A Review of Security Threats of Internet of Things

Nargis Jamal†, Sataish Riaz††, and Jawad Ibrahim†††
nargisbutt57@gmail.com riazsataish@gmail.com Jawwad.ibrahim@cs.uol.edu.pk
†University of Lahore Gujrat Campus, Pakistan,
††University of Lahore Gujrat Campus, Pakistan,
†††Faculty of Information Technology and Computer Science, University of Lahore Gujrat Campus Pakistan,

Summary
The Internet of Things (IoT) is a novel concept that allows a large number of objects to be connected to the Internet while also allowing them to be controlled remotely. The Internet of Things is extensive and has become an almost inseparable part of our daily lives. Users' personal data is frequently obtained by these linked gadgets and stored online. In recent years, the security of acquired data has become a major concern. As devices grow more linked, privacy and security concerns grow more pressing, and they must be addressed as soon as possible. IoT implementations and devices are particularly vulnerable to attacks that might adversely affect customer security and privacy, which might have an impact on their practical utility. The goal of this study is to bring attention to the security and privacy concerns that exist in IoT systems. To that purpose, the paper examines security challenges at each level of the IoT protocol stack, identifies underlying impediments and critical security requirements, and provides a rapid overview of available security solutions for securing IoT in a layered environment.

Keywords:
Internet of Things, IoT, Security Threats, Security Challenges, Security Solutions, Security Requirements

1. Introduction

We live in an era of the internet, when we are surrounded by a plethora of computer gadgets. There are several wired and wireless networks available today. Any individual has the ability would be interconnected and available online, and everything will be willing to coordinate and interact with others, according to the internet architecture. Because everything will be hooked up to the internet in the future, we can refer to it as the Internet of Things (IoT).The Internet of Things (IoT) promises to make our lives easier by transforming every physical thing in our surroundings into a smart object capable of sensing the environment, communicating with other smart things, thinking, and responding appropriately to changes in the surrounding environment[1].By 2020, it is expected that the number of IoT devices will have surpassed 50 billion[2]. IoT applications include home automation, Tourism, farming, commerce, the smart grid, medical, smart buildings, and logistics are just a few examples of smart technologies. Neglect these security and privacy concerns will have major consequences for all facets of our life, including the homes we reside in, the automobiles we drive to work, and even the impacts on our own bodies.

Malicious users or hackers can target IoT, just like any other technology. The IoT's massive and complicated design makes it simple to spot flaws. Hackers can take advantage of this vulnerability and use it to target IoT networks. Hackers can get access to IoT networks and cause damage. Network obstructing their operation, and misusing the data, as well as a lot more. Because IoT networks are so vital, they must be safeguarded and any security loopholes must be filled. Users want the highest degree of security and privacy while utilizing IoT networks[3]. Because IoT networks communicate user data, users' security and privacy are a top priority. Because of the relevance of IoT in our daily lives, the subject of IoT privacy and security has gained traction.

1.2. Development of IoT:

Internet access is getting more affordable as well as reachable all around the world. Minicomputer and nanotechnology are being used in computing equipment which resulted in a reduction in their scope and usage control simultaneously increasing their storing capacity This builds it simple toward add actuators and sensors to them. They can communicate through the internet thanks to this jumble of little devices with many functions[1]. RFID tags, NFC tags, or barcodes are affixed to tangible things, and they are scanned using machines similar to a smart phone, tablet, and RFID/NFC scanners. The internet's capability can be improved by linking the objective world and cyber planetary via smooth gadgets[4]. This will usher in a novel internet era known as the IoT. Figure-1 shows the future structural design of IoT.

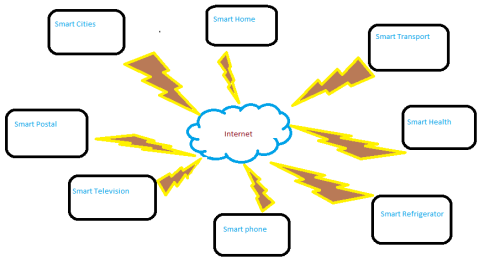

Fig_1: General internet of things sensing devices

Manuscript received June 5, 2024
Manuscript revised June 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.6.13

2. The Internet of Things' Generic Architecture:

About the layers of internet of things diverse investigators give their dissimilar view. The Internet of Things basic architecture may be broken down into four layers. Perception, Transport, Network, and Application Layers are their names. In the future, Internet of Things will confront a variety of issues, particularly in terms of safety and confidentiality[4]. The fundamental process of the Internet of Things is to connect everyone with everything so that they can interchange info with one another, as well as the quantity of communication sensing devices will grow tremendously. As a result, advancements in Internet of Things are dependent on technical advancements and are applicable to extensive choice of application and business models.

2.1. Perception Layer:

In open system interconnection In the OSI model, this layer is similar to the physical layer. Sensors and actuators of many types make up the perception layer (i.e., Quick Response code, Radio Frequency Identification, infrared ZigBee, etc.)[3]. Data is collected, sensed, and processed by these sensors (position, shaking, dampness, storm rate, dust in the air, etc.) take information as of the atmosphere and throw it to the network layer. Figure-2 shows the four layer structural design of IoT[1].

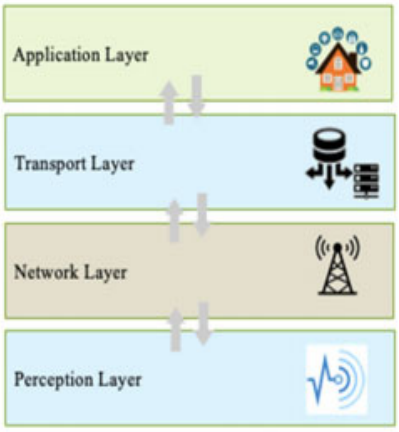

Fig_2: Show the four layers of architecture

2.2. Transport Layer:

The Transport Layer is the TCP/IP models second layer. It is an end-to-end layer for sending messages to a server. It is referred to as an end-to-end layer as it establishes a point-to-point relation among the foundation and end hosts, rather than a hop-to-hop connection, in order to deliver services consistently[4]. A segment is the smallest unit of data encapsulation in the Transport Layer.

2.3. Network Layer:

This layer is in charge of routing and transmitting data collected from various Internet of Things sensors to various Internet of Things devices and hubs over the internet. All of the data gathered by these devices must be transferred and processed. This is the responsibility of the network layer. It allows these gadgets to communicate with other smart items, servers, and network devices. It is also in charge of all data transfer[3].

2.4. Application Layer:

The user interacts with the application layer. It's in charge of providing the user with application-specific services. This might be a smart home application where users tap a button in the app to switch on a coffee machine, for example[1].

2.5. Internet of Things Protocols:

The instructions and principles that are rummage-sale for end wise communication of sensors linked to a diverse or similar network in internet of things protocols[1]. For machine to machine communication which are frequently rummage-sale will be define fleetingly in this segment. For messaging transport Communication Line Telemetry Transportation is a client sever practice. It is relaxed to appliance and frivolous. This set of rules will ride above Transmission Control Protocol/Internet Protocol[5]. Every time irregular interruption arises Message Queue Telemetry Transport will inform the concerned parties around this incident over unexpected machinery. Constraint Application Protocol can be simply converted to Hyper Text Transfer Protocol for simplification of web incorporation and it can also deliver particular requirements such as minor overhead, multicast provision, and broad-mindedness[6].

3. Layer wise Safety Problems in existing IoT systems:

There are numerous security dangers associated with IoT layers; every layer is subject to a variety of security assaults, which can be active or passive and initiate from either an internally or externally resource[7]. Active attacks will promptly disable the system, although passive attacks can steal data from the IoT system invisibly and with no disrupting services. A DoS (Disk operating System) attack can damage every layer of IoT, rendering network services inaccessible. In this subsection, we will deliberate safety problems connected to individually layer of the Internet of Things.

Table-1categorizes a few of the safety issues/attacks in the layered Iot systems.

TABLE 1: Security issues/attacks in the layered Iot systems.

IoT Layers	Security Issues/Attacks	Security Parameters
Application layer	Access control and secure authentication challenges, data privacy and restoration concerns, spear-phishing assaults, malicious Code Injection, assaults on reliability, and clone attacks are all examples of data storage and access identification concerns[8],[9].	Data privacy, access control
Middleware layer	Making informed decisions Massive data processing, malicious software attacks, multi-party verification, and suspect database management[10],[9].	Integrity, Confidentiality
Network layer	DoS attacks, spoofing, changed, or repeated routing information are all examples of clustering security issues[11],[12],[13],[14],[9].	Authentication, integrity
Perception layer	Node capturing, faked node implantation, massive node verification, cryptographic method, tag cloning, and access control mechanisms are all included[5],[9].	Reliability, authenticity, and secrecy are all important considerations.

3.1 Perception layer:

The perception layer includes any devices that are connected to an Entire system and are responsible for transmitting data, such as sensors, motors, Zigbee, RFID structures, QR codes, and Gps devices[15].This layer's security issues are at the node level. The perception layer's external users, such as sensor devices, motors, and other devices, are the source of the majority of security vulnerabilities[16]. Because the nodes contain smart devices, motors, connectors, and other components, they become perfect targets for hackers looking to expose them and replace the device software according to their own code. IoT devices, in practice, low battery power and storage ability, makes them simple, less strong, and compact size. They are also more prone to run out of power or be harmed by other extrinsic environmental variables, rendering them open to privacy attacks[17]. The most typical assaults in the physical layer are denial of service assaults, false nodes or malicious data, jamming, manipulation, node capture, and so on[5].

3.2 Transport layer:

The transport layer, which sits atop the network layer, processes large amounts of data and makes intelligent judgments[18]. It makes use of technological breakthroughs such as cloud computing, and database management. Because the layer is capable of processing large amounts of data, it can be challenging to handle large amounts of data at some points. The layer can distinguish between legitimate and harmful data. Therefore, in this layer, recognizing authentic data and filtering out dangerous content is a serious difficulty[11]. Additional challenge on this layer is how to handle dubious data. The users can exploit lists of valid data and network content, as well as substitute the data with harmful information. It has the ability to send inaccurate or dangerous data to the network, which can cause the system to fail or entirely stopped. This layer's main concerns are combined certification for supply controlled machines and firmly store information to the cloud [10].

3.3 Network layer:

Because the network layer transports a huge volume of information, it is vulnerable to assaults that cause "network congestion[8]." The authenticity and confidentiality being transferred via the system are the most important security concerns in this layer. Although the network layer's comparatively improved security measures, it is at rest susceptible to imitation attacks and man-in-the-middle attacks[11].

3.4 Application layer:

Smart gadgets that give customized services to users make up the application layer. These are typically uncomplicated, short control, and portable equipment that are prone to assault[6]. Malevolent assaults can cause the software to malfunction by replacing the programmed codes with defects. As a result, the applications might be compromise, close up, and be unsuccessful to do what they were designed to do, as well as perform authenticated services in an insecure manner. The application layer is in charge of data exchange, which can lead to issues with authentication, data protection, and unauthorized access[11], [19]. A few of the typical risks in the application layer are software vulnerabilities, malicious code attack, failure to get safety measures, and intrusion keen on the smart indicator/network [8].

4 Security Issues and Requirements for IOT:

4.1 Security Issues in IOT:

Many constraints apply to Internet of Things machines and gears, for example their computational authority and assets, as well as device heterogeneity. It brings up additional security concern Internet of Things security challenges can be classified into two categories: There are both security and technological difficulties [8].

Security challenges develop as a result of the concepts and functionalities that necessity be tracked in order in the direction of construct a safe network. The usual Internet of Things architecture is as follows: Where no monitoring system is established, some gadgets or perception sensors are deployed publicly. Outside attackers will be vulnerable as a result of this. Aggressors can gain right of entry to these sensing device and programmer them such that the devices be able to conduct information to both the index servers and the attackers' group. Following the ideas and guidelines outlined below, a safe message outline for software, procedures, belongings, as well as persons can be created[5].

4.1.1 Authentication:

Authentication is the procedure of confirming and ensuring an object's identity. In the perspective of the Internet of Things, each object must be capable to recognize and valid at all additional stuffs in the organization (or It interacts with a certain element of the structure)[20].

4.1.2 Confidentiality:

Confidentiality is the process of make sure that merely certified people have right to use data. When it comes to Internet of Things confidentiality, there are two major challenges to consider: To begin, make sure that the item getting the information will not shift or transmit the information to other substance, and then think about information organization [20].

4.1.3 Denial of Service (DoS) Attack:

An attack that brings a system or network to a halt and prohibits accredited users from connecting it [8]. This could be accomplished by flooding the organization or set-up with a huge number of spam needs all at once, as a result, the system is overloaded, and it is unable to provide the typical service.

4.1.4 Replay Attack:

Information is saved and re-transmitted with no having the ability to do so in this attack. Authentication protocols are frequently targeted by such attacks[5].

4.1.5 Routing Threats:

This is the mainly basic assault at the system layer, other than it can also happen at the perception layer during the data forwarding procedure[15]. An assailant can build a direction-finding loop, which causes a lack or addition of the course-plotting pathway, as well as an increase in end-to-end delay and error messages.

4.1.6 Distributed Denial of Service (DDoS) Attack:

DDoS assault is on a wide scale. The ability to employ a large number of IoT nodes to send traffic collected to the victim server is the most difficult problem to solve. There are suspicions that a huge quantity of IoT nodes were used in the DDoS assault known as "Mirai" that occurred in October 2016[20].

4.2 Security requirements for IoT:

In[21] data Reliability, security systems, verification, data exchange, and retreat were explored as four dimensions of IoT security.

4.2.6 Data Integrity:

In[21] several insights are hidden in the information gathered by IoT network. These records are extremely valuable and should be kept safe from prying eyes. These information should also be kept private and archived for later usage. Could traditional centralized memory tools, such as caching, be used and combined with the IoT architecture. They are prone to flaws from the start. The centralized server might quickly become a single point of failure. In addition, having additional machines with the database approach might cause many-to-one traffic congestion, system scalability issues, and incur late reply. To safeguard IoT data from deletion and degradation, blockchain-based systems could be designed. In networks, user authentication is regarded as a major concern[22]. It is worried with allowing authorized users access to their data and code over their ip rights.

4.2.7 Data Sharing:

Data is passed back and forth between IoT devices. In IoT networks, there is a principal object that works to share data across IoT objects. This could benefit businesses by allowing them to provide better services to their clients, as well as production and transportation. IoT systems generate a massive amount of data. According to a survey of US manufacturers, 35% of manufacturers rely on data generated by sensors to optimize their processes. Typically, this data are not available for free. In order to do so, a competitive and convenient data exchange technique is needed[21].

4.2.8 Authentication and Access Control:

Accessing IoT networks' confidential data and sensitive resources is a security concern. Conventional identification to an exterior organization and access control administration are dependent on a centralized authority that generates a correct key. When the number of connected devices continues to rise, the centralized Iot network becomes a barrier. Because of the changing

environment of IoT, complex trust management may lead in the platform's flexibility being sacrificed[21].

4.2.9 Privacy:

Optics in Iot network collect data from different of connected devices to aid in decision-making based on the requirements[21]. In the Internet of Things, privacy can be easily breached in a variety of ways, including data collecting, data exchange, and data analysis.The misuse of data generated by the IoT system has the potential to compromise user privacy. In[23] privacy is important for limiting data loss, deterring attackers from exploiting communication nodes, and decreasing system threats.

5 Layer Wise SECURITY SOLUTIONS FOR IOT:

Because IoT devices typically converse with one another through little individual contact, joint verification is an important part of the model. IoT gadgets are unquestionably built for everyday use, and they are commonly used to collect, store, and analyze personal data. To avoid unauthorized node right to use and to recognize system nodes, authentication and access control mechanisms should be used in the perception layer[24]. [25]Data encryption and confidentiality techniques are critical for preventing malicious code injection and protecting gathered data from change[26], [26]. Addition a powerful data encryption and key organization method, on the other hand, would significantly drain the resources of IoT devices. As a result, lightweight cryptographic methods and protocols are required to address this issue[27].To identify any harmful conduct on the network, intrusion detection systems might be used[28]. Several solutions for safeguarding IoT devices and networks have been offered in the past.

5.1 Security solutions in the perception layer:

Sensors, RFID, wireless sensor networks (WSNs), GPS, and other devices make up the perception layer. The attackers at this layer are mostly interested in node catch, assault on entrenched sensors, secret writing algorithms, and key management mechanisms. In[2] Cyber sensors, or sensors that monitor real-time data such as temperature and speed for use in real-time events and rapid actions, is another technique. In[29], the security challenges in the perception layer are discussed, as well as some potential remedies. For risks regarding node security in IoT systems, the author has anticipated an upgrade to the PKI-similar to safety system protocol. Aggarwal [30] proposed an enhanced RFID security protocol. In an IoT system, the perception layers include RFID tags for data collection and data exchange between linked objects. The author presented a more efficient approach that also protects against disclosure and resynchronization attacks. By Salami[31] presenting a lightweight encryption strategy for automated buildings, we examined privacy service, key management, and computation and communication competence challenges. The method works well on devices with limited resources and features a flexible public key management system. As a result, the approach is additional proficient in terms of encryption function, as well as contact and computing slide. The scalability of public key algorithms makes them ideal for node certification with no need for sophisticated key management protocols. In[2],[29] the perception layer, the authors have provided countermeasures to issues regarding node security. The author[31] developed a better protocol for RFID security in IoT devices.

5.2 Security solutions in the network layer:

The network layer is in charge of sending and interpreting sensor data. Because it transports a lot of data, it's vulnerable to safety assaults like DoS, man-in-the-middle, and DDoS. Risk assessment is yet secure way used by Intelligent Transportation Systems (ITS), where a public key transportation is employed in the CAs for controlling and maintaining authentication method for system nodes on ITS to protection to help data interruption[25]. In[32] author suggested a methodology for safe end-to-end connectivity among IP sensor networks and the Internet. In[32]suggested a methodology for safe end-to-end connectivity among IP sensor networks and the Internet. In[33] suggested a compact technique to protect IoT network environments from DDoS attacks. The technique was verified on a variety of network nodes, including working nodes, attacker nodes, observation nodes, and valid user nodes. The author also mentions that an attacker's ask for is only entertain once, later than which the packet are deleted and the demand is routed to the attacking record for the next time. In comparison to other current systems, the results demonstrated that the suggested method is sufficient to prevent and identifying DDoS attacks.

TABLE_2: Security Issues/Attacks and their Solution in Perception Layer.

Method/Author	Layer	Possible issue/attack	Solution
PKI – Product Key Infrastructure/Li et al., [29]	Perception Layer	Threats to the safety measures of nodes	When a node is safely sent, a "offspring node" authenticates it by sending a decryption key. The offspring node is still being upgraded and enhanced.
Cyber Sensors/Liu et. Al., [2]	Perception Layer	Data production from physical items is lacking, as is factual information.	Cyber sensors that collect information from sensor devices can then be utilized to take actions or respond to real-time events.
RFID Tags (Radio Frequency ID) /Aggarwal et al., [30]	Perception Layer	The inability to connect devices due to RFID security	Radio Frequency Identification (RFID) chips can be inserted into connected devices to facilitate quick connectivity between mobile, according to a proposed enhanced methodology.
Lightweight Encryption scheme /Al Salami et al., [31]	Perception Layer	Encryption activities are being sped up.	Encryption technique with a compact design

TABLE_3: Security Issues/Attacks and their Solution in Transport Layer.

Method/Author	Layer	Possible issue/attack	Solution
User certification technique over multiple servers /Tsai & Lo., [35]	Transport Layer	Controlling access and verification	Proposed a multi-server user identification approach.
Encrypted Query Processing approach/Shafagh et al.,[36]	Transport Layer	Effectively protect IoT data in a cloud server.	Provided an Encryption Information Retrieval technique for securely storing IoT data in the cloud storage and querying over the encrypted files.
Identity Manager and Service Manager technique/Horrow&Sardana [37]	Transport Layer	To veify the authenticity of data sent between the internet and smart devices.	By installing an uniqueness executive and a Service executive upon on endpoints, you may improve security.

TABLE_4: Security Issues/Attacks and their Solution in Network Layer.

Method/Author	Layer	Possible issue/attack	Solution
ITS Security Methods and Standards for Efficiency – Risk Analysis /Zhao et al., [25]	Network Layer	Threats to the ITS (Intelligent Transportation System) should be addressed (i.e. smart transportation)	To avoid information from being disrupted, a public key infrastructure is often used in which certification authentication (CAs) are utilized for controlling and maintaining authentication method for network nodes on ITS to endpoints.
End toEnd secure communication technique /Raza et al., [32]	Network Layer	Communications must be authenticated, encrypted, and checked for authenticity.	End-to-end encrypted communications among both the Internet and IP sensor nodes is supported by this method.
DDoS attackprevention algorithms /Zhang & Green, [33]	Network Layer	DDoS attacks	A method for preventing DDoS attacks.
Novel IoT mixed uniqueness-based certification system /Salman et al., [34]	Network Layer	Identity-based authentication	Using the idea of Software Defined Networking (SDN) on Iot systems, an unique IoT heterogeneity identity-based verification technique has been developed.

TABLE_5: Security Issues/Attacks and their Solution in Application Layer.

Method/Author	Layer	Possible issue/attack	Solution
DSM/Jafari et al., [38]	Application Layer	Informatics for evaluation criteria	They offer five factors for the provision of security measures that relate with information security and policies in particular.
Game Theory /Cox and Balasingham [39]	Application Layer	The assault of numerous complicated systems of differing complexity	To build improved safety techniques, researchers used a method of assaulting systems.
authorization framework,/Seitz & Gehrmann, n.d., [40]	Application Layer	Problems with access control and authorization in asset systems	Decisions are based on regional information and equipment circumstances in the suggested authorization scheme.
IoT-OAS targeting HTTP/CoAP servicesarchitecture /Cirani et al., [41]	Application Layer	Establish a structure for permission.	IoT-OAS architecture aimed towards HTTP/CoAP applications
Session keydistribution system /Park., [42]	Application Layer	To enable secure interoperability between devices.	A mechanism for inter-device verification and transmission of session keys was proposed.

Authentication mechanisms were mentioned in[34] as one of the features that could help with IoT security. By implementing the notion of Software Defined Networking (SDN) on IoT devices, they suggested an identity-based verification system to solve the multiplicity in IoT and to connect the numerous protocols in IoT. The result was evaluated using the AVISPA tool, and the consequence proves that it is resistant to disguise, man-in-the-middle, and replay attacks.

5.3 Security Solutions in the Transport Layer:

The transport layer is in charge of retrieving and analyzing information and making decisions depending on the results. Multi-party verification and safe cloud data storage are two of the most important challenges at this layer. In[35]explored the safety issues around data access and authentication, and suggested a user authentication mechanism that works across several servers. The suggested technique reduces connectivity and calculation time amongst numerous cloud service providers and conventional trusted third-party services. The proposed approach allows numerous cloud services from many service providers to be accessed with a single key, demonstrating that it is both reliable and effective. In[36]proposed an Encrypted Computation technique, which allows the method to safely stock up IoT objects on a cloud platform and question the encrypted information. For resource-constrained equipment, they apply ultra light encryption algorithm, and the findings show that the system is effective in relational query dispensation and successful on moderate and resource-constrained equipment's. In[37] suggested an information management model that uses an Information Controller and a Service Manager on the machines to verify data being sent among cloud and connected devices.

5.4 Security solutions in the application layer:

The application layer is accountable for providing services to end users. It is in charge of messaging among the application and the end users. In the context of IoT, it is accomplished utilizing a variety of protocols. Jafari et al. address safety measures for eHealth data systems in their Domain Specific Metrics (DSM) methodology. They recommend developing safety metrics based on five essentials: technological development analysis, threat investigation and modeling, necessities definition, rules and processes, and organization performance. Their presentation, though, does not include any methodologies for identifying, collecting, computing, or applying safety measures to solve security concerns and goals[38].Another security solution presented is Game Theory-based Adaptive Security for Smart IoT, which includes simulating the usage of tactics in which machines make decisions to design tactics to prevent, identify, and evade assaults. In the face of dangers, it provides reliability and risk assessment[39]. In[40]studied access control and certification in networked devices and provided a model for devices with limited space and computing capacity to provide configurable access control and certification. When analyzing the transmitted data among restricted and less bound servers, the proposed architecture allows exceptional flexibility for access

control models while minimizing transmission cost. In[41] introduced the IoT-OAS architecture as an authorized platform for HTTP/CoAP services that may be incorporated by calling an outside oauth-based approval provider. The planned work is adaptable and simple to interface with outside services, with minimal processing demand, flexibility, and wireless access modification as advantages. For encrypted transmission across objects, [42]suggested a solution that used inter-device certification and a session-key sharing system. The proposed approach can estimate the session key in advance, preventing threats like preview and man-in-the-middle threats.

6. CONCLUSION:

IoT system is establishing a vital communication channel among individuals. It offers a means of successful communication. Additionally, it is improving human lives by allowing the home automation, improved agricultural structures, and other intelligent devices which they require. As beneficial since this innovation is, hackers are attempting to use it in a negative means to target IoT devices and profit off innocuous confidential information. As a result, developing ways and tactics to defend Iot devices is critical. As a result, people's personal information is protected. IoT devices confidentiality's now a difficulty and a significant aspect of IoT network. The hazard degree of privacy concerns varies. There are few assaults that are more harmful than others. Furthermore, assaults change in terms of its origin; some may be inner, while others are outside. Assault might change in nature, although its bad effects are just the same varying in severity. The review of literature about IoT confidentiality was offered in this paper. On a layer-by-layer basis, the data security challenges of IoT network were also highlighted. Also highlighted are the types of security threats which might happen, how often happen, and how we can defend themselves from them. In addition, the paper reviewed attacks based on assault classification, as well as the causes behind their occurrence and how we can defend oneself from it. This review paper provided a comprehensive examination of IoT security and privacy issues.

7. Future Work:

This comprehensive article examines the security and privacy concerns of IoT devices from several angles. Also it offers protection against cyber-attacks on IoT network. There seem to be numerous viable options for safeguarding IoT devices including confidential material. These assailants, on the other hand, are attempting to improve the effectiveness and strength of their threat vectors. As a result, it's critical to develop increasingly complete and useful techniques to defend Iot devices. Perhaps can provide an appropriate strategy to defend IoT devices in the coming depends on the evidence and information supplied throughout this review study.

References:

[1] K. Y. Najmi, M. A. AlZain, M. Masud, N. Z. Jhanjhi, J. Al-Amri, and M. Baz, "A survey on security threats and countermeasures in IoT to achieve users confidentiality and reliability," *Mater. Today Proc.*, no. xxxx, pp. 2–7, 2021, doi: 10.1016/j.matpr.2021.03.417.

[2] X. Zhu, Y. Badr, J. Pacheco, and S. Hariri, "Autonomic Identity Framework for the Internet of Things," *Proc. - 2017 IEEE Int. Conf. Cloud Auton. Comput. ICCAC 2017*, pp. 69–79, 2017, doi: 10.1109/ICCAC.2017.14.

[3] Aqeel-ur-Rehman, S. U. Rehman, I. U. Khan, M. Moiz, and S. Hasan, "Security and privacy issues in IoT," *Int. J. Commun. Networks Inf. Secur.*, vol. 8, no. 3, pp. 147–157, 2016, doi: 10.4018/978-1-5225-6070-8.ch007.

[4] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, and A. Kashif Bashir, "A survey of security and privacy issues in the Internet of Things from the layered context," *Trans. Emerg. Telecommun. Technol.*, no. February, pp. 1–20, 2020, doi: 10.1002/ett.3935.

[5] A. Shukla and S. Tripathi, "Security Challenges and Issues of Internet of Things: Possible Solutions," *SSRN Electron. J.*, no. ICIoTCT, pp. 342–348, 2018, doi: 10.2139/ssrn.3166735.

[6] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," *J. Electr. Comput. Eng.*, vol. 2017, 2017, doi: 10.1155/2017/9324035.

[7] P. Dorey, "Securing the internet of things," *Smart Cards, Tokens, Secur. Appl. Second Ed.*, no. September, pp. 445–468, 2017, doi: 10.1007/978-3-319-50500-8_16.

[8] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in internet of things: Challenges, solutions and future directions," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 2016-March, pp. 5772–5781, 2016, doi: 10.1109/HICSS.2016.714.

[9] M. U.Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," *Int. J. Comput. Appl.*, vol. 111, no. 7, pp. 1–6, 2015, doi: 10.5120/19547-1280.

[10] W. Razouk, D. Sgandurra, and K. Sakurai, "A new security middleware architecture based on fog computing and cloud to support IoT constrained devices," *ACM Int. Conf. Proceeding Ser.*, 2017, doi: 10.1145/3109761.3158413.

[11] S. Kraijak and P. Tuwanut, "A survey on internet of

things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends," *Int. Conf. Commun. Technol. Proceedings, ICCT*, vol. 2016-February, pp. 26–31, 2016, doi: 10.1109/ICCT.2015.7399787.

[12] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," *Ad Hoc Networks*, vol. 20, pp. 96–112, 2014, doi: 10.1016/j.adhoc.2014.03.009.

[13] S. Kornemann, P. Langendörfer, and O. Stecklina, "SECI - Lightweight interpreter for security algorithms," *IoTSec 2017 - Proc. ACM Work. Internet Things Secur. Issues Innov.*, pp. 1–6, 2017, doi: 10.1145/3084030.3084034.

[14] R. R. der and R. V. V. S. . Prasad, "Cloud Computing Research : Challenges and Security Issues," *Int. J. Comput. Trends Technol.*, vol. 30, no. 3, pp. 157–161, 2015, doi: 10.14445/22312803/ijctt-v30p128.

[15] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wirel. Networks*, vol. 20, no. 8, pp. 2481–2501, 2014, doi: 10.1007/s11276-014-0761-7.

[16] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," *Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012*, vol. 3, pp. 648–651, 2012, doi: 10.1109/ICCSEE.2012.373.

[17] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions," *J. Ambient Intell. Humaniz. Comput.*, vol. 0, no. 0, pp. 1–18, 2017, doi: 10.1007/s12652-017-0494-4.

[18] G. Bouloukakis, N. Georgantas, P. Ntumba, and V. Issarny, "Automated synthesis of mediators for middleware-layer protocol interoperability in the IoT," *Futur. Gener. Comput. Syst.*, vol. 101, pp. 1271–1294, 2019, doi: 10.1016/j.future.2019.05.064.

[19] A. Jolfaei and K. Kant, "Privacy and Security of Connected Vehicles in Intelligent Transportation System," *Proc. - 49th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Networks - Suppl. Vol. DSN-S 2019*, pp. 9–10, 2019, doi: 10.1109/DSN-S.2019.00010.

[20] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of internet of things (IoT) authentication schemes," *Sensors (Switzerland)*, vol. 19, no. 5, pp. 1–43, 2019, doi: 10.3390/s19051141.

[21] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things," *IEEE Wirel. Commun.*, vol. 25, no. 6, pp. 12–18, 2018, doi: 10.1109/MWC.2017.1800116.

[22] G. Anil Kumar and C. P. Shantala, "An extensive research survey on data integrity and deduplication towards privacy in cloud storage," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 2, pp. 2011–2022, 2020, doi: 10.11591/ijece.v10i2.pp2011-2022.

[23] B. S. Bhati and P. Venkataram, "Preserving Data Privacy During Data Transfer in MANETs," *Wirel. Pers. Commun.*, vol. 97, no. 3, pp. 4063–4086, 2017, doi: 10.1007/s11277-017-4713-2.

[24] M. Qatawneh, W. Almobaideen, and O. AbuAlghanam, "Challenges of Blockchain Technology in Context Internet of Things: A Survey," *Int. J. Comput. Appl.*, vol. 175, no. 16, pp. 13–20, 2020, doi: 10.5120/ijca2020920660.

[25] K. Ren, C. Wang, and Q. Wang, "for the Public Cloud," *IEEE Internet Comput.*, vol. 16, no. 1, pp. 69–73, 2012.

[26] A. Jolfaei, A. Matinfar, and A. Mirghadri, "Preserving the confidentiality of digital images using a chaotic encryption scheme," *Int. J. Electron. Secur. Digit. Forensics*, vol. 7, no. 3, pp. 258–277, 2015, doi: 10.1504/IJESDF.2015.070389.

[27] A. Jolfaei and K. Kant, "A lightweight integrity protection scheme for fast communications in smart grid," *ICETE 2017 - Proc. 14th Int. Jt. Conf. E-bus. Telecommun.*, vol. 4, no. Icete, pp. 31–42, 2017, doi: 10.5220/0006394200310042.

[28] L. Chhaya, P. Sharma, G. Bhagwatikar, and A. Kumar, "Wireless sensor network based smart grid communications: Cyber attacks, intrusion detection system and topology control," *Electron.*, vol. 6, no. 1, 2017, doi: 10.3390/electronics6010005.

[29] Z. Li *et al.*, "Research on PKI-like protocol for the internet of things," *Proc. - 2013 5th Conf. Meas. Technol. Mechatronics Autom. ICMTMA 2013*, pp. 915–918, 2013, doi: 10.1109/ICMTMA.2013.227.

[30] T. Hall and E. L. Ave, "Security challenges in the internet of things Danai Chasaki * and Christopher Mansour," vol. 5, no. 3, 2015.

[31] S. Al Salami, J. Baek, K. Salah, and E. Damiani, "Lightweight encryption for smart home," *Proc. - 2016 11th Int. Conf. Availability, Reliab. Secur. ARES 2016*, pp. 382–388, 2016, doi: 10.1109/ARES.2016.40.

[32] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, and U. Roedig, "Securing communication in 6LoWPAN with compressed IPsec," *2011 Int. Conf. Distrib. Comput. Sens. Syst. Work. DCOSS'11*, 2011, doi: 10.1109/DCOSS.2011.5982177.

[33] C. Zhang and R. Green, "Communication security in internet of thing: Preventive measure and avoid DDoS attack over IoT network," *Simul. Ser.*, vol. 47, no. 3, pp. 8–15, 2015.

[34] O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab, and A. Kayssi, "Identity-based authentication scheme for the Internet of Things," *Proc. - IEEE Symp. Comput. Commun.*, vol. 2016-August, pp. 1109–1111, 2016, doi: 10.1109/ISCC.2016.7543884.

[35] J. L. Tsai and N. W. Lo, "A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services," *IEEE Syst. J.*, vol. 9, no. 3, pp. 805–815, 2015, doi: 10.1109/JSYST.2014.2322973.

[36] H. Shafagh, A. Hithnawi, A. Dröscher, S. Duquennoy, and W. Hu, "Talos: Encrypted query processing for the Internet of Things," *SenSys 2015 - Proc. 13th ACM Conf. Embed. Networked Sens. Syst.*, pp. 197–210, 2015, doi: 10.1145/2809695.2809723.

[37] S. Horrow and A. Sardana, "Identity management framework for cloud based internet of things," *ACM Int. Conf. Proceeding Ser.*, pp. 200–203, 2012, doi: 10.1145/2490428.2490456.

[38] S. Jafari, F. Mtenzi, R. Fitzpatrick, and B. O'Shea, "Security Metrics for e-Healthcare Information Systems: A Domain Specific Metrics Approach," *Int. J. Digit. Soc.*, vol. 1, no. 4, pp. 238–245, 2010, doi: 10.20533/ijds.2040.2570.2010.0029.

[39] H. Abie and I. Balasingham, "Risk-Based Adaptive Security for Smart IoT in eHealth," no. SeTTIT, pp. 269–275, 2013, doi: 10.4108/icst.bodynets.2012.250235.

[40] L. Seitz and C. Gehrmann, "Authorization Framework for the Internet-of-Things."

[41] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, "IoT-OAS: An oauth-based authorization service architecture for secure services in IoT scenarios," *IEEE Sens. J.*, vol. 15, no. 2, pp. 1224–1234, 2015, doi: 10.1109/JSEN.2014.2361406.

[42] N. Park, "Mutual authentication scheme in secure internet of things technology for comfortable lifestyle," *Sensors (Switzerland)*, vol. 16, no. 1, pp. 1–16, 2015, doi: 10.3390/s16010020.