen et al., 2011). In terms of authentication and authorization, several sorts of study have been undertaken on the IoT architecture in various scenarios and application domains.

**Authentication in Internet of Things (IoT) architecture**

Vesako l. (2017) used the SDN architecture to assist traditional networks become less inflexible. SDNs give system managers a global view of the system and the capacity to govern the network based on the needs of each company. By delivering programmable network services, SDNs simplify network consumption and operation while lowering the total cost of enterprise networks. SDNs, on the other hand, have several security flaws. Because of the lack of comprehensive authentication and authorization systems, SDN controllers are a primary target for hackers, as they serve as both the network's center point of control and the potential crucial point of calamity. For IoT-based health-care systems, Moosavi et al. (2015) presented an Architecture for a distributed smart e-health gateway. This architecture uses the certificate based DTLS handshake protocol, which is the basic IP security solution for the IoT.

This design may adapt to a variety of security issues in general healthcare systems, including scalability, trust, and consistency. DoS attacks are one flaw in the suggested architecture. The IoT heterogeneous medical domain, for example, is a scenario in which the functionality of an IoT-based healthcare system is delegated to a centralized server. A DoS attack on the server can quickly compromise it, allowing an attacker to view and recover all stored data in the confined medical domains. Another disadvantage in IoT-based healthcare applications is the issue of privacy. Because of the security level requirements, the approaches used in the proposed architecture do not support the privacy assurance re-used on constrained devices.

Ramo et al. (2015) focused on establishing a type of traditional security architecture for SOA-based IoT middleware systems that allow heterogeneity and interoperability of IoT devices, as well as information management and security. SOA-based procedures also enable an identical and well-organized reflection of services and communication with IoT devices for IoT applications. SOA-based techniques provide the confidentiality, integrity, and safety of communication channels by providing a standard and controlled abstraction of services between IoT devices.

**5.2.2 Authorization in the IoT architecture**

In the IoT architecture, authorization is achieved by exchanging identifying data between connected objects. This technique is vulnerable to eavesdropping, which could lead to identity theft a Man-in-the-Middle (MitM) attack, putting the IoT framework at risk (Sezer et al., 2013 and Karlof, 2013).

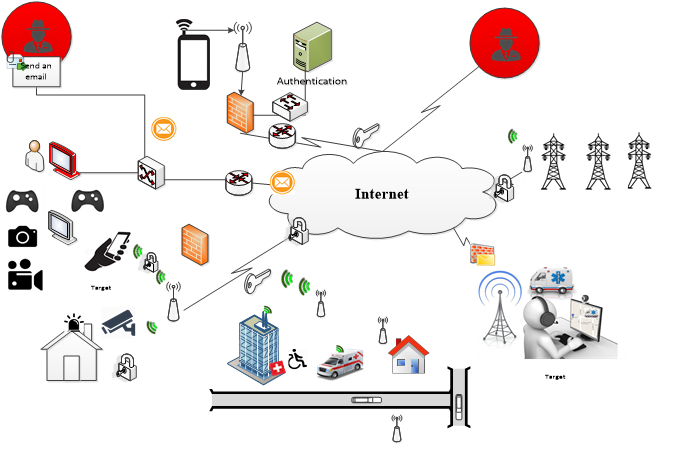
OSCAR was proposed by Vucinic' et al. (2015) for E2E security in the IoT. OSCAR was tested in two ways: (1) on two distinct hardware types using 802.15.4 LLN and M2M communication, and (2) on a real testbed using MAC layers and the Cooja emulator. Authorization servers are used in this architecture type to provide users access, allowing them to request resources from the CoAP nodes. Multicasting is supported by OSCAR's security function. This functionality allows for E2E security authorization. However, one disadvantage of this framework is the ECDSA (Elliptic Curve Digital Signature Algorithm) authorization latency, which has a significant impact on the microcontroller unit and compute capacity of IoT devices. Unauthorized users can take control of the entire system in this circumstance.

# **Communication**

Information is exchanged/shared among IoT devices or between different IoT layers in IoT communication. Despite the IoT's immense promise in many sectors, the entire IoT communication infrastructure is insecure and open to privacy breaches from the perspective of end users (Hashem et al., 2016). For attackers, the IoT communication medium serves as a decision point. The following are the probable assaults in the channel.

**6 IoT security scenario**

We all know that security and privacy issues must be addressed before IoT can be fully adopted in a variety of areas on a large scale, as indicated in the preceding sections, based on a comprehensive investigation and survey on the security threats and vulnerabilities of the IoT Due to the multiplicity of technologies and communication standards, there is currently no common standard policy for security and privacy demands in the IoT context (Chen et al., 2011). A well-defined security and privacy policy is required to maintain confidentiality, access control, and privacy for people and products. created and implemented. We suggest a conceptual form of architecture that can assist minimize the security difficulties posed on products, given the security flaws and lack of standards in the IoT environment.



*Figure 5: IoT security scenario.*

Figure 5 depicts an IoT security scenario in which various devices and sensors communicate securely with one another. A virtual healthcare system is used to demonstrate how different users communicate with one another. Let us say a user with a healthcare gadget is at home and must contact a hospital for help. Because of his or her health condition, the user is unable to visit the hospital to see a doctor in person. To minimize the stress of traveling to the hospital, the user just calls or sends an email to the hospital from home. As shown in Figure 5, the home and hospital networks are made up of a variety of sensors and wireless devices.

As indicated in Figure 5, the user's mobile device and information, as well as hospital information that uses many networks and equipment, are left open or accessible to hackers. Aside from the security features present in current networks, the security requirements for resource-constrained devices during communication must be prioritized. Current networks, on the other hand, are unable to meet the security needs of sensitive data applications. When creating the security architecture for restricted devices, network and device security are two significant needs that must be considered (Akhunzada et al., 2016). In IoT scenarios, new network service requirements are linked with individual wireless devices that interact with the Internet, collections of wireless devices, ubiquitous systems, and sensor networks (Gaur et al., 2015). As a result, a secure form of IoT architecture must be designed to meet the security standards of emerging network services.

# **7 Future Directions**

Many security, trust, and infrastructure issues confront IoT development. For IoT to be accepted and fully adopted, the hurdles must be overcome. The majority of IoT devices are wireless, hence protecting them is critical. Because security issues can emerge at multiple stages in the IoT, they are critical. For the complete IoT system to be secure, Confidentiality, integrity, authentication, authorization, non-repudiation, availability, and privacy are just a few of the security aspects that must be assured. Because of the IoT's ambient characteristics, this goal is particularly difficult to achieve.

**Challenges in the Field of Security**

Security considerations mentioned in this section include secure SGs (smart grids), lightweight authentication, heterogeneity, and quality of service.

**Secure SG (smart grids)**

Azul kina (2018) presented the SG security to investigate the security difficulties and challenges in IoT-based SGs, as well as to outline the most important security services to consider. However, no comprehensive study on the SG's major security component, the secure integration of energy-aware smart homes, has been conducted, leaving end-users vulnerable to security threats and attacks. When using smart meters/smart appliances, these threats and assaults include impersonation/identity spoofing, data manipulation, and illegal control access. An in-depth investigation of the key security element of SGs, as well as the integration of a secure energy-aware smart home, are required prior to the deployment of smart meters/smart appliances, is required. Such research could aid in reducing the susceptibility and security risks associated with smart meters and smart appliances. Gupta and Garg (2015) proposed mobile IoT applications with cloud techniques such as mobile sensor data processing engine, mobile fog, Embedded Integrated Systems (EIS), Mobile Sensor Hub (MosHub), and dynamic configuration that uses MosHub to demonstrate the different techniques used in mobile IoT applications and the cloud. They compared approaches and created cloud IoT by combining IoT applications with mobile phones and cloud computing. Because of the nature of IoT devices, an increase in the number of sensors attached to a device or an increase in GSN query demand has an impact on CPU, memory, and energy consumption.

**Lightweight Authentication**

To solve data security and privacy challenges, Yao, Chen, and Tian (2014) introduced a lightweight no-pairing Attribute-Based Encryption (ABE) technique based on ECC. In the IoT, their technique reduces processing and communication overhead. ABE, on the other hand, has limited scalability and is inflexible when it comes to revoking attributes, therefore it cannot be used in multi-authority systems. As a result, a lightweight multi-authority-oriented ABE must be designed, as well as a flexible attribute revoking method. In a distributed IoT application, Perera et al. (2014) suggested a ubiquitous lightweight verification mechanism for WSNs. To test the security performance of WSNs, the DTLS protocol is used to do a security analysis on the PAuthKey. They created the PAuthKey protocol and demonstrated its capabilities on sensor nodes with limited resources. Due to network heterogeneity and device mobility, the distributed IoT has faced numerous security threats and difficulties, including access control and multicasting. As a result, security protocols that can handle threats in distributed IoT network applications must be established, as well as an implicit certificate scheme for access control and large-scale multicasting.

Bose et al. (2015) and Raza et al. (2013) provided a lightweight system for secure channel formation that controlled the level of confidentiality, evaluated a security score using fine-grained sensor data, and preserved and protected material via a secure transfer. A simple security method can support and measure the sensor dataset's private value (i.e., how it affects the secrecy connection) (i.e., data in smart meters). However, such a technique can only evaluate a single security scenario (i.e., sensitivity), as well as how to extract sensitivity analysis and privacy degree from multivariate data. It does not consider multidimensional sensor data. To expand the concept to additional IoT instances, such as intelligent transportation, an algorithm that can extract sensitivity analysis and privacy measures based on multivariate and multidimensional sensor data must be built.

**Heterogeneity**

Because each linked item has a distinct security mechanism, the IoT has become heterogeneous in nature, making it more vulnerable to attackers (Srivastava and Garg, 2015). Memory, energy usage, bandwidth, and style of implementation and communication are all inconsistent with constrained devices. Obtaining secure E2E communication is a challenging task that typically necessitates the customization of current solutions or the use of gateways (Bekara, 2014).

Aazam et al. (2016) proposed resource estimate and management that uses fog computing for a customer's Probabilistic Resource Estimation (PRE) model to execute IoT resource management that is well-organized, successful, and reasonable. However, due to the heterogeneous devices that make up the Internet of Things, quantifying the number of resources consumed by each node and evaluating whether the requesting nodes or devices would completely utilize the resources requested is difficult. Obtaining low latency with devices such as healthcare and emergency services is extremely difficult due to the unreliable core network of accessing the cloud through shared resources. As a result, testing for minimum latency necessitates using the model in other areas of research, such as smart cities, medical centers, and smart homes. In addition, Sicari et al. (2015) investigated the available solutions in the IoT arena for security (i.e., reliability, secrecy, and verification), privacy, and trust. However, the authors' solutions do not describe the privacy policies that can govern the adaptation of IoT devices in a diverse context.

Calvin is a framework developed by Persson and Angels mark (2015) that uses a single programming model to integrate the IoT and the cloud. This framework aims to create a solution that allows developers to take advantage of heterogeneity in the IoT rather than avoid it by obscuring protocol and data transport characteristics. By avoiding a direct device-to-cloud client/server approach, it also improves communication efficiency. Calvin is currently in its initial stages of development due to the framework's hybrid nature. There has not been a single implementation that anticipated all the security and routing aspects required for autonomous migration in an IoT distributed context.

In the framework of the Internet of Things, Li, Han, and Jinn (2016) proposed a feasible access control for sensor networks. In this innovative Heterogeneous Sign Crypton, the senders are part of the Certificate-Less Cryptography (CLC) environment, while the receivers are part of the Identity-Based Cryptography (IBC) environment. This method is distinguished by its variability. The senders and recipients are from two separate cryptographic environments. It allows a message to be sent from a sender in the CLC environment to a receiver in the IBC environment. Furthermore, because of the ciphertext authenticity of this solution, the computational expense of the sensor nodes can be shifted to the gateway. The use of certificates is not required by CLC. However, it still necessitates the employment of a trusted third party, the Key Generating Center, to generate a partial private key based on the user's identification and a passkey. They also concentrated on the sensor node's computational cost and energy usage.

**QoS (quality of service)**

The core capability for routing data in re to allow data to be routed in resource-constrained devices source-constrained devices to allow differential delivery and ensure excellent service is the QoS design. Several techniques have been proposed to improve services in restricted nodes and to ensure that constrained devices receive appropriate QoS. Adaptive edge (fog) computing solutions for IoT networking at the network edges, based on Jutila (2016)'s REgressive Admission Control (REAC) and Fuzzy Weighted Queuing (FWQ) with adaptive computing approaches, that may be used to optimize and control traffic flows and network resources, are among the solutions. The FWQ control with feedback provides qualities such as system stability, low settling times, and quick response time. At the network edge, REAC aids in the management of E2E network performance. However, the methods only address one QoS measure (network capacity) and ignore other QoS issues like connectivity, dependability, and delay. To avoid network congestion, the operating capacity (IEEE 802.11p) must completely support two instances of Roadside Unit (RSU) deployment. However, it only allows for the deployment of one RSU, which causes network congestion. As a result, solutions that address interoperability concerns as well as unsolved QoS metrics like connectivity, dependability, and delay are necessary.

Chakrabarty et al. (2015) also proposed a black SDN, which encrypts the header and payload at the network layer to improve security. This method can protect IoT networks from a variety of threats while also increasing their overall lifespan and network performance. IoT nodes with limited resources are unable to support a full SDN implementation and are unable to address the security of the black link layer frame. The black network is an application delivery network that secures all data, reduces network efficiency, and complicates routing. As a result, sleep synchronization mechanisms tailored to black networks are necessary to ensure packet delivery to all nodes and several methods of securing the black link layer frame. This method enables a fine-grained approach to meta-data security. These methods include 1) replacing meta-data fields with Grain-128a IV and a keystream, 2) using AES-EAX mode, and 3) using a pre-shared IV to improve payload efficiency.

Homg et al. (2011) presented the Adaptive Weighted Fair Queue (AWFQ) adaptive bandwidth allocation algorithm for reservation protocols to enable QoS on the IoT network layer. The proposed algorithm uses queue status and priority assignment to govern bandwidth sharing across different Internet services and ensure that resource-constrained devices receive a predetermined QoS policy. The algorithm is mostly concerned with bandwidth usage (i.e., how network bandwidth is effectively and efficiently utilized among resource-constrained devices in a flexible, fair, and prioritized manner). Despite this, the issue of bandwidth scarcity on resource-constrained devices with low priority and queue congestion has not been solved.

**Trust Management**

On the Internet of Things, the privacy of nodes and users is critical, and it must be considered while creating IoT devices. The preservation of user privacy, such as personal user data, by the policy and prospect of IoT users in a flexible manner is what Trust Management (TM) entails. As a result, TM must be integrated into IoT RFID devices. Furthermore, TM occurs not only when readers and RFID tags communicate, but also when readers and base stations communicate. In the TM domain, digital signature technology is used; it is significant in the trust area because it is used for authentication (both on IoT devices and data) and data transmission between different IoT applications. (Jing et al., 2014). However, few research types on TM in the IoT domain have been performed.

TM seeks to address security challenges in a distributed system (Gu, Wang, and Sun, 2014). Trust is a dynamic concept that can protect existing IoT architecture while also providing a consistent decision-making strategy for IoT heterogeneous environments or multi-domains. As a result, Josang, Ismail, and Boyd (2012) examined TM as a potential solution to IoT security challenges. Because different network nodes have different trust criteria, addressing and computing the trust between different networks in the heterogeneous IoT is a challenging task. TM is a useful tool for analyzing the trustworthiness of IoT entities and assisting users in making informed decisions while communicating and cooperating with one another.

The technologies for regulating heterogeneous linked devices in the IoT were the focus of Liu and Wang (2010) and Yan, Zhang, and Vasilakos (2014). Their research centered mostly on a heterogeneous network model, trust directing, and TM technology. Their research points to the right way for future IoT device development. However, in the IoT arena, real-world solutions for TM are required.

The intricacy of trust relationships among varied entities was explained by Chen et al. (2011). Based on various practical trust-based concepts they gathered, they examined the security difficulties and threats offered by the IoT. After that, they presented a security IoT architecture.

Unlike Liu and Wang (2010) and Yan, Zhang, and Vasilakos (2014), who only offered a few non-practical ideas for dealing with trust in the IoT, Bahtiyar and alayan (2012) proposed a trust model that focuses on extracting trust data and providing formal security policies for IoT devices/entities as needed. They aimed to offer an organization with a defined security policy on how to extract trust data from a secure system for service. However, to analyze the authentication of the parameters used and decide how it might be deployed in the IoT, no specific network architecture has been addressed in this model.

Yan, Zhang, and Vasilakos presented Autonomic TM (ATM), which gives perfect benefits and reliably supports Human–Computer Interaction (HCTI) (2014). Trust, on the other hand, has a broader scope than security. As a result, it is difficult to construct, guarantee, and maintain. Because different network nodes have varied TM requirements, disseminating and enumerating trust throughout multiple networks in a heterogeneous IoT is a challenging task. Similarly, ATM is challenging to implement because the cloud of things' deployment, mobility, and low computation capacity are difficult to regulate. Improvements in performance, such as the most efficient technique for key dissemination, how to create lightweight security and preservation solutions, and how to avoid complex and energy-intensive cryptographic controls, all remain significant risks. As a result, lightweight security, and trust components for the IoT that can be deployed on small items must be created, with a focus on mitigating probable DoS or DDoS attacks.

In addition, Sicari et al. (2015) investigated the available solutions in the IoT arena for security (i.e., reliability, secrecy, and confirmation), privacy, and trust. The future communication between two devices will be supported by the trust connection between these devices. If these devices trust each other, they can always exchange resources. They did not, however, address the creation of a trust negotiation tool capable of handling data streams, access control, and a single vision for ensuring security and privacy in such heterogeneous environments. Different technology and communication criteria are used in this strategy. As a result, well-defined privacy regulations addressing scalability and adaptive infrastructure capable of managing security threats in a dynamic IoT environment must be built.

Much research on TM for the IoT has lately been done, and various trust models have been proposed (Lopez et al., 2010 and Gu et al., 2012). These trust models could be included in the IoT TM development. There has been no associated work that develops a trust mechanism disclosed, so this is still an open issue for the IoT.

**Infrastructure**

This section discusses numerous infrastructure concerns, including SDN, smart e-health, and middleware. Because there is no uniform IoT infrastructure, IoT devices are exposed to assaults and threats (Chen, Lai, and Wang, 2011).

**SDN**

Chakrabarty, Engels, and Member (2016) developed a secure IoT architecture for smart cities that tackles traditional IoT system vulnerabilities. A black network, trusted SDN controller, unified registry, and key management system is the four core IoT architectural pieces for securing smart cities. Confidentiality, integrity, privacy, secure routing (black packets), route availability, identity management, node authentication, authorization, availability, efficient key distribution, and secure use of symmetric keys by authorized devices are all provided by the IoT architectural blocks. Chakrabarty and Engels, on the other hand, did not focus on IoT security architecture or SDN deployment. Because the SDN architecture modifies the IoT network's communication patterns, this situation results in new attack types, necessitating an innovative approach to secure the IoT network. Encrypting the header causes routing issues for IoT nodes, which are frequently sleeping. As a result, sleep synchronization protocols appropriate for black networks must be established and constructed to assure packet delivery to all nodes, as well as a secure form of IoT architecture that can help address translations, specify location privacy, and characterize mobility. Jararweh et al. (2015) developed a software-defined framework model (SDIoT) to improve IoT management and give a fundamental solution for vulnerabilities in traditional IoT architectures by forwarding, storing, and safeguarding data generated by IoT objects. A SDN, SDStore, and SDSec are all combined into a single software-defined control architecture in this manner. As a result of the SDIoT framework, IoT control and management procedures are accelerated and simplified, and traditional architecture challenges are addressed. By producing segments/fragments and permitting transparent information flow, this framework also allows cloud users to make the best use of cloud resources. Despite this, there are still concerns with SDN compatibility, security, and interoperability. There is no realistic and experimental SDIoT framework for testing various IoT topologies. As a result, an SDIoT framework is needed to examine various forms of IoT topologies that can handle security and interoperability challenges in the SDN.

**Smart e-health**

Moosavi et al. (2015) used a distributed smart e-health gateway architecture to establish a secure and efficient type of verification architecture for IoT-based healthcare systems. Due to its dispersed nature drawn from the end-user, the gateway might be misused on medical sensor nodes. Is a gateway also capable of adapting to many challenges in pervasive healthcare systems, such as scalability, security, and dependability? Abuse or privacy issues may deter the general population from using IoT-based health-care systems. Because resources constrain the security level needs and framework design of IoT-based healthcare applications, traditional security, and privacy mechanisms, as well as current cryptographic solutions, secure protocols, and privacy assurance, cannot be utilized. To mitigate hazards in the architecture, secure network infrastructures for short- and long-range communication are necessary.

Gaur et al. (2015) proposed using semantic web technologies and the Dempster–Shafer uncertainty theory to enable communication between WSNs and ICTs (Information and Communication Technologies) in a smart city setting. This architecture type assists Alzheimer's sufferers and the elderly with daily breathing exercises by delivering reminders to users when they forget or are unable to complete them. By connecting information from many smart city sectors, this framework can also act as a smart platform for individuals who live in a smart society. The proposed architecture, on the other hand, cannot cover a huge area and has yet to be tested. As a result, an architecture type must be established that can span a full city without ignoring any area and conduct tests on the concept mentioned.

**Middleware**

Ramo et al. (2015) looked at the benefits of establishing a well-defined standard security architecture for SOA-based IoT middleware, as well as the current research efforts. They also detailed the security facilities that may be used to reduce security concerns in SOA-based IoT middleware frameworks while creating the IoT security architecture. SOA-based techniques also give an inflexible and ordered reflection of security facilities required for item communication in IoT applications (i.e., IoT devices). These methods aid in system interoperability and provide system services based on devices that are used by applications. However, the combination of SOA (Service Oriented Architecture) and resource-oriented architecture (ROA) introduces a new set of traditional security requirements that must be met in resource-constrained contexts to ensure system safety. None of the studies described above proposed solutions that addressed all the middleware security concerns. To defend IoT middleware from assaults, a security countermeasures system in the middleware architecture must be established.

Furthermore, Vucinic' et al. proposed OSCAR with CoAP (2015). OSCAR is an E2E security middleware architecture for the Internet of Things. In two hardware settings and MAC layers, OSCAR was tested in two scenarios: 802.15.4 LLN and M2M communication. Multicasting, asynchronous data transfer, and caching are all supported by this method. With the basic DTLS approach, it handles security and permission issues in E2E while maintaining full data integrity. Failure of the node that functions as a PAN coordinator in a beacon-enabled 802.15.4 network, on the other hand, disrupts the network's periodic beacon transmission. Once the information in the CoAP header is gone, existing solutions are unable to recover lost keys. Zhao and Ge (2013) presented a solution to various IoT security challenges that arise in a three-layer system architecture, as well as the essential technologies involved. Security issues were discovered in every stage of the IoT architecture, including the perception, network, and application layers, according to their research. RFID, ZigBee, and all sensor kinds are among the key pieces of equipment in the perception layer. Attackers can easily obtain access to the hardware, control it, or physically hurt it. The network layer of the Internet of Things is prone to security flaws. For diverse sectors or contexts, heterogeneity reduces network security, interoperability, and coordination. The application layer has its own set of security challenges, making security more complicated and difficult. There has yet to be established a uniform IoT security architecture. As a result, data security necessitates encrypting the RFID signal using an appropriate method. Furthermore, for several types of network topologies, a precise unified authentication method, E2E authentication, key agreement mechanism, Public Key Infrastructure (PKI), wireless PKI, security routing, and intrusion detection must be set up.

# **Conclusion**

The Internet of Things (IoT) has lately gained popularity as a research topic. It allows different sensors and equipment to communicate with each other without the need for human involvement. Furthermore, the requirements for large-scale IoT deployment are fast growing, with considerable security issues. We provide a thorough overview of the most recent IoT security risks and vulnerabilities. We classified the Internet of Things (IoT) by offering a taxonomy of existing security threats and vulnerabilities in relation to its application, design, and communication. We also talked about the most up to date IoT-enabling connectivity technology. We also offered a possible IoT security solution structure to address security concerns in the IoT environment. Finally, we discussed open research questions and IoT security difficulties. However, IoT security research is still in its initial stages and has yet to be put to the test (Gaur et al., 2015). For the IoT to be completely adopted by users, workable solutions to the discussed security threats and weaknesses must be implemented/applied.

**Reference**

1. Aazam, M., St-Hilaire, M., Lung, C.-H., and Lambadaris, I. (2016). PRE-Fog: IoT trace based probabilistic resource estimation at Fog. *2016 13th IEEE Annual Consumer Communications and Networking Conference (CCNC)*, 12–17.
2. Abdmeziem, M. R., and Tandjaoui, D. (2015). An end-to-end secure key management protocol for e-health applications. *Computers and Electrical Engineering*, *44*, 184–197. http://doi.org/10.1016/j.compeleceng.2015.03.030
3. Akhunzada, A., Gani, A., Anuar, N. B., Abdelaziz, A., Khan, M. K., Hayat, A., and Khan, S. U. (2016). Secure and dependable software defined networks. *Journal of Network and Computer Applications*, *61*, 199–221.
4. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of things: A survey on enabling  technologies, protocols, and applications. *IEEE Communications Surveys and Tutorials*, *17*(4), 2347-2376.
5. Al-turjman, F., and Gunay, M. (2016). CAR Approach for the Internet of Things Approche de la CAR pour l’ internet des objets. *Canadian Journal of Electrical and Computer Engineering*, *39*(1), 11–18.
6. Aman, W., and Snekkenes, E. (2016). Managing security trade-offs on the Internet of Things using adaptive security. *2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015*, 362–368.
7. Atzori, L., Iera, A., and Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805.
8. Babar, S., Stango, A., Prasad, N., Sen, J., and Prasad, R. (2015). Proposed embedded security framework for Internet of Things (IoT). *2015 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless VITAE 2011*, 1–5.
9. Bahtiyar, Š., and Ufuk Çaǧlayan, M. (2012). Extracting trust information from security system of a service. *Journal of Network and Computer Applications*, *35*(1), 480–490.
10. Bandyopadhyay, D., and Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, *58*(1), 49–69.
11. Bansal, G., Kenney, J., and C. Rohrs, C. (2013). “LIMERIC: A Linear Message Rate Control Algorithm for DSRC Congestion Control,” IEEE Transactions on Vehicular Technology, to appear fall 2013.
12. Barreto, L., Celesti, A., Villari, M., Fazio, M., and Puliafito, A. (2015). An Authentication Model for IoT Clouds. *Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015*, 1032–1035.
13. Yao, X., Chen, Z., and Tian, Y. (2014). A lightweight attribute-based encryption scheme for the Internet of Things. *Future Generation Computer Systems*, *49*, 104–112.
14. Ye, N., Zhu, Y., Wang, R. C., Malekian, R., and Lin, Q. M. (2014). An efficient authentication and access control scheme for perception layer of internet of things. *Applied Mathematics and Information Sciences*, *8*(4), 1617–1624.
15. Yinbiao, S., Lee, K., Lanctot, P., Juanbin, F., Hao, H., Chow, B., … Qui, W. (2014). Internet of Things: Wireless Sensor Networks. *International Electronic Commision*, (December), 1–78.
16. Zhao, K., and Ge, L. (2013). A survey on the internet of things security. *Proceedings - 9th International Conference on Computational Intelligence and Security, CIS 2013*, 663–667.
17. Zhu, C., Leung, V. C. M., Shu, L., and Ngai, E. C. H. (2015). Green Internet of Things for Smart World. *IEEE Access*, *3*, 2151–2162.
18. Zhu, S., Setia, S., and Jajodia, S. (2015). LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks Categories and Subject Descriptors. *ACM Transactions on Sensor Networks (TOSN)*, *2*(4), 500–528.
19. Vishvakarma, N. K., James, W., and R.R.K. Sharma. (2015). *Internet of Things Applications - From Research and Innovation to Market Deployment*. *JIMS*, *15*(1), 35–43.
20. Vučinić, M., Tourancheau, B., Rousseau, F., Duda, A., Damon, L., and Guizzetti, R. (2015). OSCAR: Object security architecture for the Internet of Things. *Ad Hoc Networks*, *32*, 3–16.