Quest Journals
Journal of Software Engineering and Simulation
Volume 9 ~ Issue 4 (2023) pp: 30-39
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

Review of Security of Internet of Things (IOT) Devices

Helly Mavani[1] , Ayush Raj[2] , Anusha Seshadri[3] , Chandra Mohan B.[4,*]
[1-3] *UG Student, SCOPE,VIT Vellore, India*
[4,*] *Associate Professor (Senior), SCOPE, VIT Vellore, India*

Abstract:
With IoT devices in our homes, places of employment, and public areas, the "Internet of Things" (IoT) has cemented its place as an integral part of our everyday lives. The growth of IoT devices, however, has also given rise to significant security concerns that require resolution. This study offers a thorough examination of IoT security, including numerous aspects and areas. The article starts out by going through the distinct security difficulties that various IoT device types, including sensors, actuators, gateways, and edge devices, provide. The risks of data breaches, denial-of-service attacks, and device hijacking are examined for each type of IoT device. The evaluation also investigates the safety of IoT networks and communications. It examines the various IoT network topologies and the security threats they provide, as well as the various communication protocols in use and any potential security flaws they may have. It also looks at the function of VPNs, firewalls, and other network security solutions in defending IoT networks from cyber-attacks. In conclusion, safeguarding IoT products and services necessitates cooperation between producers, programmers, consumers, and regulators. This study is helpful for researchers and students who want to construct a safe smart home since it offers a full examination of the vulnerabilities and best practices for each layer of IoT security. In the end, to create a reliable and secure IoT ecosystem, a comprehensive approach to IoT security that includes device-level, network, and application security is required.

Keywords: IOT, security of IOT, DDoS attack, Network Layer Security

Received 25 Mar., 2023; Revised 05 Apr., 2023; Accepted 07 Apr., 2023 © The author(s) 2023.
*Published with open access at **www.questjournals.org***

I. Introduction:

The Internet of Things (IoT) is on the cusp of becoming a ubiquitous technology in commercial settings, following years of anticipation and gradual acceptance. The utilization of IoT devices by businesses has surged from 13% in 2014 to around 25% at present. Architecture is a structure for detail of a system/program's actual parts and their useful association and set up, its functional standards and techniques, as well as information designs utilized in its activity. The layers for the same IOT Architecture are discussed below:

It comprises different services and applications that can be offered by IoT. Smart transportation, utilities, smart homes, etc. can be considered as an example This is the scenario in the Application layer of the system.

The perception Layer describes that here various devices are utilized for sensory purposes i.e., to detect the change in the environment in a wide variety of ways. For exactly same purpose we require different sensors to process and locate different objects, some of the notable ones are RFID sensor, Humidity sensor and much more. The network Layer comprises the physical components and communication software of the network, including various elements like topologies, servers, network nodes, and other components that facilitate communication among devices. Its primary function is to ensure effective communication between devices and receivers.IoT is made up of diverse computing heterogeneous devices with varying standards due to the wide-ranging requirements of different applications this lies in the domain of the middleware layer. This device hetero1geneity leads to device compatibility. To address this problem, a middleware platform is used between things or objects and applications.

The design of a "Automated and High Security Homes" is a technological advancement that allows individuals to intelligently control and monitor various household devices automatically [1], [2]. There are some devices available which can be controlled over remote distance i.e. the Internet of Wi-Fi these devices are really helpful for daily usages some mentions are mobile applications, Digital hangings and many more. These Advancements offer an alternative to traditional methods and can be utilized for tasks such as household power

management, temperature control, and opening/closing doors [2]. Examples of applications in a smart home include smart lighting, intrusion detection, and intelligent appliances. [3].

The Automated High Security Homes has a basic hierarchy that consist of three important layers, which consist of mainly the sensing layer, Web layer and the application layer. Here the first layer collects the information using various tools and methods like Global Positioning System, Radio-Frequency Identification and some sensors include vibration sensor, pressure sensor and much more [1], [4], [5]. The accuracy, privacy, and authentication of data must be ensured by the sensors that collect it [1], [6].

As soon as the information is collected it gets transferred over to the application unit present in the system. The Network layer is helps in transporting the information to the processing unit that which process and refines it for further use. Numerous number of technologies such as sensors, Global Positioning System, Wi-Fi are implemented in various systems. Some notable mentions are cloud . Thus to relay the data to the application unit, we implement wireless and fast systems [1], [6], [4], [5].

Ultimately, the data is delivered to the application layer, which is entirely dependent on end-users [1]. End-user interfaces using this layer include smartphones and laptops. As a result, end-users will be able to interface directly with devices in the application layer [6], [4], [5]. In this layer, IoT is used and supported by a lot of applications, like smart homes, smart cities, and many more [4], [5], [7]. Ultimately, the data is delivered to the application layer, which is entirely dependent on end-users [1]. End-user interfaces using this layer include smartphones and laptops. As a result, end-users will be able to interface directly with devices in the application layer [6], [4], [5]. In this layer, IoT is used and supported by a lot of applications, like smart homes, smart cities, and many more [4] [5], [7].

- Vulnerabilities: In this section, some typical cybersecurity flaws in smart devices will be discussed as what they are and what hazards they pose. The idea is that manufacturers of smart home devices can take precautions against these major cybersecurity vulnerabilities as part of standardized cybersecurity operations.
- Perception layer: This layer collects data from sensors. However, security risks can compromise this layer in three ways: (i) disrupting wireless transmission channels between sensor nodes, (ii) physically tampering with hardware and components of sensor nodes, and (iii) exploiting the limited battery power, storage, and processing capability of IoT nodes. The Perception layer is susceptible to various types of attacks, such as malicious code injection attacks [8], replay attacks [9], and eavesdropping attacks [10]. To prevent these attacks, secure encryption techniques are essential.
- Network layer: The layer mentioned here is works on to get the network resources working. Due to this it also under constant attack of Hackers and intruders including spoofing attacks and Denial-of-service.
- Application Layer: The application layer provides the fundamental services required by consumers. This layer may provide a variety of issues, such as phishing attacks, harmful viruses, malicious scripts, and so on. To combat malicious virus/worm attacks in IoT, defensive measures such as a reliable firewall and worm-detecting software can be used.

Insufficient authentication/authorization: Weak (default) passwords like "1234" or "password" are common on IoT devices, including smart home devices. Weak passwords are a severe security vulnerability in the IoT, according to various studies. In a study conducted in 2015, the most commonly used IoT devices, including smart thermostats and smart locks, were examined. A big instance of a security breach in IoT devices, owing to the exploitation of weak passwords is Mirai Botnet. In the study, researchers employed 61 commonly used username-password combinations, such as admin-1234, to gain access to roughly 400,000 IoT devices, including popular ones such as smart thermostats and smart locks [12]. The system made i.e. Mirai botnet was configured and made in accordance to launch various attacks on the targeted applications (websites, or apps or IOT devices) directly or by targeting DNS host and these attacks includes DDoS (distributed denial-of-service)[13]. Another significant security concern, likely due to weak or default passwords, involved the hacking of baby monitors, where unauthorized individuals accessed the video feeds or used the speakers to communicate with the baby. Some occurrences have included gaining access to a whole smart home due to the home automation system's complete absence of strong passwords. According to OWASP, insufficient authentication and authorization can result in "loss of data or degradation, a lack of accountability, or denial of access, and can result in a total compromise of the device and its user profiles"[14].

Lack of transport encryption: Information is encrypted by converting some plaintext phrase into an unintelligible (ciphertext) phrase that can be decrypted only by using the encryption key shared by the verified sender and receiver. Cryptographic approaches, such as symmetric cryptography and public key cryptography, can be used to accomplish this. When an IoT device broadcasts unencrypted information, it can be stolen in plaintext as it transits over a local network or the internet, exposing the information to everybody. This is especially critical when it comes to sensitive and personal data or username and password combinations. [19] One of the primary findings of a survey of IoT devices undertaken by HP in 2015 was that most of the devices (around 70%) did not encrypt data transported to the local network and the internet.

II. Literature Survey:

This literature survey explores the various layers of IoT devices and there different merits and demerits some of the points related to various layers and there limitations are discussed with details -

2.1. Application Layer

The proposed models in research papers lack efficiency in message delivery, despite good accuracy. While some protocols perform better, they are not suitable for all conditions. Message authentication and security are not adequately integrated, and long-term security is lacking in the application layer. Decentralizing IoT systems and implementing blockchain for enhanced security is challenging, and middleware devices are not cost-efficient, requiring separate processing power and time-consuming data conversion.The table below compares the various techniques used to secure the application layer.

Table-1 Analysis of various approaches to the application Layer.

Methods	**Issues**	**Solution**	**Limitation**
Compact EDHOC, alightweightalternativetoEDHOCisproposed,security parameternegotiationsaretakenfromtheprotocol'score.	Message transfer Authorization and authentication is dealt to make the message channel secure.	communications are protected using symmetric and asymmetric key encryption.	Both proposed models demonstrated good accuracy, but they suffer from low delivery efficiency due to the long time required for messages to reach their destination.
Application LayerProtocols such as MQTT,CoAP,AMQP,DDS,SSDP.	Comparativeanalysisofdifferentstandardsandprotocolsisconductedsoastofindoutthemostviable standardandplatform.	Thechoiceofstandardandprotocol should be based uponthe nature of system which ismainlyclassified into 2 parts:datacollectionservicesandaddressspecificservices.	Whilesomestandardsandprotocolsgavebetterresults,theystillaren'tviable to useineverycondition.
Communication Models inIoT such as RFID, PacketStructures.	The communicationmodelstransferdataefficiently but there is littletonoaspectofmessagesecurity.	The messages can be encryptedusing cryptographic techniquestoprovidemessagesecurity.	Theintegrationofsecuringmessagesas wellasauthenticationofsaidmessagesis notprovided.
MiddleBridge (BridgedMQTTwithHTTP).	MostIoTapplicationssupport only 2 applicationlayerprotocols.	To make the process of transmitting data more seamless for both senders and receivers, it may be possible to introduce an intermediary device that can translate the data into an application protocol supported by the middleware. This step can be performed without any disruption to the data flow.	The integration of middlewaredevicesisnotcostefficient. TheMiddleBridgealsorequiresseparate processingpower to convert data makingittimeinefficient.
AWS IoT, Web Sockets, Bosh IoT.	The level of IoT security provided by different layers is analysed and investigated.	Input Validation Control, changing TelNet port numbers and SSH accounts can be one solution.	The solutions provided tho secure the network for a short span of time but there is a lack of long-term security guarantee in the application layer.
Blockchain Based IoT Security.	Privacy protection, DoS and DDoS attacks are tracked and addressed.	Integrating Blockchain and cutting off third party mechanisms is proposed especially for identity verification. Log and auditing as well as access control.	It is not easy to decentralise IoT system and incorporate. blockchain methods to enhance security while ensuring proper functioning.

2.2. Physical Layer

The solutions proposed in all these papers aim at providing security at the physical layer. A common problem with all the models proposed in these research papers is the lack of efficiency and mitigation of congestion that

comes along with integrating a considerably large number of RFID receivers. Network failure is another bottleneck that exists in these papers. Additionally, there is a need of balancing the algorithms' security and privacy against computational viability. The Comparison of different methods used for the security of Physical layer is given in the following table:

Table-2 Comparison of different methods used for the security of Physical layer.

Methods	**Issues**	**Solution**	**Limitation**
RF connectivity is utilised within the home to create a smart home security system that is IoT-enabled [16].	Low-cost architecture is required due to the high cost of creating a smart-home setup.	The recommended architecture utilises a Raspberry Pi 2 and an Arduino-compatible Elegoo Mega 2560 microcontroller board to connect with a web server that supports RESTful API.	Several home appliances utilise RF signals to communicate, which causes a number of RF receivers to attempt to send messages to the Raspberry Pi at the same time or cause it to receive unwanted signals.
a hybrid identification method for improving the security of mobile RFID devices that combines a security check handoff (SCH) with a group-based and collaborative approach [17].	Although major efforts have been made to assure privacy and anonymity in RF systems, speed, scalability, and customizability challenges necessary for reliable IoT deployment have received little attention. The shortcomings of current protocols include throughput delays, inadaptability, and identifying methods that are either unsecure or inefficient.	The proposed protocol ensures secure and scalable RFID deployment for IoT with customizability and adaptability. It also includes malware detection for extra protection. The protocol's security, scalability, and customizability were tested through a randomness battery test, showing improvement over existing protocols.	The computational complexity rises as the number of tags rises.
The proposed technique in the paper suggests shuffling to protect the bit positions of original fields and prevent unauthorized access[18].	A bit-flipping attack is a type of attack that enables the modification of specific fields on ciphertext without requiring decryption.	Eachoctetintheframepa yload is shuffled to enhancecomplexityand makebitflippingattacks more difficulttoexecute.	Session key is known only toend device and network serverwhichmight be a bottleneckincaseofnetworkfai lure.
Key Generation - Whether through peer-to-peer or trusted third-party means, the use of secret keys for integrity checks can stop illegal access to the system. Anomaly Detection: After defining the behaviour of a healthy system and comparing the observed behaviour to current typical features, the identification of anomalous behaviour for specific smart grid devices is made feasible.	Asmartenergysystem'swidespreaduseofcurrentcomputertechn ologyandcommunicationstandardsexposesittoaslewofcyber-threats.	The authors propose a framework based on machine learning, physical layer security techniques, and better key generation to improve the security of smart energy systems across multiple applications. This architecture attempts to safeguard the smart energy system's physical layer.	Whenworkingwithsmartgrida lgorithms,maintainingprivacy might be a challenge.Inaddition,therema ybeatrade-offbetweenanalgorithm'ssecu rityanditsefficiency.

Acryptographic hashfunction-basedRFIDprotocolisemployed.	RFID tags are susceptible to unauthorized scanning by hostile readers due to their long transmission range. To address this vulnerability, the study proposes an RFID protocol that provides forward privacy service. However, the research also shows that attackers can track a target tag by examining its failed past sessions.That is,the RFID protocol does notprovidetheadvertisedforwardprivacyprotection.	A solution to the privacy issues of the proposed RFID technology is presented in the form of an RFID protocol that utilizes cryptographic hash functions.	The RFID protocol falls short of meeting all the practical needs in the real-world scenario.

2.3. Perception Layer

The solutions proposed in the research papers works towards securing and strengthening the perception layer. Most of them lack coverage of security aspects. It is necessary to integrate more reasonable access control methods and authentication algorithms. The proposed models lack testing against actual threats as well. Data integrity is another aspect that is compromised in some of the papers and need to be balanced with the efficiency of the algorithm. It is also a necessity to enhance time and energy consumption of the algorithms. The comparison of different methods used for the security of Perception layer is given in the table below:

Table-3 Comparison of different methods used for the security of Perception layer.

Methods	**Issues**	**Solution**	**Limitation**
Based on a broad comprehension of security concerns, an effective authentication and access control solution is created for the Internet of Things' perception layer (IoT).	Used to address resource-constrained problems in the internet of things' perception layer.	Elliptic Curve Cryptography is used to provide for more secure reciprocal authentication between user and sensor nodes as well as for intermediary procedures.	The Internet of Things' security confronts several challenges every day, and in order to protect data security, WSN, which serves as a backup to the IoT perception layer, needs more efficient authentication and access control methods.
a learning-based method for protecting against perception-layer attacks on particular sensor types in smart furniture for individuals with disabilities.	A problem that has to be fixed right now is that some Internet of Things solutions are still in the prototype stage and ignore possible threats and the accompanying security countermeasures.	This method is based on the study of time series and uses a dynamic time warping methodology to compute similarity between time series and a special anomaly detector to find abnormalities. It has been proven by defending a smart cabinet with magnetic sensors on the door against simulated magnetic assaults on its perception layer.	In order for SCs to be prepared for commercialisation and practical assistance for people with disabilities, further security safeguards still need to be added to them, and they must be tested against a range of genuine dangers.
In order to ensure safe transaction processing and integrity, the technique suggests using and integrating Blockchain with the Fog. The technique employs a smart contract algorithm that performs a check called the integrity check on entered data and prevents the entrance of incorrect values through the system by rectifying the entered data in accordance with normal operating circumstances [19].	The main problem with the perception layer is that it is vulnerable to several physical and digital risks, like the extremely dangerous insider threat like logic bomb. This strategy deals with this issue.	As a solution to the issue, the authors developed a framework that combines edge computing and Ethereum blockchain to carry out tests and maintain the robustness of entering data priorto it is analysed, processed, and stored. In order to build a method to safeguard the robustness of system data for precise analytics and processing, it is necessary to know how different change in the state of environment affects the integrity of data received by sensors in the perception layer.	Feature extraction, which would have been helpful in further case studies or application areas, was not addressed in the approach. The approach concentrates on data integrity within specific low and high standards that, if surpassed, might endanger the system.
Nodes in the perception layer are secured using the Securing Nodes in IoT Perception Layer (SNPL) technique. In order to maintain security and meet performance requirements, the SNPL is built using cutting-edge lightweight algorithms, as well as safety solutions that offer security isolation for delicate processes [20].	The perception layer in IOT, regulates the data's original source, serving as "the final mile of communications." IoT nodes are also the sources of data, which is crucial for IoT security. This plan resolves the problem and safeguards these nodes.	To guarantee the reliability of IoT nodes that are based on nodes' properties, the SNPL method has been suggested. In this system, an IoT node's private value, which serves as an identity property, is generated using the MD5 algorithm. Next, node authentication in TEE—a trusted development environment for carrying out critical operations—is	If the data is not from genuine nodes, it is meaningless. The major drawback is that data from rogue nodes that are intentionally altered might have disastrous effects for decision-making systems that rely on them.

		implemented using the node's attribute and a present access policy.	
The suggested watermarking technique includes digital watermark extraction, digital watermark creation, and digital watermark embedding [21].	This strategy is used to reconcile the contradiction between perception layer security and constrained resources. A method called position random watermark has been developed to enhance security, which utilizes the temporal dynamics of sensing data to determine the embedding location.	The suggested approach can successfully thwart a number of assaults, including packet forging attacks and packet transmission delay attacks, among others. In addition to reducing the complexity in computational and enhancing validation effectiveness and security, it also guarantees revokable watermark extraction and lossless data restoration.	Malicious data modification might have significant repercussions. Additionally, the encryption algorithm uses complicated computing instructions to ensure security, which requires additional storage space for the keys and presents an important challenge to computational load, consumption of energy, and storage capacity of sensor node.

2.4. Network Layer

The solutions proposed in all these research papers proposed solutions for network layer security issues. A common bottleneck in these papers is viability and feasibility. While the solutions may be efficient theoretically, the problems of latency and computational overhead is still prevalent in these proposed solutions. Furthermore, attack detection framework is not as secure as it may give the hackers the power to take over and modify vulnerable nodes. The comparison of different methods used for the security of Network layer has been explained in the table below:

Table-4 Comparison of different methods used for the security of Network layer.

Methods	**Issues**	**Solution**	**Limitation**
Framework for attack detection that chooses IoTN nodes from which to perform its distributed algorithms [22].	The requirement for swift detection of any network layer assaults on a specific IoTN.	Every 30 seconds, the MNS protocol is used to choose a subset of nodes to act as monitoring nodes. To identify Network layer assaults, the monitoring nodes in turn execute the distributed algorithms of ADF.	The hacker has a lot of power because to ADF. They could be able to seize control of a few IoTN nodes, changing the weaker nodes in the process.
Malware Analysis Architecture (MARS), which uses SDN to control the network movement, performing the inspection of network traffic in a centralised fashion [23].	Malwares target IoT devices with weak built - in defences and turn them into bots.	MARS consists of a set of APIstocommunicatewiththenetworklayerbyexecutingpacketswitchingandbyallowingpacketinspection.	The resources are not made available to researchers to compose their own customised malware analysis process.
Encrypting the header and payload of communications at the network layer to secure communications and protect against different threats [24].	Issues are with the purpose of preventing risks like traffic analysis and unauthorised data collection.	The payload and meta-data of an IoT protocol link layer communication are encrypted by Black Network. Using encryption at the Network layer to encrypt the header and content, Black SDN also secures communication.	Further latency and routing overhead issues will be brought on by the suggested architecture.
Security ofMiddlewar	The issue is with the	The study secures the communication between devices using entity identification, safe storage, security audit, and dataencryption/decryption.	Middlewareisnotyetwidely used

e.	requirement for security for communication and intelligent home systems.		andintegratedinIoT

2.5. Middleware Layer

The proposed middleware for edge layer security needs to be enhanced with multi-factor user authentication, support for more application layer protocols, and expanded security beyond MQTT protocol. The feasibility of using blockchain with fog needs to be confirmed for scalability. The middleware's trust-based approach can be improved over time with the use of AI-based techniques, while globally unified standards need to be set for maximum effectiveness. SDKs in Java and Arduino are available for device integration. The Comparison of different methods used for the security of Middleware layer is given in the table below:

Table-5 Comparison of different methods used for the security of Middleware layer.

Methods	**Issues**	**Solution**	**Limitation**
'Session Resumption' and 'Optimal Scheme Decider' algorithms are used by middleware to reuse encrypted sessions [25].	IoTdevicesina resourceconstrainedenvironmentcanbecomehighlyunstable due to undesirablesecurityoverheads.	In times of unstable network conditions, "Intermittent Security" allows for rapid reconnections, while "Flexible Security" gives users the option of selecting the best security configuration.	Itisconcernedabouttheefficientimplementationofmiddlewaresecurityonlyontheedgelayer.
Middlewareasaninterfacefortheusertointeractwithsensordatausing RESTAPI[26].	Becauseoftheenormouskeysize,calculating ciphertextbecomesacomputationallycostly operationinIoTsystems.Hence,PKIbecomesanissue.	A middleware design offers contributors who contribute sensing data an end-to-end security solution. Using the REST API, this approach makes it possible to encrypt data from beginning to finish.	There is a need for a multi-factor user authentication scheme in the proposed middleware.
A middleware suggested by [29] that supports the application-layer protocols MQTT, CoAP, and HTTP[27].	Devices lack personal credentials or mechanisms for device authorization, the MQTT Protocol has limitations, and packet size optimisation is not implemented.	The six parts that make up the suggested solution are: interoperability; persistence and analytics; context; resource and event; security; and GUI. They meet the prerequisites in terms of scalability, security, dependability, etc.	For device integration, only JAVA and Arduino SDKs are available. For greater reach, the number of supported application layer protocols can be extended.
Framework for Internet of Things communication leveraging blockchain and fog technologies[28].	Service time is a variable with a random distribution that may occasionally exceed the period time; as a result, it is unavoidable that some packets may run into a busy channel and be lost.	In each of its three layers—Internet of Things, Blockchain, and Fog—the proposed system uses a retransmission method, variable packet length, and saturated traffic conditions.	The feasibility of this framework is not confirmed as the scalability of blockchain with fog is questionable.

III. Results and discussions:

Considering the diversity of devices, the intimacy of the devices to the user, and the sensitive nature of the information they contain, there is an urgent need of finding the best available solutions to the known vulnerabilities.

In the application layer, Compact EDHOC and hybridization of application layer protocols with HTTP can provide a huge benefit to IoT security for maintaining and enhancing 2 wide aspects namely: authentication and authorization. Blockchain-based security protocols can provide security at a higher level once calibrated and integrated with various IoT applications on a pocket-friendly budget. The enhancement of already existing messaging protocols and also provide security on a smaller scale if not on a long-term basis.

Smart homes and other IoT ecosystems alike are known to be vulnerable due to a lack of transport encryption. Cryptographic technique which uses the same cryptographic keys for both encryption and decryption processes is known as the symmetric-key algorithm. There is another cryptographic technique which has two different keys, one key is made public, and the other key is private which is known only to the owner. [1] defines a mix of symmetric and asymmetric encryption that addresses communication between IoT devices, or within the IoT system.

To facilitate a full implementation of IoT, performance, scalability, and customizability concerns have not received much attention at the physical layer. Existing protocols also have a variety of flaws, including slow throughput, inadaptability, and insecure or ineffective identifying methods. An identification technique based on a hybrid approach (group-based approach and collaborative approach) and security check handoff (SCH) for the Mobility of RFID systems that ensures the deployment of an RFID system in a safe and scalable manner while also allowing for customization and adaptation is needed to support a strong distributed structure like the IoT.Here, a GBC-IoT system is developed, a group-based machine learning method that looks for connected IoT devices by analysing network traffic.

Collaborative filtering is a technique for creating automatic predictions (filtering) about a user's interests by combining preferences from several users (collaborating).The protocol uses an integrated malware detection approach as an additional layer of defence against malware. Morshed Chowdhury, Jemal Abawajy, Biplob R., and Ray analysedhow the protocol was put to the test using a randomness battery, and the results demonstrated that it outperformed existing protocols in terms of security, scalability, and customizability [17].

Certificate Authorities (CAs) administer and track network node security credentials on Intelligent Transportation Systems (ITS) devices using public key infrastructure to reduce data interruption. Risk analysis is another security technique implemented by ITS[30].

Middleware is being utilized as a security tool more frequently now. Middleware can be used to protect device communication using encryption [31]. The middleware put out by da Cruz employs an Arduino and Java microservices architecture and supports the application layer protocols MQTT, CoAP, and HTTP. The effectiveness of the solution was assessed and compared to other open-source solutions now available, taking into consideration response times, the percentage of erroneous requests, and packet size, and it was discovered to be the most effective. It was chosen as the best middleware for a smart home because it balanced the security it offers with the speed at which it does so [32], [27].

The perception layer serves the primary purpose of converting analog signals into digital form and vice versa in the IoT architectural tiers. The paper titled "SNPL: One Scheme of Securing Nodes in IoT Perception Layer" by authors Fan, Yongkaiet et al. focuses on the protection and security of the perception layer nodes, which is the most efficient and optimized solution to ensure the security of the perception layer out of the vulnerabilities and issues reviewed in this paper. According to experimental findings, the proposed SNPL security strategy may accurately and efficiently distinguish between legitimate and malicious nodes based on their distinctive identification information.

Network layer: Data obtained from the perception layer is sent over the network via the network layer. This layer is susceptible to a number of assaults since it gets data from several heterogeneous devices. So, identifying the threat that is being posed and its source becomes essential. To identify Network layer assaults, the monitoring nodes in turn execute the distributed algorithms of ADF[22]. The issue of finding vulnerabilities in this layer is resolved by the use of entity identification, safe storage, security audit, and data encryption/decryption to protect the connection between devices. By leveraging SDN and encrypting the header and the payload at the network layer, Malware Analysis Architecture [23] and Black Networks further contribute to mitigating possible attacks on the network layer.

IV. Conclusion:

In conclusion, to eliminate possible hazards to people and businesses, it is crucial to address the security of IoT devices. It is difficult to safeguard IoT devices effectively due to the rising number of connected devices and the complicated network infrastructure.

The application layer, transport layer, and physical layer of the network should all have various security features and methods in place to protect IoT devices. By employing a layered security strategy, it is possible to reduce potential security risks and make sure that the devices and the data they gather are protected from intrusion and attacks.

However, securing IoT devices is not solely the responsibility of device manufacturers or network providers. End-users also play a critical role in securing their devices by following best practices, such as using strong passwords, regularly updating firmware, and enabling two-factor authentication.

Overall, securing IoT devices requires a collaborative effort between device manufacturers, network providers, and end-users. By implementing robust security measures and educating users on security best practices, the security risks associated with IoT devices can be mitigated, ensuring that they remain secure and functional.

In this study, the security flaws as well as the roles of various IoT layers are examined. Furthermore, the many solutions proposed by the various authors are explored. The security flaws based on the layers that comprise IoT are grouped and explored with numerous flaws with examples. The literature on existing approaches for protecting IoT infrastructure was also reviewed and described these security solutions in terms of

how they address IoT vulnerabilities. The existing security approaches' drawbacks were evaluated and suggested future work recommendations to solve these limitations.

References:

[1]. Kumar, P., Braeken, A., Gurtov, A.V., Iinatti, J.H., & Ha, P.H. (2017). Anonymous Secure Framework in Connected Smart Home Environments. IEEE Transactions on Information Forensics and Security, Vol. 12, pp. 968-979

[2]. T. Malche and P. Maheshwary, "Internet of Things (IoT) for building smart home system," 2017International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2017, pp. 65-70

[3]. S. A. Kumar, T. Vealey and H. Srivastava, "Security in Internet of Things: Challenges, Solutions and Future Directions," 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 2016, pp. 5772-5781

[4]. Adat, Vipindev, and BB Gupta. (2018) "Security in internet of things: issues, challenges,taxonomy,andarchitecture."TelecommunicationSystems,Vol. 67, no. 3, pp. 423–441

[5]. Yassein, M.B.; Hmeidi, I.; Shatnawi, F.; Mardini, W.; Khamayseh, Y. Smart Home Is NotSmart Enough to Protect You—Protocols, Challenges and Open Issues. Procedia Comput. Sci.2019, pp.134–141.

[6]. MarkWalker,KeltonShockey,AndrewNeiman,&AshtynStephan (2018),Awakening GlobalGovernments: An International survey of Internet of Things regulation, The 46th ResearchConferenceonCommunication,InformationandInternetPolicy, pp. 3-4

[7]. Seda Gurses and Bart Preneel, 'Cryptology and Privacy in the Context of Big Data' in Bartvan der Sloot et al. (eds) (2016) Exploring the boundaries of big data (Amsterdam, AmsterdamUniversityPress pp. 53-62 .

[8]. Ray, B.R., Abawajy, J.H., & Chowdhury, M.U. (2014). Scalable RFID security framework and protocol supporting Internet of Things. Comput. Networks,Vol. 67, pp. 89-103.

[9]. Cruz da, Mauro AA, Joel Jose PC Rodrigues, Jalal Al-Muhtadi, Valery V. Korotaev, andVictorHugoC.deAlbuquerque.(2018)"Areferencemodelforinternetofthingsmiddleware."IEEEInternetofThingsJournal5,no.2, pp.871-883.

[10]. Albuquerque de. C .(2020) "In. IoT—a new middleware for internet of things." IEEE Internet ofThingsJournal8,no.10, pp. 7902-7911.

[11]. Lee, JungWoon, DongYeop Hwang, JiHong Park, and Ki-Hyung Kim. (2018) "Risk analysis andcountermeasure for bit-flipping attack in LoRaWAN." In 2017 International conference oninformationnetworking(ICOIN),Vol. 8, no. 4, pp.549-551.IEEE.

[12]. Wara,MohammadShafeul,andQiaoyan Yu. (2020) "New replay attacks on zigbee devices forinternet-of-things (iot) applications." In 2020 IEEE International Conference on EmbeddedSoftwareandSystems(ICESS),pp.1-6.IEEE.

[13]. Mohammad,Zeyad,ThaerAbuQattam,andKholoudSaleh. (2019) "SecurityweaknessesandattacksontheInternetofThings applications." In 2019 IEEE Jordan International JointConferenceon Electrical Engineering and Information Technology (JEEIT), pp. 431-436.IEEE.

[14]. Abughazaleh,Nada,R.Bin,andMaiBtish. (2020)"DoS attacks in IoT systems and proposedsolutions."Int.J.Comput.Appl, Vol.176,no.33, pp.16-19.

[15]. Garg, Hittu, and Mayank Dave. (2019) "Securing iot devices and securely connecting the dots usingrest api and middleware." In 2019 4th International Conference on Internet of Things: SmartInnovationandUsages(IoT-SIU),pp.1-6.IEEE.

[16]. Alam,Tanweer. (2020)"Designablockchain-basedmiddlewarelayeronthe Internet of ThingsArchitecture."JOIV:InternationalJournalonInformaticsVisualization,Vol. 4,no.1 , pp. 28-31.

[17]. Castilho, Sergio D. , Eduardo P. Godoy, and Fadir Salmen. "Implementing security and trust in iot/m2m using middleware." In 2020 International Conference on Information Networking(ICOIN),pp.726-731.Ieee.

[18]. Sun, Da-Zhi, and Ji-Dong Zhong.(2018) "A hash-based RFID security protocol for strong privacyprotection."IEEETransactionsonConsumerElectronics, Vol. 58,no.4, pp.1246-1252.

[19]. Mrabet, Hichem, Sana Belguith, Adeeb Alhomoud, and Abderrazak Jemai.(2020) "A survey of IoTsecurity based on a layered architecture of sensing and data analysis." Sensors, Vol. 20, no. 13: pp.3625-3635.

[20]. Nebbione,Giuseppe,andMariaCarlaCalzarossa. (2020)"SecurityofIoTapplicationlayerprotocols:Challengesandfindings."FutureInternet, Vol.12,no.3, pp.55-64.

[21]. Swamy, S. Narasimha, and Solomon Raju Kota.(2020) "An empirical study on system level aspectsofInternetofThings(IoT)."IEEEAccess, Vol.8, pp.188082-188134.

[22]. Tukur Y.M. ,Thakker D. and Awan I., (2019) "Ethereum Blockchain-Based Solution to InsiderThreats on Perception Layer of IoT Systems," 2019 IEEE Global Conference on Internet ofThings(GCIoT),pp.1-6.

[23]. You-guo,Li,andJiangMing-fu. (2011) "Thereinforcementofcommunicationsecurityoftheinternet of things in the field of intelligent home through the use of middleware." In 2011FourthInternationalSymposiumonKnowledgeAcquisitionand Modeling, pp. 254-257.IEEE.

[24]. da Cruz, Mauro AA, Joel JPC Rodrigues, Pascal Lorenz, Petar Solic, Jalal Al-Muhtadi, and Victor Hugo C. Albuquerque. (2019) "A proposal for bridging application layer protocols to HTTP on IoT solutions." Future Generation Computer Systems Vol. 97: pp. 145-15

[25]. Adina,Prasesh,RaghavH.Venkatnarayan,andMuhammadShahzad. (2018) "Impacts&detectionofnetwork layer attacks on IoT networks." In Proceedings of the 1st ACM MobiHoc WorkshoponMobileIoTSensing,Security,andPrivacy,pp.1-6..

[26]. Islam, Shama Naz, Zubair Baig, and Sherali Zeadally. (2019) "Physical layer security for the smartgrid:Vulnerabilities,threats,andcountermeasures."IEEETransactionsonIndustrialInformatics, Vol.15,no.12 , pp. 6522-6530.

[27]. Qian, Quan, Yan-Long Jia, and Rui Zhang.(2018)"A Lightweight RFID Security Protocol Based onEllipticCurveCrytography."Int.J.Netw.Secur, Vol.18,no.2 , pp. 354-361.

[28]. Perez,Salvador,JoseL.Hernandez-Ramos,ShahidRaza,andAntonioSkarmeta.(2019)"Application layer key establishment for end-to-end security in IoT." IEEE Internet of Things Journal, Vol.7,no.3, pp. 2117-2128.

[29]. Henriques,M.S.,Vernekar,N.K.,(2017), "Usingsymmetricandasymmetriccryptographytosecure communication between devices in IoT", International Conference on IoT andApplication(ICIOT), pp.1-4.

[30]. Zhao, Walker and Wang(2012). "Security Challenges for the Intelligent Transportation System",ProceedingsoftheFirstInternationalConferenceon Security of Internet of Things, pp.107-115.

[31]. LiYou-guo,JiangMing-fu. (2011) "The Reinforcement of Communication Security of the InternetofThingsintheFieldofIntelligentHomeThroughtheUseofMiddleware",FourthInternational Symposium on Knowledge Acquisition and Modeling (KAM), pp. 254 – 257.

[32]. Islam, Md Jahidul, Md Mahin, Shanto Roy, Biplab Chandra Debnath, and Ayesha Khatun (2019)."Distblacknet: A distributed secure black sdn-iot architecture with nfv implementation forsmart cities." In 2019 International Conference on Electrical,

Computer and CommunicationEngineering(ECCE),pp.1-6.IEEE.
[33]. Sardana and S. Horrow (2010), "Identity management framework for cloud-based internet ofthings", Proceedings of the First International Conference on Security of Internet of Things,pp.200-203,2012.
[34]. LuigiAtzori,AntonioIera,GiacomoMorabito."TheInternetofThings:Asurvey,"ComputerNetworks,Vol.54, No. 1, pp.2787–2805.
[35]. Y.Jie,J.Y.Pei,L.Jun,G.YunandX.Wei (2013),"SmartHomeSystemBasedonIOTTechnologies," 2013 International Conference on Computational and Information Sciences,pp.1789-1791
[36]. Mukherjee, Bidyut, Songjie Wang, Wenyi Lu, Roshan Lal Neupane, Daniel Dunn, Yijie Ren,QiSu,andPrasadCalyam (2018)."FlexibleIoT security middleware for end-to-end cloud–fogcommunication."FutureGenerationComputerSystems, Vol.87, pp. 688-703.
[37]. Rizvi, Syed, Andrew Kurtz, Joseph Pfeffer, and Mohammad Rizvi (2018):. "Securing the Internet ofThings (IoT): A security taxonomy for IoT." In 2018 17th IEEE International Conference onTrust, Security and Privacy in Computing and Communications/12th IEEE InternationalConferenceonBigData Science And Engineering (TrustCom/BigDataSE), pp. 163-168.IEEE.
[38]. Abbasi, Mohammad Asad, Zulfiqar A. Memon, Nouman M. Durrani, Waleej Haider, KashifLaeeq,andGhulamAliMallah.(2021)"Amulti-layertrust-basedmiddlewareframeworkforhandling interoperability issues in heterogeneous IOTs." Cluster Computing, Vol. 24, no. 3, pp.2133-2160.
[39]. Qian, Yongfeng, Yingying Jiang, Jing Chen, Yu Zhang, Jeungeun Song, Ming Zhou, andMatevz Pustisek.(2018) "Towards decentralized IoT security enhancement: A blockchain approach."Computers&ElectricalEngineering, Vol.72, pp.266-273