iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** XII **Month of publication:** December 2023

DOI: https://doi.org/10.22214/ijraset.2023.57760

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XII Dec 2023- Available at www.ijraset.com

Security Issues on Internet of Things (IoT): A Recent Challenges and Countermeasures

Prachi Goel[1], Apurva Jain[2], Deepika Juneja[3]
CSE Department, ADGIPS

Abstract: ***This paper contains a surveyas well as an investigation and examination of the present situation statesecurity for the Internet of Things (IoT). The Internet of Things aims to connect anybody with anything, anyplace. In contrast to the fixed Internet, IoT uses multiple wired and wireless networks to connect a large number of machines, limited-resource devices, and sensors. The realization, network, and application layers are the three hypothetical layers that make up an IoT.The security challenges that exist within and across these layers are described in this study. There are also several security ideas that need be implemented at each tier. Previous work on ensuring security for each IoT layer, as well as related countermeasures, is also examined. Finally, the report discusses potential acquisition strategies.***
Keywords: Integrity, Security, Policies.

I. INTRODUCTION

The Internet of Things (IoT) is a networked collection of connected devices, communication, data, and information-sharing services, people, and devices in order to achieve objectives in a variety of fields and applications. Transportation, energy, healthcare [1], agriculture, generation and distribution, among other things more fields that necessitates things to connect to via the internet execute business assignments without the need for human intervention can all benefit from IoT. Devices that join the Internet of Things often use an Identity Management (IM) solution that allows a set of similar and dissimilar devices to be identified. In the Internet of Things,An IP address is a unique identifier for a device, but each entity inside that geographical area is identifiable by a distinct identifier.In recent years, IoT techniques have witnessed fast expansion, with additional Wireless Sensor Networks [2] and Radio Frequency Identification are two examples of such technologies (RFID) are being released (WSN). The IoT's primary restructuring method is RFID, which qualifies the tagging or labeling of each and every component. Each "thing" (people, equipment, etc.) thanks to WSN, it can become a wirelessly [3] unique object capable of interacting with the use of cyberphysical and digital worlds.
The remainder of this work is organized as follows. The 3-layer IoT framework and architecture are described in Section 2. Section 3 delves into security concerns linked to various security concepts [4] and IoT device features.In this section also discusses the security concerns that each layer of the Internet of Things has. Section 4 discusses recent research initiatives aimed at demonstrating IoT security defenses [5]. Section 5 gives a broad overview of all the IoT security-related research that has been done.In view of the current level of IoT security, Section 6 explores probable future paths. The paper comes to an end with Section 7.

II. ARCHITECTURE

The functions and devices used by each tier in IoT architecture are discussed.On a variety of levels, there are many perspectives on the Internet of Things. There are three layers to the Internet of Things:, network, application and perception.Each tier of IoT security concerns has its own set of rules issues Figure 1. The IoT's [6] three-layer architectural structure, as well as theEach and every layer is surrounded by devices and technologies are described below, is depicted in Figure 1.

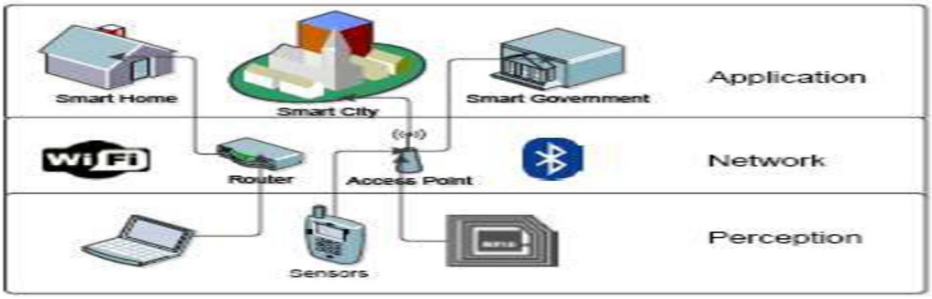


Figure 1: IoT Architecture with 3-layers

A. *Perception Layer*

The perception layer is commonly known as the "Sensors" layer. The actual goal of this layer is basically to gathera couple of data from the environment with the help of sensors. This layer alsocollects monitorsand analyses sensor data before passing it to the network layer. This layer is also capable of connecting IoT nodes [7] in both local and short-range networks.

B. *Network Layer*

The network layer of the Internet of Things handles data routing and communication between different IoT hubs and devices. Internet gateways, switching, and routing equipment, among other things, are found at this layer.WiFi, LTE, Bluetooth, 3G, Zigbee, and other cutting-edge technologies are used to power the system [8] to offer a variety of network services. Network gateways act as a bridge between various IoT nodes by aggregating, filtering, and transmitting data to and from various sensors.

C. *Application Layer*

The application layer ensures the correctness,confidentiality and integrity of the data. At this layer, the goal of IoT in creating [9] smart environments has been completed.

III. MULTIPLE SECURITY ISSUES IN IOT

The same fundamental security objectives of Availability, Integrity, and Confidentiality that should be provided for any interactions involving the use of computers and networks should be provided for IoT security. However, when it comes to components and devices, the IoT has a lot of constraints and limitations computingand energy resources, as well as the diversified and pervasive nature of it, all of which necessitate additional research in order to organize security [10]. This section is divided into two parts: the common security characteristics and the each stratum of the IoT have its own set of security concerns.

A. *Security Features of IOT*

There are two types of security issues to consider: security and technical concerns [11]. The technology problems arise from the diverse and widespreadIoT devices have a unique nature, the complexity of safety is determined by the ethics and utility that must be adhered to in order to build a secure network. Throughout the creation and operation of all devices and hubs, security should be considered. The following are the security principles to follow while creating a secure interaction framework in an IoT [12] for people, software and processes. IoT Security market ration has been displayed in following figure 2.

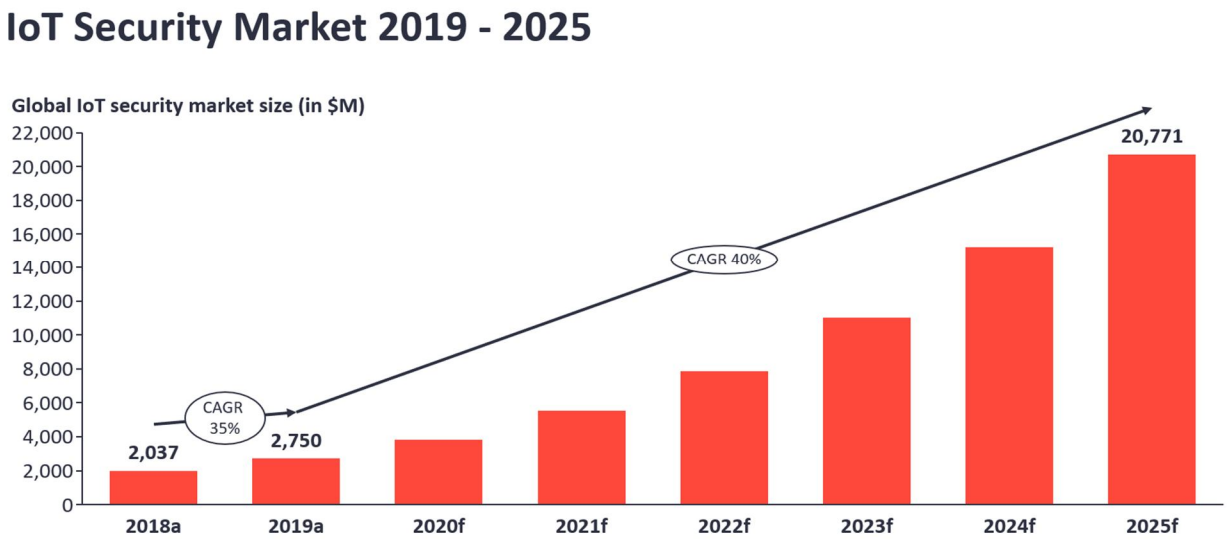


Figure 2: Recent IoT Security Issues in Market Next Five Years

1) Confidentiality-It is critical to ensure that data is secure and that only authorized individuals have access to it authorized personnel have access to it. The Internet of Things is based on the exchange of information and data between various kinds of devices. As a result, it's vital to double-check the data's accuracy, make sure it's coming from the right sender, and make sure it's not being tampered with regard to during [13]the transmissionbecause of the purposeful or inadvertent interference.

2) Availability-The goal of the IoT is used to connect as multiple smart devices as possible.Visitors to the site's Internet of Things should have access to all data at all times. However, data isn't the only component of the Internet of Things [14];If IoT predictions are able to produce data then services and devicesshould be reachable and accessible when required in a timely manner.

3) Authentication-Each and every object should be able to unambiguously identify and verify other objects. However, due of the nature [15] of it, this procedure can be challenging because various entities (Devices, service providers, people, services, and processing units are all examples of processing units) are jumbled up. Furthermore, for the first time, objects may need to converse with other objects (objects they are unfamiliar with). As a result, a technique for mutually authenticating entities in every IoT conversation is necessary.

4) Lightweight Solutions- All of the previously discussed IoT security objectives are not unique, however it is possible to add unique traits and limits to each one of them In however, confidentiality,In generalterms, authentication, integrity and availabilityare taken into account core computer and network security objectives.

5) Heterogeneity- IoT connects a wide range of entities, each with its own level of complexity, potential, and vendors. The devices have a variety of usage of release dates and versions a variety of technical interfaces and bitrates, and are meant for a variety of purposes. As a result, responsibilities must be defined in order to work on a range of devices and in various settings.IoT aims to connect devices, humans, and people, and as a result, it connects a wide range of things and networks. Another issue to consider the environment is important in IoT constantly As a result of alterations (dynamics), A device could be directly connected to an entirely various set of devices at any given time. Furthermore To provide security, an effective cryptography system [16] with suitable Security and key management standards is required.

6) Policies-Regulations and standards must be in place to ensure that data is properly safeguarded, maintained, and transmitted,but, more crucially, a method to carry out such a strategy is required to ensure that every business follows the requirements. Every service that is engaged must have unambiguous Service Level Agreements (SLO). Human consumers will be more likely to trust the IoT paradigm if these criteria are followed, resulting in its growth and scalability in the future. The lots of devices are connected and having policies during the agencies so here we appointed in figure 3.

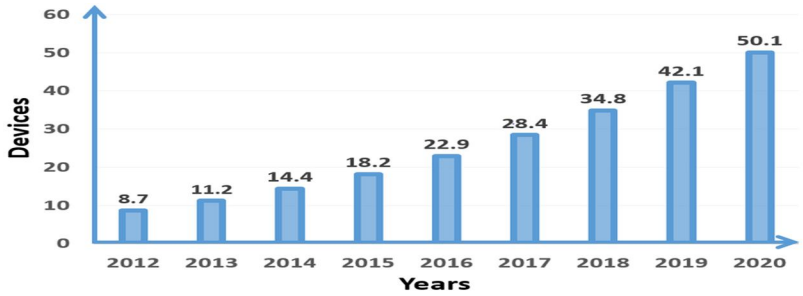


Figure 3: IoT Devices Connected within the policies areas

B. *Security Threats In Each Layer*

Security threats and assaults can be managed at each layer of the Internet of Things. These can be passive and active and they can originate from outside sources or an internal network hacked by an insider. The service is disrupted by the active attack,the differential type, on the other hand, monitors IoT without interfering with network data. A Denial of Service attack [17] against IoT devices and services is possible. (DoS) attacks at each layer, this causes the device to be rendered, users can't access a resource or a network that have been granted access. The security measures are listed in Table 2 issues at each tier, a brief discussion of these concerns is provided below.

1) *Perception Layer.*

The IoT perception layer has three security issues. The impact of wireless transmissions is the first factor to consider. Wireless technology is frequently used to exchange signals between IoT sensor nodes, which could be usefully weakened by convulsing waves. Second, because IoT nodes are frequently used in outdoor and outdoor settings, Physical attacks on Internet of Things sensors and devices are growing concern in devices, the sensor node can be attacked not only by the owner, but also by attackers. Sensorsthe majority of the perception layer is made up of RFIDs, therefore their power, storage, and compute capabilities are severely constrained, making them open to a wide range of threats and attacks.

Replay Attacks, which include faking, changing, or replaying the identification information One of the IoT gadgets, for example, can readily undermine this layer's security confidentiality.Alternatively, in a Timing Attack, The encryption key can be discovered by calculating the amount of time it takes to conduct the encryption. Another threat to confidentiality is when an attacker takes control of anode and seizes all data and information [18];this is referred to as a Node Attack on the capture. By transmitting an attacker can add another node to the network using Malicious Data jeopardizingthe data's integrity in this layer. This may result in a denial-of-service attack sinceit consumes the energy of the system's nodes, preventing them from going into sleep mode.

Encryption can be used to address the above-mentioned security challenges at the perception layer (It might be an end-to-end or a point-to-point connection), authentication (which verifies the sender's genuine identity), and access control Section 4 contains additional security procedures and methods to solve this problem.

2) Network Layer.

At the network layer, DoS attacks can be prevented of the Internet of Things, as previously indicated. The adversary can damage network confidentiality and privacy in addition to DoS assaults through eavesdropping, traffic analysis, and passive monitoring.These attacks are more likely to occur as a result of remote access mechanisms and device data transfer. At the network layer,Attacks by a man-in-the-middle, which may be followed by eavesdropping, are very manageable.The secure interaction channel will be completely weakened if the devices' keying material is intercepted.The key to the Internet of Things is connectivity exchange method To prevent eavesdropping and identity theft, the system must be secure.

3) Application Layer.

In the Internet of Things, there are several security concerns because there are yet no comprehensive policies and standards in place to oversee communication as well as application expansion.Various authentication techniques can be found in various applications and apps, making data privacy and identity identification challenging to achieve through unification of all of them. The high there will be a huge increase in the number of linked devices sharing data increase in the number apps for data analysis, which may have a big impact on the service of availability.

IV. IOT SECURITY REMEDIES

In 2011, Zhao et al. proposed a method for change authentication for IoT systems and terminal nodes. The strategy's bases are hashing and characteristic extraction. The feature based extraction was integrated by the hash function to detect collision attacks. In the IoT, this technique effectively assigns a good authentication solution. The features extraction process is irreversible, which is advantageous in terms of security, as well as It is light weight, which is beneficial in the Internet of Things. When the platform tries to send data to terminal nodes, it encounters problems;the strategy concentrates on the authentication process, not the other way around.While the technique will improve security while reducing data delivery volume, it is purely theoreticalwith no experimental proof of concept to back it up.

In their research, Wen et al. propose a new method for ID authentication at sensor nodes. It's a one-time one cypher based on a request-reply system. For security, creating precise the importance of access restrictions is equal to that of IoT security requires both authentication and encryption, and the two go hand in hand To address these functionalities, Mahalle et al. proposed an Identity Authentication and Capability-based Access Control for the IoT. This study attempts to fill a vacuum in the market for a combined protocol that accomplishes authentication as well as access control inorder to establish reciprocal identity in the Internet of Things. The model employs a public key technique that can be used in conjunction with IoT devices' mobile,lightweight, widely dispersed as well as being computationally constrained characteristics, as well as existing access technologies such as WiMax, Bluetooth, 4G, and Wi-Fi. By encrypting the authentication message between the devices with a timestamp that serves as the Message Authentication Code, it safeguards against man-in-the-middle attacks (MAC).

The method is divided into three stages: first, the Elliptical Curve is used to generate a secret key; second, the Elliptical Curve is used to create a secret key; and third, the Elliptical Curve is used to.The identity is constructed using finally, there are protocols for single-way and mutual authentication, as well as access control is achieved using cryptography and the Diffie Hellman algorithm (ECCDH).

Because elliptic curve cryptography is used, the shared secret key is made up of a public key and a private based parameter, and it is modest in size and computationally cheap (ECC). The entrance is made possible by storing a key. Access rights, a device identity, and a random number are all associated with each IoT device.

Hashing device ID with access rights yielded this random number. In terms of preventing DoS attacks, the IACAC paradigm isn't flawless. However, it reduces it because only one ID can access a resource at a time.

A. Trust Establishment

Because the Internet of Things allows goods or gadgets to physically move from one owner to another, to begin a seamless transition of the IoT device in terms of access control and permissions, trust between the two owners is essential. By offering a framework for item-level access control, in this paper, we provide a common belief for the Internet of Things' inter-system securityIt builds confidence throughout the IoT development, operation, and dispatch phase. The creation key and the token are two methods for establishing trust.

B. Mediated Architecture

It's difficult to keep track of security in the IoT since there aren't any standardized procedures or standards for controlling the design and execution of algorithms.To address the heterogeneity of diverse devices, software's, and protocols, a unified architecture that permits internal autonomy or a centralized unit is crucial for IoT. The study in advocated a clarification for coupled IoT, and a methodology for access control delegation is offered based on that concept. The approach described takes into account the fundamental properties of IoT systems: adaptability and scalability. Another attempt was made to establish a Secure Mediation Gateway framework for critical infrastructures (SMGW). This satisfies an IoT hypothesis because it may be applied to any type of distributed infrastructure that is entirely heterogeneous in nature and function. SMGW can recognize and allocate all suitable information from various nodes, to get around the heterogeneity of heterogeneous nodes, whether they're power, water distribution, or telecommunicationnodes, and they send and receive all messages and data across the untrustworthy Internet network. This research validates the continuation of another federated strategy, In order to develop a Smart Home structure based on the SMGW, which was delivered in. To ensure security, Procedures and standards alone are insufficient in place.It is also necessary to take enforcement measures. To tackle this problem, Neisse ET integrates a security toolkit called SecKitMQ Telemetry Transport (MQTT) is a mechanism for transferring data between MQ servers. Established strategies may not be viable due to the dynamic nature of IoT. The proposed approach mechanism has the potential to improve IoT security, but it increases the duration of the procedure.

C. Security Awareness

Another key security component for the success and extension of the IoT structure is the knowledge and review of human users who are members of the IoT network. The authors used real-world data to show the repercussions of failing to secure the Internet of Things. They were Internet of Things (IoT) gadgets (traffic control devices, web cams, SCADA devices, and printers) had no password or a default password that was open to the public.

The information gathered was fascinating, revealing that many of these technologies were indeed feasible. If people remain unconcerned about security and use the bare minimum of security, such as the default password that comes with the product, the Internet of Things will cause more harm than good. If one of the network's devices isn't secure, hackers will have more opportunities to attack the entire network.

V. THE OVERVIEW PICTURE

The various elements and security integrities stated earlier stress on IoT security,for a long time, the difficulties that IoT security faces have been the topic of several studies.This section evaluates some comparable work as well as the paper's offerings. An in-depth examination of the Internet of Things (IoT) and its security challenges, as well as the need for IoT standards, is discussed in a survey article provided by Roman et al. in. However, no solutions are presented for the security threats that have been identified. Following this, the survey resolution was completed, in which all security threats were addressed and remedies were supplied.

VI. FUTURE DIRECTIONS

During the last few years, In domains including logistics monitoring, environmental monitoring systems telemedicine platforms, and intelligent transportation systems, the Internet of Things has advanced quickly, among others. According to some estimates, by 2020, the total number of things will have risen to 26 billion. However, in order for the IoT to expand and mature, its security vulnerabilities must be addressed.

A. Architecture Standards

IoT now expands a wide range of services, devices and responsibilities to achieve a common goal. However, In order to complete a larger structure, a network of IoT structures must be accommodated from the micro to the macro levels of IoT recognition, a set of criteria must be followed, such as forming a smart town by connecting many smart homes. The Internet of Things now necessitates clearly defined architectural standards,among these are data models. Individuals, devices, languages, and operating systems necessitate interfaces and obligations that can accommodate a diverse set of operating system, humans, devices and many more languages.

B. Identity Management

In this term, the Internet of Things is achieved by exchanging finding information between devices on the first time connection. Overhearing can occur in this phase, resulting in a man-in-the-middle attack posing a threat to the entire IoT infrastructure. As a result, in order to prevent identity theft, some set of identity management entity is required to control the device relationship process using encryption and other techniques.

C. Session Layer

According to most researchers, the 3-layer architecture of IoT does not include the closing,opening and controlling of a session between two items. As a result, there is a need for requirements that may solve these issues while also simplifying device interaction. In IoT design, an abstract session layer should be included as an additional layer to manage the connections, obligations, and sessions between interacting devices.

D. Generation Protocol

IPv4 will undoubtedly fall short of the massive amounts of IP-identifiable items required to implement IoT. As a result, there is a push to implement IPv6, which can support 3.4x1038 devices. However, such a large number of devices will generate a lot of traffic, causing additional delays and necessitating more bandwidth. The 5G aims to deliver speeds of 20-900 Gbps, which is a significant improvement over current technology (4G), which provides speeds of 2-1000 Mbps. The traffic should be handled by 5G generated by IoT devices. IPv4/IPv6 structure translation is intended for use in 5G technology to support both IPv4 and IPv6.

VII. CONCLUSION

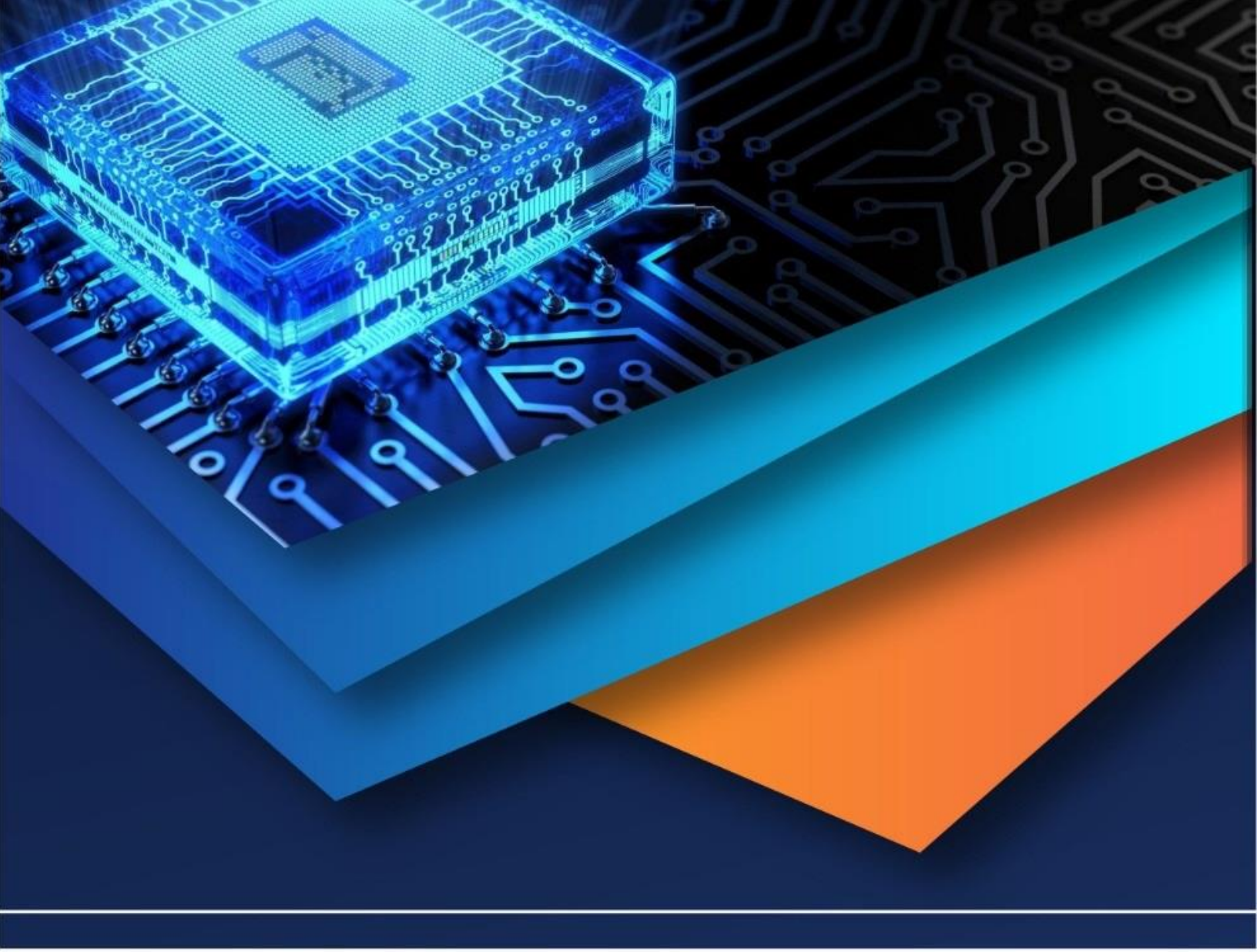
At each tier, the IoT framework is vulnerable to assaults. As a result, several security concerns and requirements must be addressed. Currently, the majority of research is centered on authentication and access control protocol;however, due to the rapid advancement of technology, In a particular sequence to achieve the progressive mash-up of IoT topology, it is becoming increasingly important to consolidate new networking protocols such as IPv6 and 5G.

The biggest IoT advancements are mostly on a small scale, such as within enterprises and in a few niche industries. To scale the IoT structure from a single organisation to a discipline of multiple companies and systems, various security concerns must be addressed. The Internet of Things has a lot of potential to change how we live today. However, security is the most important discipline in recognizing truly smart structures. If privacy, confidentiality, authentication, access control, end-to-end security, trust management, global rules, and standards are completely abandoned, the Internet of Things has the potential to transform everything in the near future. To address the current open research vulnerabilities in IoT, new identification, wireless, software, and hardware technologies, such as device standards, key management and identity setup systems, and trust management hubs, is required.

REFERENCES

[1] Mahmoud, R., Yousuf, T., Aloul, F., &Zualkernan, I. (2015, December). Internet of things (IoT) security: Current status, challenges and prospective measures. In 2015 10th international conference for internet technology and secured transactions (ICITST) (pp. 336-341). IEEE.
[2] Bhabad, M. A., & Bagade, S. T. (2015). Internet of things: architecture, security issues and countermeasures. International Journal of Computer Applications, 125(14).
[3] Yousuf, O., & Mir, R. N. (2019). A survey on the internet of things security: State-of-art, architecture, issues and countermeasures. Information & Computer Security.
[4] Siddiqui, S. T., Alam, S., Ahmad, R., & Shuaib, M. (2020). Security threats, attacks, and possible countermeasures in internet of things. In Advances in data and information sciences (pp. 35-46). Springer, Singapore.

[5] Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials, 22(1), 616-644.
[6] Rajendran, G., Nivash, R. R., Parthy, P. P., & Balamurugan, S. (2019, October). Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures. In 2019 International Carnahan Conference on Security Technology (ICCST) (pp. 1-6). IEEE.
[7] Ghazal, T. M., Hasan, M. K., Hassan, R., Islam, S., Abdullah, S. N. H. S., Afifi, M. A., & Kalra, D. (2020). Security vulnerabilities, attacks, threats and the proposed countermeasures for the Internet of Things applications. Solid State Technol, 63(1s), 2513-2521.
[8] Sarker, I. H., Khan, A. I., Abushark, Y. B., &Alsolami, F. (2022). Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. Mobile Networks and Applications, 1-17.
[9] Sinha, B. B., & Dhanalakshmi, R. (2022). Recent advancements and challenges of Internet of Things in smart agriculture: A survey. Future Generation Computer Systems, 126, 169-184.
[10] Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the Internet of Things in Industrial Management. Applied Sciences, 12(3), 1598.
[11] Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. Computers & Security, 112, 102494.
[12] Rondon, L. P., Babun, L., Aris, A., Akkaya, K., &Uluagac, A. S. (2022). Survey on enterprise Internet-of-Things systems (E-IoT): A security perspective. Ad Hoc Networks, 125, 102728.
[13] Wang, J., Chen, J., Ren, Y., Sharma, P. K., Alfarraj, O., & Tolba, A. (2022). Data security storage mechanism based on blockchain industrial Internet of Things. Computers & Industrial Engineering, 164, 107903.
[14] Gupta, M., Singh, V. P., Gupta, K. K., & Shukla, P. K. (2022). An efficient image encryption technique based on two-level security for internet of things. Multimedia Tools and Applications, 1-21.
[15] Aboamer, M. A., Sikkandar, M. Y., Gupta, S., Vives, L., Joshi, K., Omarov, B., & Singh, S. K. (2022). An Investigation in Analyzing the Food Quality Well-Being for Lung Cancer Using Blockchain through CNN. Journal of Food Quality, 2022.
[16] Wangkhem, K., & Joshi, K. (2018). IoT for Healthcare and Its Challenges. International Educational Journal of Science and Engineering, 1(2).
[17] Diwakar, M., Sharma, K., Dhaundiyal, R., Bawane, S., Joshi, K., & Singh, P. (2021, April). A Review on Autonomous Remote Security and Mobile Surveillance Using Internet of Things. In Journal of Physics: Conference Series (Vol. 1854, No. 1, p. 012034). IOP Publishing.
[18] Paulraj, G. J. L., Francis, S. A. J., Peter, J. D., &Jebadurai, I. J. (2018). Resource-aware virtual machine migration in IoT cloud. Future Generation Computer Systems, 85, 173-183.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY