IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ENHANCEMENT OF LAYERED SECURITY IN IOT FOR CLOUD INFRASTRUCTURE

[1]Niraj Kumar Tiwari, [2]Praveen Kumar Tripathi, [3]Rajesh Tripathi, [4] Prashant Srivastava, [5]Shivam Bhardwaj

[1]Assistant Professor, [2]Assistant Professor, [3]Assistant Professor, [4]Associate Professor, [5]Assistant Professor

[1]Computer Science & Engineering Department

[1] Shambhunath Institute of Engineering & Technology, Jhalwa , Prayagraj, India

Abstract: Numerous applications of the Internet of Things are employed to make life easier on a daily basis. A sophisticated security environment is required for the Internet of Things. Internet of Things security is crucial in opening up new business prospects and protecting us from danger. In order to improve and safeguard the growing number of connected "things" on our network, it is also a cloud subscription service available on demand [2]. The Internet of Things and cloud computing together not only improve its security but also broaden the range of its applications. But it also reveals important security flaws and some serious issues that need to be fixed. The research group has recently been concentrating on the security concerns and difficulties in the Internet of Things powered by the cloud. At this time, more and more surveys were being conducted on topics like intrusion detection systems, developing technologies, and threat modeling [5]. This article discusses the impact of IoT on data security to highlight the gap. This research paper discusses several security difficulties and challenges in the Internet of Things by combining the idea of a cloud-based Internet of Things architecture with various layers.

Index Terms **- IoT, Cloud Computing, Security, Authentication**

I. INTRODUCTION

The Internet of Things (IoT) was created to support rapid technological advancement in other fields. A wide range of applications, including those in health, transportation, smart cities, and industry maintenance systems, utilize this technology. IoT data security and privacy problems include authorization, authentication, privacy, and verification, among others. The goal of the Internet of Things is to secure data collection systems by integrating the capabilities of sensor and actuator devices. Security risks are created by the IoT solutions' greatly expanded acceptance. Some security measures are necessary to correctly understand with the Cloud based IoT security, taking into account the concerns and challenges in the form of data preservation [1]. In the commercial world, cloud computing is mostly utilized for on-demand network access, database storage, resource virtualization, and service interaction providers. Cloud computing is predicated on attributes like flexibility, shared services, dynamic behavior, and unrestricted scaling. Software-as-a-Services, Platform-as-a-Service, and Infrastructure-as-a-Service are three types of services that are included in the cloud computing model. Additionally, it includes deployment models that include public, private, hybrid, and community clouds. Many new technologies are being developed every day that use physical components like sensors and actuators to carry out important tasks. IoT data security on cloud platforms creates a number of problems and difficulties for massive data storage and accessibility [9].

Security Issues on IoT

The Internet of Things (IoT) connects a large number of smart people and sensor equipment to one another to enable the delivery of services at anytime, anywhere, and for any purpose. IoT also offers services to any business, person, or group in any situation or setting, using any device or network [3]. All sensor devices are connected to the Internet because of the wide range of effects they have on daily life, and this makes them all susceptible to privacy and security concerns including authenticity, confidentiality, and integrity [9]. A technique that prevents unwanted access to the system state and maintains privacy is referred to as security. Data's concealment is referred to as confidentiality; whereas its integrity verifies that it was not altered during transmission. In a secure network some of the required capabilities are:

i. Data Authentication: The sensed data & related information collected from secured, authenticated devices must be followed some technical mechanism & allow transmitting.

ii. Resilience to attacks: During data transmission if the system crashes, it should be automatically recover itself as same data uses in different domain. A cloud server must be protect smartly & intelligently himself from an intruders or eavesdropper [2].

iii. Client Privacy: At client side, the used data & information must be secure and safe. Personal data should be accessed by privately through the authorized person and maintain the privacy[6]. The private data should be protected i.e. no irrelevant authenticated user or other types of client can't be access the private data from the client.

iv. Access control: Only authenticated and authorized person can access the control. The general user can access the system by providing user name and password & their access rights, which will be controlled by the system administrator [4]. Different user can access the specific portion of the database or programs to smoothen running the system.

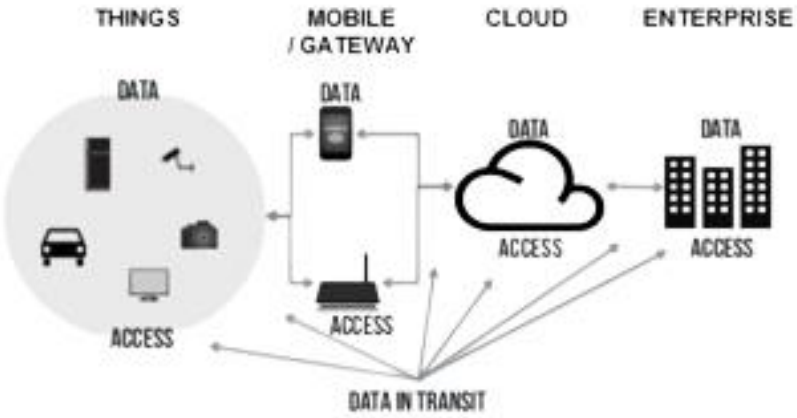

Figure 1. Security & Privacy in IOT

II. Cloud Based IOT

The convergence of Cloud Computer with the Internet of Things, or IoT, significantly alters the way high-performance is achieved in the global computing environment. IoT connected to the cloud is used to link machines and devices for controlling and monitoring. It became necessary due to the volume of data generated by IoT devices that needed to be processed and stored in the cloud. Data from sensors that are connected to machines are gathered by the cloud-based IoT. Because IoT users and devices are constantly sharing computing and networking resources remotely, security concerns are becoming increasingly urgent [7]. Privacy Data preservation is a significant issue in cloud-based IoT. Currently, privacy and security concerns need to be constantly expanding. Due to the numerous hazards and difficulties that must be overcome, we concentrated on the privacy and security issues. We examine the cloud-based IoT architecture, its various layers, and applications in order to accomplish this. In this research paper we also cover a lot of privacy and security-related concerns, problems, and open challenges.

III. Cloud based IoT Applications

IoT can benefit from the pay-per-use, scalability, security, performance, and reliability features of cloud computing infrastructure. Integration of cloud and IoT technology improves usage and analysis of several applications that continuously improve the IoT environment and provide potential for affordable on-demand scalability. Application of Cloud based IoT are discussed as below:

i. Smart City

A smart city is a technologically advanced metropolitan region that uses various electronic techniques and sensors to gather particular data. The data is utilized to generate information that is used to effectively manage resources, services, and assets; in turn, this information is used to enhance operations throughout the city. Information and communication technology (ICT) is used in smart cities to increase operational effectiveness, disseminate information to the general public, and improve the quality of public services and citizen welfare. IoT and the cloud enable ICT to connect machines and networked things for data transmission.

ii.Smart Home

A smart home system is employed to improve comfort and simplify life. Smartphones are used to control the majority of smart home systems. Smartphone applications are used to monitor and manage house functions. The objective of a smart house is to boost comfort while keeping costs down overall.

iii.Healthcare

Specialists and other doctors employ embedded IoT devices like wearables and monitoring equipment to monitor patients' health more conveniently even when they are not there. The collection of data from IoT devices is very beneficial for specialists who can pinpoint the precise patient issue and implement the best treatment strategy to get the desired results.

iv.Smart Grid

In order to improve population management and temperature control, IoT devices including sensors and actuators are used in wireless sensor networks (WSN). Given that it makes use of a combination of IoT, AI, sensors, and actuators, it is also known as the "Smart Environment Monitoring System".

v.Smart Logistic

It is an electrical network that makes use of a set of software, hardware, and electromechanical interfaces that enables two-way communication between the computing system and supply chain. Managing parking spots and traffic signs from a distance are other uses for it.

vi.Video Surveillance

IoT automation equipment aids industrial devices including machines, robots, and employees in the smart factory. To improve operations and boost efficiency, automation brings about significant changes in a variety of businesses. The main objective of Internet of Things automation is to lower running costs when various automation devices, actuators, and sensors operate remotely.

vii. Agriculture

Utilizing cloud-based services A system known as "IoT smart farming" was developed to monitor the crop field using sensors. IoT sensors are also beneficial for gathering a lot of information to determine the quality of the soil and to automate the irrigation system. By accessing data on temperature, humidity, soil moisture, nutrient presence, level of acidity, etc., farmers may monitor and assess field conditions from anywhere.

IV. Cloud Based IoT Architecture

A framework that is used to specify a network's physical components, as well as its many performance principles and procedures, is called a cloud-based IoT architecture. Layer architecture provides security from various attacks on those layers while also demonstrating the functions and purposes of various network layers. Three fundamental levels make up the cloud-based IoT architecture: the application layer, the network layer, and the perception or sensor layer. Figure below shows how the cloud-based IoT architecture is composed of three levels.

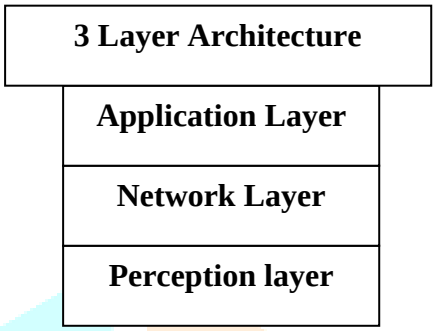

Figure 2. Three Layer Architecture

i.Application Layer

The upper layer of a cloud-based IOT architecture is known as the application or service layer because it offers a variety of services to the end user and carries out a number of actions on the data it receives from the middleware layer or the network layer. Additionally, this application layer offers many data services including data analytics methods, data mining, etc[5]. This layer interacts with the network layer to access data and offers services to third parties or the data owner. Service Oriented Architectural (SOAs), which is based on the layered architecture concept, is used to connect the application layer and network layer.

ii.Network Layer

Perception layer and application layer are connected by the network layer. This layer satisfies the requirements of wired and wireless protocols for secure connections, and one of its key tasks is to gather and store data in databases that are hosted in the cloud. The application layer receives the data and processes and analyses it so that it can be used in corporate decision-making and service provision. The inputs and outcomes are also sent between the application and the perception layer via the network layer.

iii.Perception layer

Due to its inclusion of physical components like sensors and actuators, the perception layer is also known as the physical layer. The physical devices' raw data are collected by the embedded sensors in this layer and sent to the network layer [11]. The objects that are taken into account in this layer vary in connectivity, have limited storage, and use little power, but they have a propensity to generate a lot of semi-structured data. This layer is also referred to as the object layer [10].

V. Issues and Challenges of Cloud Based IoT Architecture

The many levels of the cloud-based IoT architecture are vulnerable to active and passive attacks [13]. These attacks can be grouped according to the network behavior, which includes the following:

Active Attacks: In an active attack, the attackers compromise the network's functionality by exposing data during engagement or communication.

Passive Attacks: Passive attackers eavesdrop on communication channels and steal information from it.

A. Security threats and Issues of Application Layers

1) Malicious Code Attack: It is a particular code attack that targets a piece of software in order to have unintended consequences and activities, as well as to harm the system. The harmful code is uploaded by the intruders into the software, infecting the system.

2) Cross-site scripting: It's sometimes referred to as an injection attack. It enables the attacker to introduce a client-side script into various websites used by various people, such as JavaScript [8]. By using this technique, an intrusion can be made, and the user's data can be used illegally.

B. Security Threats and Issue of the Network Layer

1) Man-in-The-Middle Attack: This attack allows the attacker to alter data that is sent directly between the sender and the receiver by interrupting the communication line. Because the assigned system is unable to identify an attack, it assumes that a network mistake is to blame for the existence of this kind of issue.

2) Denial of Service (DoS) Attack: A network or system may be shut down using this technique, which also stops the intended user from using the machine or network resources. Flooding services and crashing services are two DoS attack techniques [12].

Flood Attack arises when there is too much traffic for the server to handle at once. Service to Crash attacks frequently exploits weaknesses.

3) Storage Attack: Users save a lot of valuable and confidential information on the cloud or other storage systems. The attacker has access to both the storage devices and the cloud to alter this valuable data. Additionally, an attacker may manipulate user data by adding incorrect information.

4) Exploit Attack: An exploit is a piece of software or code that has the ability to steal network data while also controlling the computer system. An exploit is a malicious assault that makes use of a bug or vulnerability in a hardware, software, network, or system.

C. Security Threats and Issue of the Perception layer

1) Eavesdropping: It is an passive attack. The attacker only listens to communications between two parties, such as phone conversations, faxes, and text messages. Attacker seeks to expose confidential information transmitted through a network.

2) Replay Attack: A replay attack, also known as a playback attack, involves falsely repeating or delaying a valid data transmission. It is an attack where the data is intercepted and then sent again through a network. In this attack, a person with unauthorized access intercepts traffic and then sends communications to their intended recipients while pretending to be the original sender [12]. While the communication recipient believes the message to be genuine, the attacker actually sent it.

3) Timing Attack: An attacker uses a side-channel assault in which the information is obtained through the cryptosystem rather than from a genetic flaw. It is typically used in computing underpowered devices.

VI. Survey Related to Cloud Based IoT Security

TABLE I – Cloud Based IoT Architecture Layer Attacks and Solutions

Layer	Attacks	Solutions
Application Layer	Privacy, Accessing Control, Privacy of information , Data Transit attack, Data Alteration, Reprogramming, Malicious code injection	Authenticity, Lithe solution, Anti-virus filtering , key agreements and user privacy protection across networks , Information Flow Control
Network Layer	DoS attack, Routing, Back Door Attack, Flooding, Black Hole , Tracking, , Eavesdropping, Phishing	Public-key Cryptography, Encryption, Primitives, Configured Firewalls , Authorization, Access Control, Monitoring, Malware Detection.
Perception Layer/	Sensor Layer Jamming, Physical Attacks, DoS, Tampering, Unfairness, OS Vulnerability, Data Transit Attack, Collisions .	Access control, Cryptography , Spread-Spectrum Techniques , Hiding, Security Test, Error Correcting Code.

VII. Cloud Based IoT Data Security Issues and Challenges

IoT offers numerous advantages to users, but it also worsens privacy and security issues because a lot of private data is IoT devices transmitting data to suppliers or third parties data management, data gathering, and data privacy both access control for personal data and The IoT architecture is cloud-based. some methods, such as maintaining confidentiality, encryption access control, etc. useful, but none alone are sufficient. Some of the risks and difficulties were discovered by researchers. which are linked to the development of the Internet of Things include resulting from massive amounts of data collected online, analysis, significant flaws, and a dearth of encryption. Data gathering and the absence of IoT devices raises questions about data privacy [11]. The three most crucial user characteristics for accessing IoT data on the cloud are authentication, authorization, and non-repudiation. The fundamental aspects of data security that are tested in the public cloud development model are confidentiality, availability, and database integration.

VIII. Conclusion

In a cloud-based IoT system, two recent research domains as Cloud Computing and IoT are combined. IoT application services based on the cloud do face some privacy and security challenges, though. A new cloud-based IoT architecture built on many levels is intended to reduce various assaults, privacy invasion, and unauthorized access. This architecture includes mechanisms that guarantee the security of the IoT and facilitate effective problem solving. A wide range of experimental findings demonstrate how effectively this cloud-based IoT system performs different functions and ensures that data privacy is maintained. There is still considerable work to be done for the full Cloud-based IoT system, though. Future research will focus on finding ways to perfect the architecture so that it can address other problems.

REFERENCE

[1]. Mohiyuddin, A.; Javed, A.R.; Chakraborty, C.; Rizwan, M.; Shabbir, M.; Nebhen, J. Secure Cloud Storage for Medical IoT Data using Adaptive Neuro-Fuzzy Inference System. Int. J. Fuzzy Syst. 2021, 1–13.
[2]. Ronghua Xu , Yu Chen , and Erik Blasch," Decentralized Access Control for IoT Based on Blockchain and Smart Contract" John Wiley & Sons, Inc.,pp.505-528, 2020.
[3]. D. Singh, Pushparaj, M. K. Mishra, A. Lamba, S. Swagatika, "Security Issues in Diffeent Layer of IoT and Their Possible Mitigation", International Journal of Scientific & Technology Research, Vol. 9, Issue 04, pp-2762-2771, April 2020.
[4]. Jamali, M. A. J., Bahrami, B., Heidari, A., Allahverdizadeh, P., & Norouzi, F. (2020). IoT Security.In Towards the Internet of Things (pp. 33-83). Springer, Cham.
[5]. Tabrizchi, H.; Rafsanjani, M.K. A survey on security challenges in cloud computing: Issues, threats, and solutions. J. Supercomput. 2020, 76, 9493–9532.
[6]. Riaz, S.; Khan, A.H.; Haroon, M.; Latif, S.; Bhatti, S. Big Data Security and Privacy: Current Challenges and Future Research perspective in Cloud Environment. In Proceedings of the 2020 International Conference on Information Management and Technology (ICIMTech), Bandung, Indonesia, 13–14 August 2020; pp. 977–982.
[7]. A. D. Jurcut, P. S. Ranaweer, L. Xu," Introduction to IoT Security", Wiley, DOI- 10.1002/9781119527978.ch2, 2019
[8]. M. Fenandez, J. Jaimunk, B. Thuaraisingham, "Privacy-Preserving Architecture for Cloud-IoT Platforms", 2019 IEEE International Conference on Web Services (ICWS), DOI 10.1109/ICWS.2019.00015, pp. 11-19, 2019.
[9]. Hasan Ali Khattak, M. A. Shah, S. Khan, I. Ali, M. Imran, "Perception Layer Security in Internet of Things", Elevier, pp-144-164, 2019
[10]. Kumar, P.R.; Raj, P.H.; Jelciana, P. Exploring data security issues and solutions in cloud computing. Procedia Comput. Sci. 2018, 125, 691–697.
[11]. Frustaci, Mario, P. A. C. E. Pasquale, A. L. O. I. Gianluca, and Giancarlo FORTINO., "Evaluating critical security issues of the IoT world: Present and Future challenges", IEEE Internet of Things Journal (2017).
[12]. Zhou J, Cap Z, Dong X, Vasilakos AV. Security and privacy for cloud-based IoT: challenges. IEEE Commun Mag. 2017;55(1):26–33. https //doi.org/10.1109/MCOM.2017.16003 63CM.
[13] Ramachandra, G.; Iftikhar, M.; Khan, F.A. A comprehensive survey on security in cloud computing. Procedia Comput. Sci. 2017, 110, 465–472.