**Securing IoT for Sustainable Industrial Transformation: Frameworks and Strategies**

Ms. Samiksha Khule, Mr. Yogesh Kumar Sharma, Dr. Monika Chauhan, Ms. Aruna Bajpai, Mr. Gaurav Dubey

Institute Of Technology and Management, Gwalior (M.P)

Samikshakhule.cse@itmgoi.in

**Abstract:**The Internet of Things (IoT) consists largely of innumerable Internet-connected technologies.Advanced information and communication technologies are essential for the emergence of smart IoT systems. The rise of untrustworthy third-party IoT applications has led to an increase in IoT-based malware assaults, compromising data security and privacy. IoT security solutions protect information and things against unwanted access, modifications, or destruction whereas the privacy schemes serve control over the use and purpose of acquired information.The Privacy and security are fundamental issues in the Internet of Things (IoT), posing considerable hazards due to inadequate device updates, a lack of efficient and comprehensive security procedures, user unawareness, and extensive active device monitoring.These challenges jeopardize the security and dependability of IoT systems, making it critical to address them for safer and more efficient IoT settings. In this Chapterwe coversnumerous IoT architecture, IoT systems and security measures, which involve identifying security and privacy issues, approaches to securing components, existing security solutions, and appropriate key challenges for various layers of IoT-driven applications. This article also provide a quick overview of major IoT issues, includingconfidentiality, integrity, authentication, and availability.By addressing these essential issues, we hope to provide a thorough understanding of how to improve the security and privacy of IoT systems. This is critical for guaranteeing the integrity and dependability of IoT deployments, which fosters confidence and encourages the continuous expansion and integration of IoT technologies across multiple sectors.

Keywords: Internet of things (IOT). Security, Privacy, Authentication, Artificial Intelligence.

**Introduction**

The Internet of Things' (IoT) fast expanding connected device count has drastically increased the risks associated with data privacy and cybersecurity, making these subjects essential for exploration.As IoT systems become more prevalent in numerous industries, the vulnerabilities in these devices and networks represent significant dangers to data security and privacy. This chapter discusses crucial research areas targeted at reducing these dangers. The key focus areas are developing privacy-preserving data gathering and processing techniques, designing robust and lightweight authentication mechanisms, and assuring secure communication and data transmission. It also investigates secure software processes and assesses privacy and security concerns in specific IoT applications such as smart homes and healthcare. The Internet of Things (IoT) is a technological paradigm revolution that connects an enormous number of things and devices—wired or wireless—through the Internet. This massive infrastructure makes it feasible to communicate and exchange data with ease for a variety of applications, which include smart homes, industrial automation, healthcare, and transportation. IoT is being opted for at a rapid pace, demonstrating its profound influence across a range of industries and promoting increased convenience, productivity, and creativity. Through IoT integration, devices can communicate with one another on their own, giving real-time data and insights that promote better decision-making and operational enhancements[1].

Geographical barriers are no longer an obstacle due to this interconnectedness, or hyperconnectivity, which enables people and organizations to interact and work from almost anywhere. As a result, IoT transforms how we approach both simple and complicated activities, improving communication while also opening the door for cutting-edge services and solutions. IoT is a key component of current technological breakthroughs and a vital force behind upcoming advances as its continuous evolution pushes the envelope of what is feasible [1].

The Internet of Things (IoT) is becoming a growing number of a target for cyberattacks, according to security experts. This is primarily because of its frequently inadequate security rules and procedures. Even though a lot of safeguarding methods have been created to protect IoT devices, comprehensive and consistent security documentation is still notably lacking. The dearth of comprehensive rules increases the susceptibility of Internet of Things (IoT) systems to diverse cyber threats. It is imperative to solve these security flaws as IoT devices grow more integrated into daily life and professional settings. Mitigating risks and protecting sensitive data from potential breaches require strengthening documentation and developing strong, standard procedures[2].

The ultimate goal is to establish trust in IoT technologies, allowing them to expand and integrate across industries while assuring secure and reliable IoT environments. This boosts confidence, promoting the ongoing development of IoT systems and their successful application in a variety of industries.

**Internet Of Things:**

The Internet of Things (IoT) is revolutionizing how we interact with the world around us and marks an enormous step forward in technical progress. IoT is fundamentally about using distinct Internet Protocol (IP) addresses to connect a wide range of machines, devices, and objects so they may communicate with each other without any requirement for human intervention. Numerous previously unthinkable applications are made possible by this link. For improved efficiency and convenience, IoT devices in smart homes have the ability to automatically control the lights, heating, and even place grocery orders depending on user preferences and usage patterns. In a manner similar to this, IoT sensors in industrial settings watch over equipment, anticipate maintenance requirements, and streamline manufacturing procedures, greatly increasing operational effectiveness and cutting downtime[3].

The Auto-ID Center at the Massachusetts Institute of Technology (MIT) initially presented the idea of the Internet of Things, which was a significant turning point in the development of digital technology [4]. This framework projected a time when commonplace items may have sensors built into them and be linked to the Internet, which led to a massive network of networked gadgets. As IoT technology quickly assimilated into several facets of industry and daily life, this vision has gradually come reality[5].

IoT is having a huge influence and is radically changing how we communicate and use technology. It makes it possible to gather and analyze data in real-time, facilitates wise decision-making, and promotes global connectivity. IoT is expected to spur more advancements and efficiency as it develops, highlighting its pivotal role in determining how digital engagement and automation will evolve in the future. IoT's rapid adoption in our daily lives is evidence of each its revolutionary potential and its continuously state of growth[5].

**IoT Architecture**

IoT designs fall into a number of different categories, each of featuring a unique method for integrating and inspecting IoT devices[6][7]. These classifications are composed of:

1. Three-Layer Architecture
2. Middleware-Based Architecture
3. SOA-Based Architecture
4. Five-Layer Architecture
5. Social IoT (SIoT)

**Three-Layer Architecture:**

An essential structure for comprehending the Internet of Things (IoT) and how it functions is provided by the Three-Layer Architecture[8][9]. There are three main layers that make up the IoT ecosystem, and each one has specific functions to play:  
  
*The perception layer*: It usually termed as the sensing layer, is where data collection gets started. The Perception Layer physically interacts with the surroundings using a variety of sensors, RFID tags, and cameras. Its primary job is to locate and collect information about thing or entities associated with the Internet of Things. For instance, temperature sensors could keep an eye on the weather, while RFID tags could record the whereabouts of products. As the IoT system's "eyes and ears," this layer essentially "senses" and logs data.

*Network Layer*: After the Perception Layer gathers data, it must be sent to other system components. This important task is dealt with by the Network Layer. It ensures smooth data flow throughout the system by connecting servers, smart devices, and network devices. The upkeep of network infrastructure, such as switches, routers, and other networking devices, as well as communication protocols, fall under the purview of this layer. It guarantees that data collected from several sensors and devices gets to its intended location effectively and safely[10].

*Application Layer*: This is the layer where end users' useful services and applications are created using the data that has been gathered. This layer provides beneficial characteristics and solutions by utilizing the data from the Network and Perception Layers. It can support smart healthcare apps that track and manage patient health, or it can allow smart home systems to change lighting and heating based on user preferences. Smart homes, smart cities, intelligent transportation systems, and other applications are contained in the application layer, which gives people access to relevant and actionable data[11].

The requirements of more sophisticated or complex applications are unlikely to be entirely met by the Three-Layer Architecture, despite the fact that it successfully describes the fundamental structure of IoT systems. To address scalability, data processing, and integration issues in such circumstances, further architectural models or layers may be needed[12].

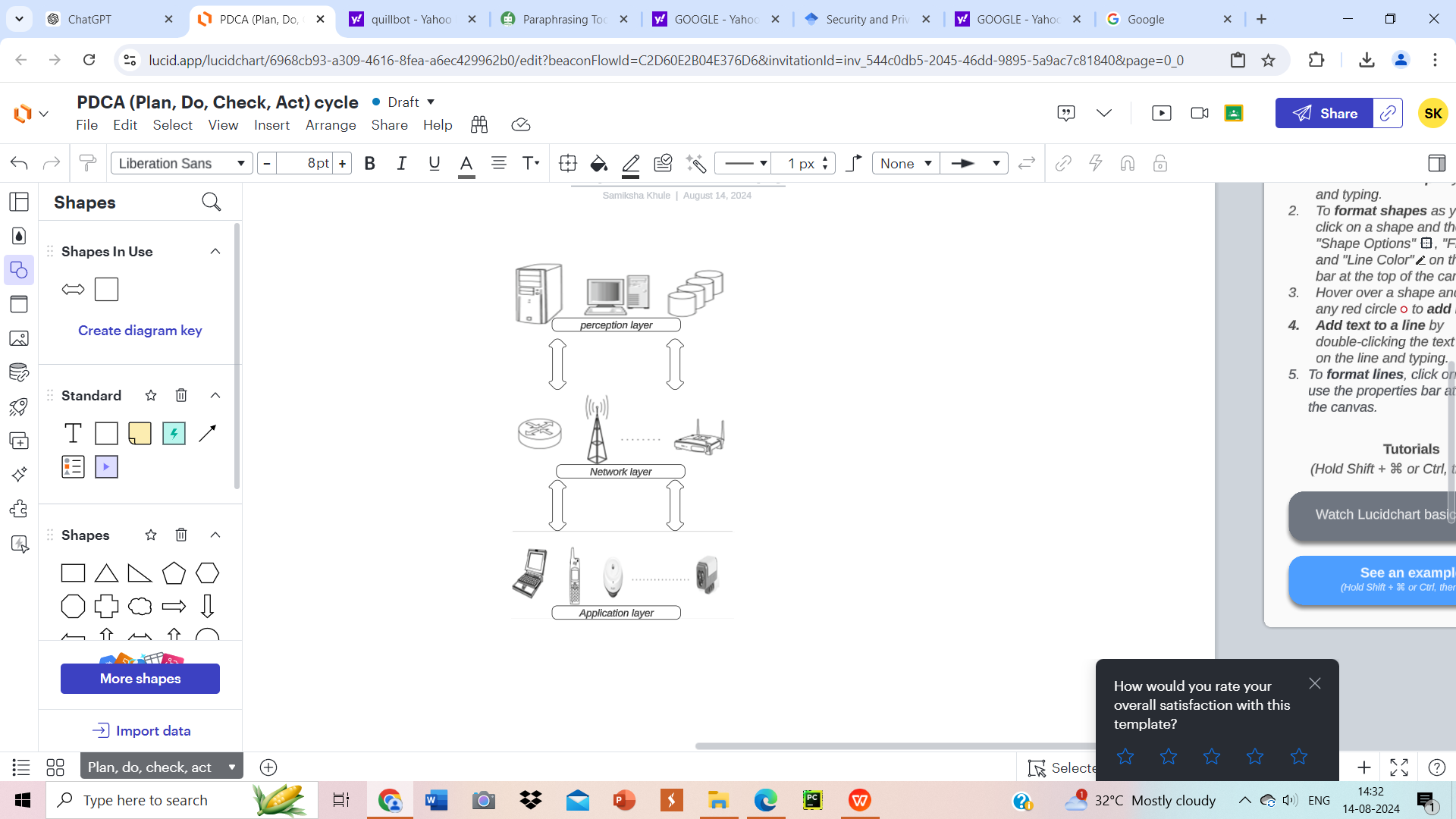


Figure1: IoT Three-Layered Architecture

**Middleware-Based Architecture:**

Middleware-oriented For a vast range of IoT devices and apps to integrate and communicate with each other effectively, IoT architecture is essential. The architecture is divided into multiple discrete levels, all of which are essential to the seamless functioning and flexible expansion of Internet of Things systems. The IoT network's hardware base is made up of the Edge Technology Layer. It consists of embedded systems, sensors, RFID tags, and other gadgets that gather and process environmental data at first. This layer collects vital data for later use and serves as the IoT system's sensory input[13].

The Access Gateway Layer controls how data is transmitted between networks and devices. It manages activities including publishing messages, routing data, and subscribing to other services. This layer makes sure that the Middleware Layer and other layers receive the data that the Edge Technology Layer has collected.

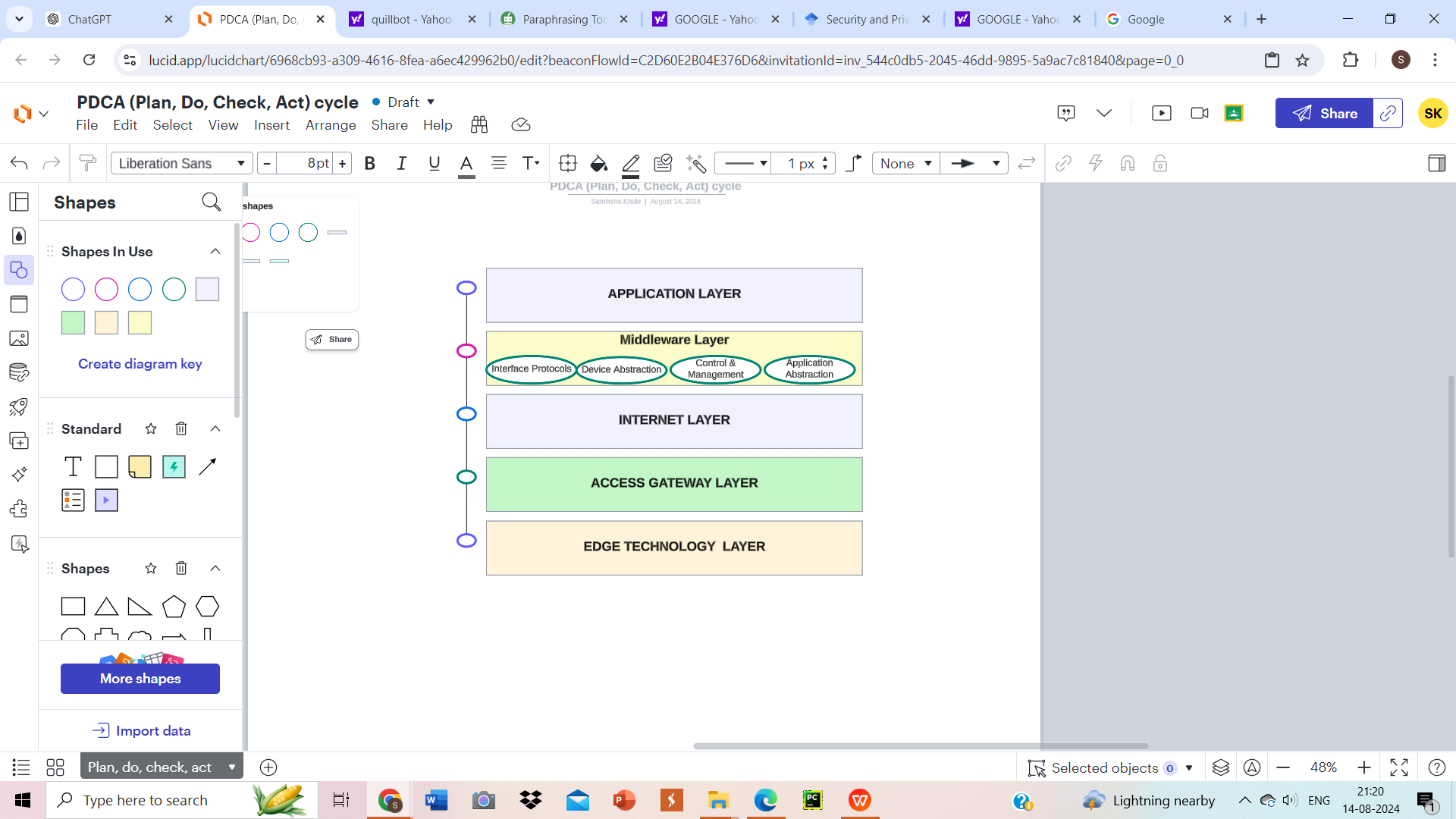


Figure 2: IoT Middleware Based Architecture

Data management and guaranteeing system compatibility rely on the middleware layer. It consists of multiple essential components: Device Abstraction ensures syntactic and semantic interoperability by harmonizing data formats and meanings; Interface Protocols provide technical interoperability by standardizing communication methods; and Control and Management components adjust the behavior of the system based on interactions. Furthermore, users can communicate with and operate devices through the Application Interface[13].

Lastly, the Application Layer provides useful, user-focused applications like intelligent automation, smart home controls, and healthcare monitoring by utilizing the data and services supplied by the lower layers. Middleware technologies, such as AURA, HYDRA, and others, facilitate these functions by improving integration and communication, guaranteeing smooth interoperability between disparate systems. Whatever is considered, this design makes it possible for diverse devices to work together and provide integrated services, providing a coherent and useful Internet of things ecosystem.

**SOA-Based Architecture:**

The integration and administration of many IoT devices are managed in an organized and effective manner in an IoT framework built on Service-Oriented Architecture (SOA). The Abstraction Layer, which offers a standard interface for accessing and controlling a wide variety of IoT devices, is an essential part of this architecture. This layer makes sure that multiple systems work together effortlessly by converting each device's unique functionalities into a common format.  
These Internet of Things devices' services are supervised by the Service Management Layer. By defining essential features while regulating their performance and availability, it makes sure that every service runs efficiently throughout the network. Service reliability and system coherence remain intact by this layer. By combining distinct services from various devices into coherent, application-specific solutions, the Service Composition Layer expands on that structure. This feature allows different services to be integrated to generate apps that are specifically designed to meet the needs of the user. Utilizing the integrated functions, users can engage with the Application Layer at the top by using easily navigable interfaces. This layer enhances the overall usefulness and efficacy of the technology by guaranteeing that the services provided by the IoT system are realistic and quick to use. SOA-based IoT architecture facilitates improved user experience, simple integration, and flexibility through these layers[13].

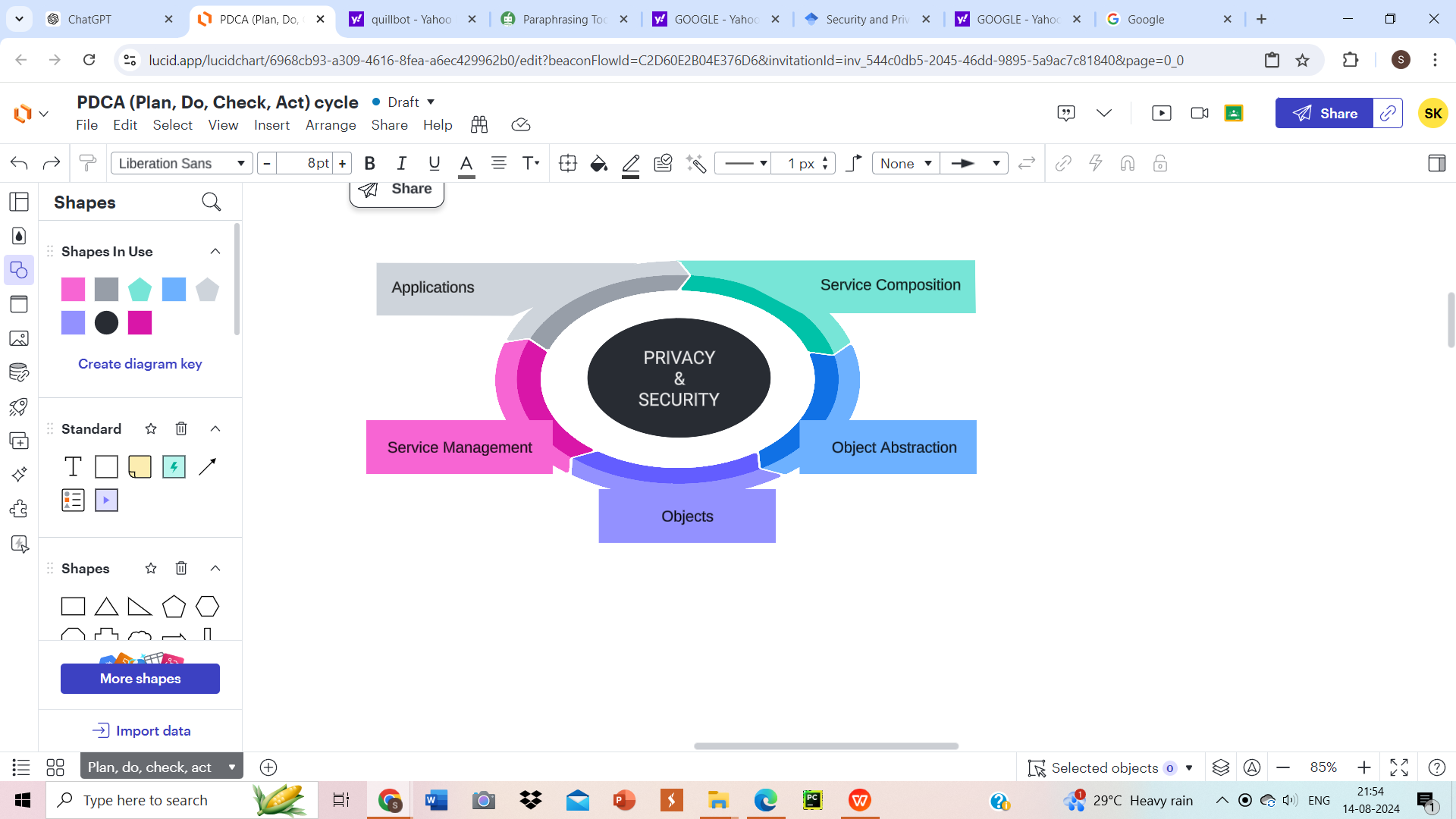


Figure 3: IoT SOA Based Architecture

**Five-Layer Architecture:**

The Perception, Network, Application, and Business levels are the five individual but connected layers that make up the Five-Layer IoT Architecture, which provides a thorough framework for managing and optimizing IoT systems. The foundation of the design is the Perception Layer, which focuses on the physical representation and data collecting of Internet of Things objects. This layer contains gadgets like cameras, RFID tags, and sensors that collect data from the natural world and feed it into the system in real time. The Middleware Layer and the Perception Layer are interlinked by the Network Layer. It is in charge of effectively and consistently transmitting the gathered data, guaranteeing seamless contact between hardware and processing units[14].

The central processing unit is the middleware layer. The function of this component is to gather, store, and examine the information that is sent across the network layer. This layer manages the data and carries out the necessary calculations so that the system can produce insights that are valuable. The Middleware Layer's data processing is applied by the Application Layer to run multiple services and applications. Through direct user interaction, it offers beneficial capabilities and user interfaces that are informed by data-driven insights. The Business Layer takes care of an IoT application's business side. It is in charge of setting pricing policies, controlling delivery of services, and supervising the IoT solution-related business operations. Ensuring robust privacy and security protections is crucial across all of these layers. To protect data integrity and confidentiality across the Internet of Things architecture, these factors are incorporated at each phase. This rigorous methodology offers a comprehensive foundation for scalable, safe, and effective Internet of Things solutions.

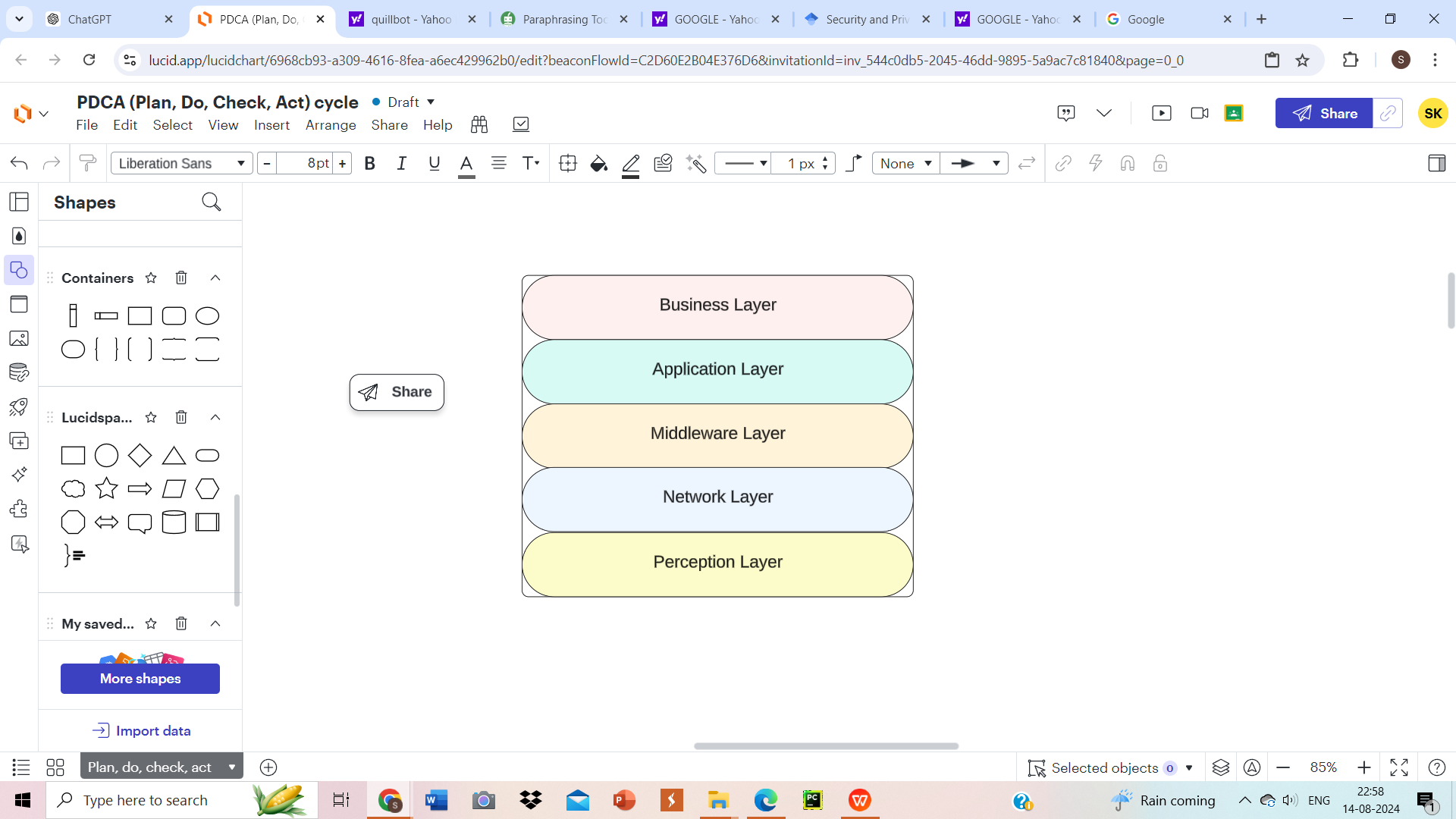


Figure 4: IoT Five Layered Based Architecture

**Social IoT (SIoT):**

Social IoT (SIoT) allows devices to establish and sustain social ties akin to those found in human social networks, improving the usefulness and interactivity of IoT systems[15]. SIoT maximizes the cooperative potential of objects and services by enabling them to function as independent entities that create and modify connections over time.

The Perception Layer establishes social ties between things and collects data from IoT devices. The Network Layer receives this data and the relationship information to be used by numerous Internet of Things applications. The recommendation system of SIoT boosts the system's efficiency and flexibility by providing personalized services that utilize shared data.

**IoT Applications**

Only a small number of the many possible services offered by IoT have become widely accepted. Applications for it greatly improve people's quality of life and fall into several major distinct groups: automotive, medical, military, industrial, environmental, agricultural, retail, and consumer[16].

IoT also affects the domains of personal and social life, smart environments (such as smart homes and offices), healthcare, and logistics and transportation. These several uses highlight the Internet of Things's enormous potential to transform many facets of industry and daily life through revolutionary technology[17].

Table 1: Overview of IoT application and challenges assosciated.

|  |  |  |
| --- | --- | --- |
| **Domain** | **Applications** | **Key Challenges** |
| **Medical** | Remote monitoring, intelligent sensors, connected inhalers, continuous glucose monitoring (CGM) systems, wearable devices, and patient surveillance. | Data security and privacy, handling large data volumes, adherence to protocols, integration of connected technology, and the risk of data overload impacting decision-making[18][19]. |
| **Military** | Disaster response, battlefield communication systems, essential voice operations, tracking of military equipment, threat assessment, intrusion detection, and personnel training[20]. | Security and reliability, data manipulation risks, ensuring strong node authentication, addressing traditional defense mechanisms' inadequacies, maintaining secure communication and data protection[21]. |
| **Industrial** | Manufacturing oversight, intelligent metering, predictive upkeep, automated systems, smart grid management, motion regulation, and machine-to-machine interactions. | Interoperability, security, data analysis and transfer, convergence of IT and OT, handling legacy systems, real-time data analysis, secure data deduplication[22][23]. |
| **Automotive** | Parking management, crash response, vehicle diagnostics, integrated navigation, traffic management, vehicle-to-vehicle communication. | Network congestion and data packet collisions, safeguarding personal information, managing a high number of sensors, ensuring secure data transmission, and maintaining real-time data processing[24]. |
| **Environmental** | Waste management, water management, weather monitoring, animal tracking, environmental protection, smart agriculture. | Real-time assessment of environmental data, ensuring precision in monitoring changes, handling substantial data volumes, guaranteeing sensor reliability, and keeping environmental information up-to-date[25][26]. |
| **Agriculture** | Advanced farming techniques, soil analytics, intelligent greenhouse systems, livestock tracking, and aerial agricultural drones.Top of Form  Bottom of Form | Safeguarding agricultural data, preventing unauthorized access, accurately monitoring climatic conditions, and optimizing resource utilization[27]. |
| **Retail** | Inventory control, product tracking, supply chain management, smart-store applications, connected consumer experiences. | Challenges include infrastructure limitations, data security and privacy concerns, managing large volumes of IoT data, ensuring effective data analysis while protecting customer privacy, and integrating blockchain to secure transactions[28]. |
| **Consumer** | Home automation, connected appliances, building health monitoring, remote device control, smart home applications. | Challenges include managing machine behavior in unpredictable situations, ensuring data security and privacy, achieving interoperability among devices, addressing slow technology adoption, and maintaining user control over automated systems[29]. |

**Security Concerns in IOT**

For IoT systems to be functioning securely and dependably, the fundamental concerns of confidentiality, integrity, authentication, and availability must be addressed.

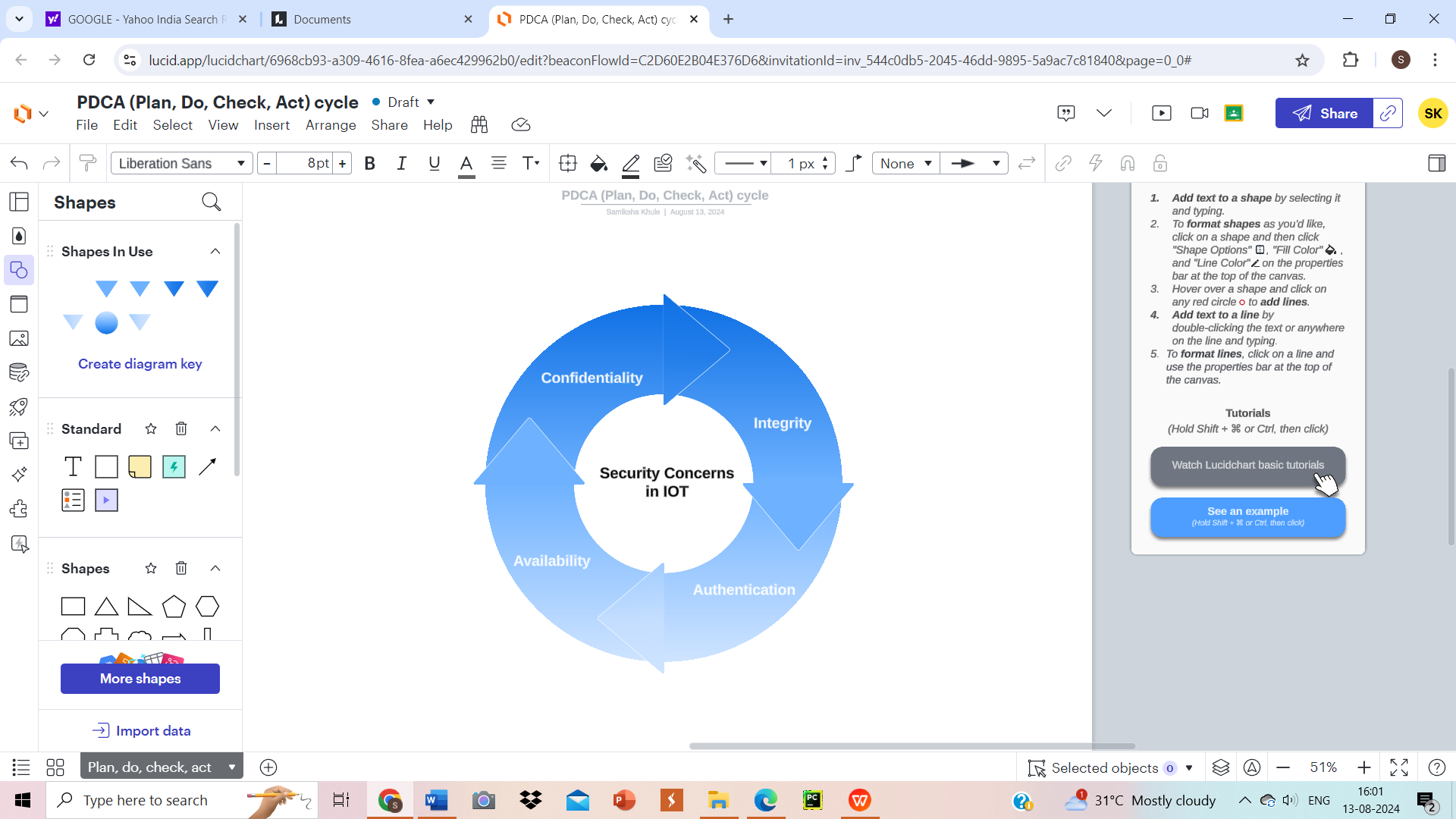


Figure 5 : IoT Security Concerns

**Confidentiality**

End-to-end encryption, secure storage, and efficient access control protocols are just a few of the crucial techniques used to protect data from unwanted access. Data is encrypted from the moment it leaves the sender until it reaches the destination by means of end-to-end encryption, which makes it extremely difficult for unauthorized parties to decode the data while it is being transmitted. Utilizing this technique, data transiting across networks is protected against manipulation and interception. However, whether data is stored on servers or IoT devices, secure storage techniques safeguard it. To avert unauthorized entry or data breaches, this entails utilizing sophisticated encryption methods and safe database setups[30].

Access control measures enhance security by controlling who has access to and can alter data[31]. These systems make sure that only authorized users have the right authorizations to deal with sensitive data by putting strong authentication and authorization procedures in place. When combined, these strategies offer a multi-layered defense that protects the integrity and privacy of data while it's in transit and at rest. Upholding strict security protocols is crucial as IoT devices proliferate with the aim to safeguard sensitive data processing and fight against changing cyberthreats.

**Integrity**

Use of methods like digital signatures, hash functions, and checksums to prevent corruption and unauthorized changes is necessary to guarantee data accuracy and consistency in Internet of Things systems. These strategies are essential for confirming the authenticity and correctness of data, especially in industries where trustworthiness and authenticity are crucial such as industrial control systems and healthcare. By creating distinct codes using the data, checksums and hash functions can be utilized to identify any unauthorized modifications or corruption that may have occurred during transmission or storage[32][33].

Through the verification of data origin and validity, digital signatures give an extra degree of security, guarding against manipulation and fabrication. Robust data integrity controls are indispensable in these sensitive realms, where decision-making and operational stability depend on correct information and high stakes[34]. IoT systems promise that data is dependable and trustworthy throughout its lifecycle by integrating these robust integrity controls. This helps to enable essential services and preserve the accuracy of the data that informs important choices and activities. Data integrity protection is becoming more and more important as IoT develops in order to ensure the general security as well as effectiveness of networked systems[35].

**Authentication**

Verifying that only authorized people and devices can access particular resources or data is crucial when it comes to the Internet of Things (IoT). The limited processing power and memory of many IoT devices renders the usage of efficient yet lightweight means of authentication mandatory. While enabling strong protection, these techniques must be readily available to use within the constraints of the device[36].  
Scalability is a significant consideration since Internet of Things networks frequently have an enormous amount of linked devices. Large-scale authentication requires effective handling by authentication systems in order to guarantee correct identification and authorization of every device without triggering lag or malfunctions in performance. Unauthorized access and prospective security breaches can be avoided with the help of efficient device identification and control.

IoT systems can sustain secure access control and safeguard the dependability and integrity of operations by putting in place simplified and scalable authentication remedies This is especially crucial in numerous kinds of scenarios, including industrial control systems, smart homes, and healthcare facilities. Ensuring the seamless operation of IoT systems and maintaining the credibility of data and network exchanges is made possible by reliable authentication. In conclusion, appropriate authentication promotes the general stability and efficacy of IoT systems in addition to securing access[37].

**Availability**

IoT service and data availability must be guaranteed, particularly for critical systems where downtime might have dire repercussions[38]. It is necessary to take a few critical steps in order to ensure continuous operation. First, it's critical that we protect against Denial-of-Service (DoS) violations. The primary objective of these attacks is to overload systems with traffic such that services remain unavailable. safeguards that protect like rate limitation and traffic filtering work well to reduce this threat.

Implementing fault-tolerant architecture further improves the dependability of the system[39]. Building systems with fault tolerance entails making sure they can keep working even if some of their components break. Maintaining continuous service requires the use of strategies like automatic failover mechanisms, which transfer operations to backup systems after a loss, and redundancy, which involves numerous systems or components performing the same employment opportunity.

Furthermore, efficient resource management is vital as well. Efficient resource allocation and monitoring guarantees that systems can withstand fluctuations in load and mitigate bottlenecks or crashes. IoT networks may guarantee that critical services and data are always accessible by combining three tactics—failure tolerance, resource management, and defense against DoS attacks. This strategy guards against any disruptions that can affect vital applications and services in addition to ensuring operational stability.

**Privacy Concerns in IOT**

The process in which data is collected, shared, and managed in the Internet of Things (IoT) context makes ensuring privacy a critical concern. IoT devices frequently communicate autonomously over the Internet using unique identifiers, therefore it's critical to safeguard the privacy of the data they send. Numerous pieces of information can be automatically collected and transmitted by these devices. Even though a single piece of data could appear innocuous by itself, integrating data from several sources can disclose private information[40].

Everyone should be in possession of their data and be able to determine how much of it they want to share. As things stand, it's hard to keep track of who has access to and uses personal data, making it tough to manage and avoid misuse. Users must be aware of who is using their information and why. For effectively handling the wide variety of IoT devices and apps, a solid authorization and control framework is essential to an IoT privacy solution.

Three primary areas are often the focus of IoT privacy research: data gathering, sharing, and management[41]. IoT data acquiring uses a variety of technologies, such as GPS devices, RFID tags, wireless sensors, and mobile devices with connectivity characteristics. These technologies all carry different privacy dangers. Since sensitive, human-centric data is frequently involved in IoT networks, data management and sharing are especially important. It is crucial to make sure that sensitive data is appropriately safeguarded during network transmission. If not sufficiently protected, wireless communication and other data transfer techniques might raise the danger of exposure. Data that is processed and kept at several nodes also needs to be protected for the purpose to keep its confidentiality and integrity. In the IoT ecosystem, appropriate safeguards must be in place to stop data breaches and maintain personal data.

**Ensure Data Privacy and Protection**  
**Data Encryption:** Use strong encryption techniques to protect data while it's being transmitted and stored[42]. This guarantees that private data, whether traveling across networks or idle in storage systems, is protected from unwanted access and alteration. Encrypting data safely is essential to preserving its integrity and covertness.

**Access Control:**Secure user identities and control access by implementing strong authorization and authentication procedures. This entails putting in place strict permission procedures to guarantee that users may only access the information and systems they are permitted to use, as well as multi-factor authentication to validate users' identity. These procedures considerably increase security and thwart unwanted access.

**Regular Security Updates:**Update IoT systems and devices frequently with the newest patches to address security flaws. Updates that are applied on time improve the overall security posture, guard against potential breaches, and ensure that devices are running the most recent security improvements. It also prevent the exploitation of known vulnerabilities[43].

**Network Segmentation:** Removing IoT devices from critical systems is an important security step that makes a big difference in network safety. Organizations lower their chance of critical systems and sensitive data being damaged by potential breaches by putting IoT devices on different networks or subnets. By reducing the attack surface, minimizing breaches, and streamlining monitoring, this isolation enhances security overall. Moreover, it lets management of security upgrades and rules be simpler and promotes regulatory compliance. In the end, network segmentation for IoT devices contributes to keeping critical systems safe from IoT-related threats.

**Strategies to Enhance IoT Security**  
**1. Implementing strong authentication and encryption mechanisms:** To ensure that only authorized users may access IoT systems, deploy robust authentication techniques like multi-factor authentication. Furthermore, safeguard sensitive data from potential breaches and unwanted access by using encryption during data transfer and storage[44].

1. **Performing frequent security audits and penetration testing to detect weaknesses:** Conduct penetration tests and security audits on a regular basis to find weaknesses in IoT systems. These assessments assist in identifying possible risks and vulnerabilities, enabling prompt correction and enhancing the IoT infrastructure's overall security posture.
2. **Creating and enforcing rigorous access control regulations to prevent unwanted access:** Implement stringent access control procedures and put them into place to restrict who has access to IoT devices and data. Ensure sure that permissions are only given out in accordance with roles and requirements in order to lower the possibility of internal threats and illegal access[45].
3. **Using network segmentation to segregate IoT devices and reduce potential attack vectors:** To reduce the impact of such breaches, divide up IoT devices into distinct network zones. By keeping security threats contained within discrete segments, this strategy lowers total risk by preventing them from propagating throughout the network.
4. **Ensure that all IoT devices and software are regularly updated with the latest security patches and firmware upgrades:** Implement the most recent firmware upgrades and security fixes to IoT devices' software on a regular basis. By strengthening the device's defenses against fresh attacks and addressing established weaknesses, this technique ensures continued strong security[46].

**Conclusion**

The Internet of Things (IoT) refers to a wide range of interconnected technologies, with enhanced information and communication systems playing an important part in the creation of smart surroundings. The Internet of Things, or IoT, has completely changed the way we use technology by enabling the connection of multiple devices to improve productivity and ease of use in a variety of industries. To preserve sensitive data and guarantee system integrity, this enormous network of interconnected devices raises serious security and privacy issues that need to be carefully handled. The enforcement of comprehensive security strategies is needed in order to tackle all of these challenges. This entails implementing robust authentication techniques, including multi-factor authentication, to confirm user identities and employing encryption to protect data both in transit and storage. For possible vulnerabilities to be found and fixed before they can be exploited, regular security audits and penetration tests are essential. Furthermore, by limiting access to IoT systems to just those who are permitted, stringent access controls reduce the possibility of both internal and external vulnerabilities. Isolating IoT devices from important systems through network segmentation is essential for preventing potential intrusions and streamlining security management. Maintaining the security patches installed on all IoT devices and related software is equally crucial since they fix known vulnerabilities and fortify protections against new threats. IoT technology offers incredible breakthroughs, it is crucial to manage the security and privacy issues associated with it. Organizations may secure their IoT systems, protecting data integrity and promoting trust in this quickly developing technology, by putting strong authentication, encryption, frequent security assessments, strict access limits, network segmentation, and timely updates into place.

**REFRENCES**

1. Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102
2. Conti, M.; Dehghantanha, A.; Franke, K.; Watson, S. Internet of Things security and forensics: Challenges and opportunities. Future Gener. Comput. Syst. 2018, 78, 544–546.
3. Chanal, P. M., & Kakkasageri, M. S. (2020). Security and privacy in IoT: a survey. Wireless Personal Communications, 115(2), 1667-1693.
4. Miao, W., Ting, L., Fei, L., Ling, S., & Hui D. (2010). Research on the architecture of internet of things. In Proceedings of the IEEE international conference on advanced computer theory and engineering (pp. 484–487), China.
5. Jinxin, Z., & Mangui, L. (2010). A new architecture for converged internet of things. In Proceedings of the international conference on internet technology and applications (pp. 1–4), Brazil.
6. Kraijak, S., & Tuwanut, P. (2015). A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends. In Proceedings of The 11th international conference on wireless communications, networking and mobile computing (WiCOM 2015) (pp. 1–5), China.
7. Inge, G. (2008). Architecture for the internet of things (IoT): API and interconnect. In Proceedings of the 2nd international conference on sensor technologies and applications (pp. 802–807), Syria.
8. Mashal, I., Alsaryrah, O., Chung, T. Y., Yang, C. Z., Kuo, W. H., & Agrawal, D. P. (2015). Choices for interaction with things on internet and underlying issues. Journal of Ad Hoc Networks, 28, 68–90.
9. Said, O., & Masud, M. (2013). Towards internet of things: Survey and future vision. Journal of Computer Networks, 5(1), 1–17.
10. Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010). Research on the architecture of internet of things. In Proceedings of the 3rd IEEE international conference on advanced computer theory and engineering, China.
11. Chowdhury, S. N., Kuhikar, S. M., & Dhawan, S. (2015). IoT architecture: A survey. Journal of Industrial Electronics and Electrical Engineering, 3(5), 88–92.
12. Sethi, P., & Sarang, S. R. (2017). Internet of things: Architectures, protocols, and applications. Journal of Electrical and Computer Engineering, 17, 1–25.
13. Mughaid, A., Obeidat, I., Abualigah, L., Alzubi, S., Daoud, M. S., & Migdady, H. (2024). Intelligent cybersecurity approach for data protection in cloud computing based Internet of Things. International Journal of Information Security, 23(3), 2123-2137.
14. Sani, A.S., Yuan, D., Jin, J., Gao, L., Yu, S., Dong, Z.Y.: Cyber security framework for Internet of Things-based Energy Internet. Futur. Gener. Comput. Syst. 93, 849–859 (2019).
15. Liu, X.; Zhao, M.; Li, S.; Zhang, F.; Trappe, W. A security framework for the internet of things in the future internet architecture. Future Internet 2017, 9, 27.
16. Dey, N., Shinde, G., Mahalle, P., & Olesen, H. (2019). The internet of everything: Advances, challenges and applications.
17. Zaidan, A. A., & Zaidan, B. B. (2020). A review on intelligent process for smart home applications based on IoT: Coherent taxonomy, motivation, open challenges and recommendations. Journal of Artifcial Intelligence Review, 53, 141–165.
18. Yang, Z., Zhou, Q., Lei, L., Zheng, K., & Xiang, W. (2016). An IoT-cloud based wearable ECG monitoring system for smart health care. Journal of Medical Systems, 40(12), 286–296.
19. Gil, D., Terol, R. M., Azor, J., & Szymanski, J. (2017). An IoT-based computational framework for healthcare monitoring in mobile environments. Sensors, 17(10), 1–25.
20. Fraga-Lamas, P., Fernández-Caramás, T. M., Suárez-Albela, M., Castedo, L., & González-López, M. (2016). A review on internet of things for defense and public safety. Sensors, 16, 1644.
21. Zielinski, Z., Chudzikiewicz, J., & FurtakAn, J. (2019). Approach to integrating security and fault tolerance mechanisms into the military IoT: Technology, communications and computing. In Security and fault tolerance in internet of things (pp. 111–128).
22. Mazzei, D., Baldi, G., Fantoni, G., Montelisciani, G., Pitasi, A., Ricci, L., et al. (2020). A blockchain tokenizer for industrial IoT trustless applications. Journal of Future Generation Computer Systems, 105, 432–445.
23. Sharma, S., & Sain, H. (2020). Fog assisted task allocation and secure deduplication using 2FBO and MoWo in cluster-based industrial IoT (IIoT). Journal of Computer Communications, 152, 187–199.
24. Dimitrakopoulos, M. G. (2011).Intelligent transportation systems based on internet-connected vehicles: Fundamental research areas and challenges. In Proceedings of The 11th IEEE international conference on information technology and system telecommunications (pp. 145–151), Cyprus
25. Lagkas, T., Eleftherakis, G., Dimopoulos, K., & Zhang, J. (2020). Signal strength based scheme for following mobile IoT devices in dynamic environments. Journal of Pervasive and Mobile Computing, 65, 1–24.
26. Elmustafa, S. A. A., & Mujtaba, E. Y. (2019). Internet of things in smart environment: Concept, applications, challenges, and future directions. International Scientifc Journal, 134, 1–51.
27. Punitha, A., & Geetha, V. (2018). Review on challenges and opportunities of IoT in agriculture. Journalof Advanced Research in Applied Science, 5(11), 25–31.
28. Dlamini, N. N., & Johnston, K. (2016). The use, benefts and challenges of using the internet of things (IoT) in retail businesses—A literature review. In Proceedings of the international conference on advances in computing and communication engineering (ICACCE) (pp. 430–437), Durban.
29. Quevedo, J., Corujo, D., & Aguiar, R. (2014). Consumer driven information freshness approach for content centric networking. In Proceedings of the IEEE information centric networking to support disastar management workshop on name-oriented mobility (pp. 482–487), Canada.
30. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Journal of Ad Hoc Networks, 10(7), 1497–1516.
31. Usman, M., Ahmed, I., Aslam, M. I., Khan, S., & Shah, U. A. (2017). SIT: A lightweight encryption algorithm for secure internet of things. Journal of Advanced Computer Science and Applications, 8(1), 12–20.
32. Atzori, L., Iera, A., & Morabito, G. (2017). Preserving data integrity in IoT networks under opportunistic data manipulation. In Proceedings of the international conference on big data intelligence and computing and cyber science and technology congress (pp. 446–453), USA.
33. Zhang, G., Kou, L., Zhang, L., Liu, C., Da, Q., & Sun, J. (2017). A new digital watermarking method for data integrity protection in the perception layer of IoT. Journal of Security and Communication Networks, 2017, 1–12.
34. Fongen, A. (2012). Identity management and integrity protection in the internet of things. In Proceedings of The 3rd international conference on emerging security technologies (Vol. 4, pp. 111–114), Portugal.
35. Li, C., Liu, Q., & Wang, G. (2014). Survey of integrity detection methods in internet of things. In Proceedings of The 13th IEEE international conference on trust, security and privacy in computing and communications (pp. 906–913), Finland.
36. Joshitta, S. M., & Arockiam, L. (2016). Authentication in IoT environment: A survey. Journal of Advanced Research in Computer Science and Software Engineering, 6(10), 140–145.
37. Sharaf-Dabbagh, Y., & Saad, W. (2016). Authentication of devices in the internet of things. In Proceedings of the IEEE 17th international symposium on a world of wireless, mobile and multimedia networks (Vol. 32, No. 6), Portugal.
38. Pokorni, S. (2018). Reliability and availability of the internet of things. Military Technical Courier (pp. 588–600).
39. Kolisnyk, M., Kharchenko, V., Piskachova, I., & Bardis, N. (2017). A Markov model of IoT system availability considering DDos attacks and energy modes of server and router. In Proceedings of the international conference on ICT education, research and industrial applications (pp. 1–14), Ukren
40. Vignesh, R., & Samydura, A. (2017). Security on internet of things (IoT) with challenges and countermeasures. Journal of Engineering Development and Research, 5(1), 417–423.
41. Usman, M., Ahmed, I., Aslam, M. I., Khan, S., & Shah, U. A. (2018). Preserving privacy in internet of things: A survey. Journal of Information Technology, 10, 189–200
42. Khan R, Khan SU, Zaheer R, Khan S (2012) Future Internet the Internet of things architecture, possible applications and key challenges. In: 2012 10th international conference on frontiers of information technology. IEEE, pp 257–260
43. Weis SA, Sarma SE, Rivest RL, Engels DW (2004) Security and privacy aspects of low-cost radio frequency identification systems. In: Hutter D, Mller G, Stephan W, Ullmann M (Eds) Security in pervasive computing. Number 2802 in Lecture Notes in Computer Science. Springer, pp 201–212
44. Dimitriou T (2005) A lightweight RFID protocol to protect against traceability and cloning attacks. In: Security and privacy for emerging areas in communications networks, 2005. IEEE, pp 59– 66
45. Borgohain T, Kumar U, Sanyal S (2015) Survey of security and privacy issues of internet of things. arXiv:1501.02211 [cs]
46. Weber Rolf H (2010) Internet of Things new security and privacy challenges. Comput Law Secur Rev 26:23–30