IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁙ Impact Factor 8.066 ⁙ Peer-reviewed / Refereed journal ⁙ Vol. 10, Issue 7, July 2023

DOI: 10.17148/IARJSET.2023.107126

Securing the Internet of things: Challenges and Solutions

Parth Kangralkar[1], Vinayak Kori[2], Pavan Mitragotri[3]

Department of MCA, KLS Gogte Institute of Technology/VTU, India[1]

Department of MCA, KLS Gogte Institute of Technology/VTU, India[2]

Department of MCA, KLS Gogte Institute of Technology/VTU, India[3]

Abstract: The rapid proliferation of the Internet of Things (IoT) has brought about heightened concerns regarding system security. Organizations must focus their efforts on safeguarding IoT devices, as even a single vulnerability could result in catastrophic system failures or large-scale cyberattacks. IoT security teams are grappling with growing complexities, including diverse inventories, operational challenges, and increasing threats. In particular, wireless communication networks, widely used in various sectors such as military, healthcare, and transportation, are highly susceptible to security breaches. As IoT continues to shape our future, ensuring data integrity, confidentiality, authentication, and authorization in IoT networks remains paramount. To tackle these pressing challenges, extensive research and deployment of robust security and privacy protocols are essential to protect against potential attacks and secure the promising potential of IoT applications. [1,2]

Keywords: Internet of Things (IoT), security issues in IoT, security, privacy, data integrity, confidentiality, authentication, access control, IoT applications.

I. INTRODUCTION

The Internet of Things (IoT) is a transformative technology that has the potential to reshape various aspects of our lives and industries. It involves connecting a wide range of devices, objects, and systems to the internet, allowing them to communicate and exchange data with each other, making them "smart" and capable of autonomous decision-making and actions. The concept of IoT was first introduced by Kevin Ashton in 1999, and since then, it has rapidly evolved due to advancements in mobile communication, Wireless Sensor Networks (WSN), Radio Frequency Identification (RFID), and cloud computing. These developments have made communication between IoT devices more seamless and efficient [4].

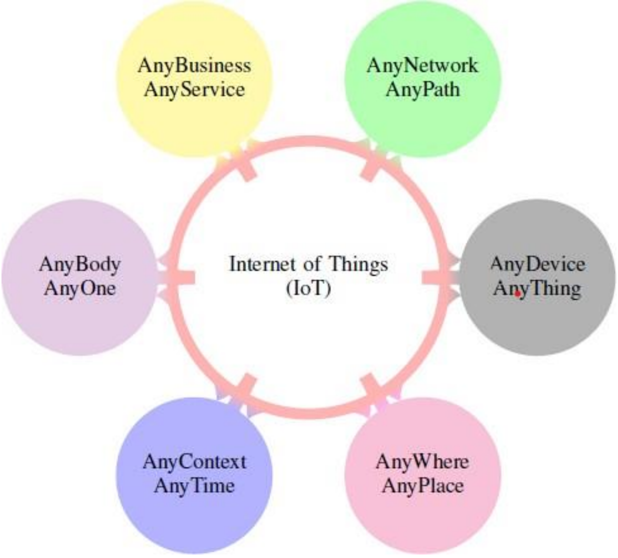
The IoT ecosystem includes an extensive array of devices, ranging from smartphones, personal computers, and tablets to various embedded devices used in different industries. These devices rely on cost-effective sensors and wireless communication systems to share data with each other and a centralized system. The centralized system processes the information and delivers it to the intended destinations, enabling real-time decision-making and actionable insights.

One of the key advantages of IoT is its ability to merge the virtual and real worlds on the same platform. As our daily routines become more focused on the virtual world provided by the internet, IoT offers the integration of physical and digital experiences. This integration has the potential to create a superior world for human beings by optimizing processes, enhancing efficiency, and providing more personalized services. IoT applications span a wide range of sectors, including smart living, smart healthcare, smart transportation, smart cities, and more [2,4]. The adoption rate of IoT devices is growing rapidly, and it is estimated that billions of devices will be connected to the internet by the year 2020, generating significant revenue in various industries.

However, along with its potential benefits, IoT also brings forth various security and privacy challenges. Many IoT devices and applications are not adequately designed to handle security threats, making them vulnerable to attacks and intrusions. Common security concerns in IoT networks include confidentiality, authentication, data integrity, access control, and secrecy [5]. Hackers and intruders target IoT devices regularly, and a significant percentage of these devices are found to be easily exploitable.

To ensure the security of IoT devices and networks, efficient security mechanisms and protocols are essential. 1,6] Addressing these security and privacy issues is crucial to unlocking the full potential of IoT technology and its positive impact on society and industries.

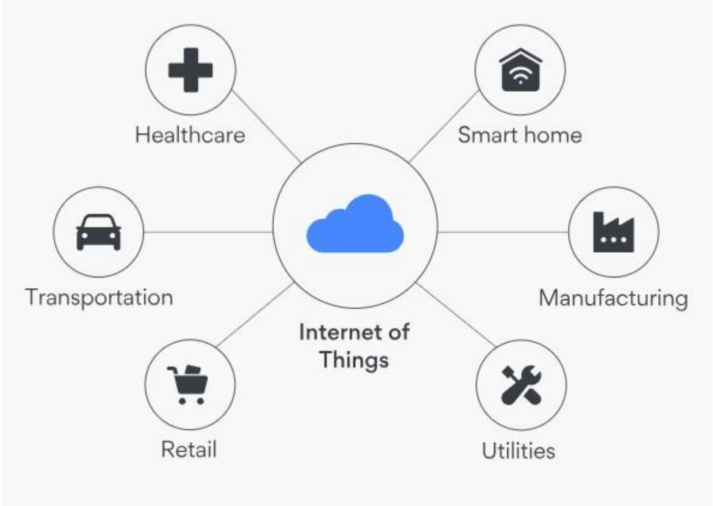
DOI: 10.17148/IARJSET.2023.107126



Definition of IOT

The Internet of Things (IoT) is a network of interconnected devices that can communicate and exchange data with each other over the internet.

Example



II. PURPOSE

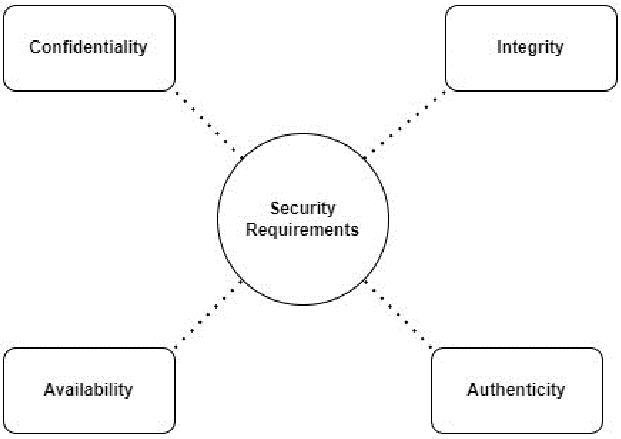
Securing the Internet of Things (IoT) is a big challenge because many smart devices are connected, and they can have weak security. This could lead to problems like data breaches or hackers taking control of devices. To fix this, we need strong security measures like better encryption and secure ways to update devices. Everyone involved, like device makers and users, must work together and follow security guidelines to make IoT safer. By doing this, we can protect our data, privacy, and the future of the IoT.

In the world of the Internet of Things (IoT), where smart devices are all around us, keeping things safe is super important. But it's not easy because these devices can have weak spots that hackers might use to cause trouble. To make IoT more secure, we need to use strong methods like powerful passwords and special codes to protect information. It's also essential for everyone involved, like companies making the devices and people using them, to team up and follow safety rules. By doing this, we can create a safer IoT world where our personal data and privacy are well-protected.

DOI: 10.17148/IARJSET.2023.107126

III. SECURITY REQUIREMENTS

Defining security requirements is crucial to ensuring the safety and reliability of IoT systems. The security principles mentioned in the passage are fundamental aspects that need to be addressed in any IoT implementation. [35,36,37] Let's further elaborate on each security requirement:



1. **Confidentiality:** Confidentiality ensures that sensitive information and data are protected from unauthorized access. In the context of IoT, it means that unauthorized services, devices, or individuals should not be able to access private or sensitive data transmitted or stored within the IoT ecosystem. This includes personal information, proprietary data, and any other sensitive information that should only be accessible to authorized parties.
To achieve confidentiality, measures like encryption, access control, and secure communication protocols are commonly employed. Encryption ensures that data is scrambled and can only be deciphered by authorized parties with the appropriate decryption keys [1,10]. Access control mechanisms restrict access to data and resources based on user roles and permissions, minimizing the risk of unauthorized access.

2. **Integrity:** Integrity ensures that data and IoT devices remain unaltered and trustworthy throughout their lifecycle. It means that data should not be modified, tampered with, or corrupted by unauthorized users or objects. Additionally, it involves validating the authenticity of data to ensure it has not been manipulated during transmission or storage.
To maintain integrity, techniques such as data integrity checks, digital signatures, and blockchain technology are utilized. Data integrity checks verify the integrity of data during transmission or storage, ensuring it remains unchanged. Digital signatures provide a way to validate the origin and integrity of data, ensuring that data is coming from a legitimate and verified source. Blockchain, as an immutable and decentralized ledger, can be employed to enhance data integrity in distributed IoT systems.

3. **Availability:** Availability ensures that IoT systems and services are accessible and operational when required. This includes the proper functioning of IoT devices, computing resources, and communication channels. In the context of IoT, availability is crucial because interruptions or failures can have severe consequences, especially in critical applications like healthcare, transportation, and industrial automation.

To maintain availability, redundancy, failover mechanisms, and real-time monitoring are commonly employed. Redundancy involves deploying backup systems and components, so if one fails, the backup takes over to maintain continuous operation. Failover mechanisms automatically switch to backup systems when a failure is detected. Real-time monitoring allows proactive identification of potential issues, enabling swift action to prevent or mitigate downtime.

4. **Authenticity:** Authenticity ensures that participants in IoT transactions are genuinely who they claim to be. This principle is critical to prevent unauthorized access, data manipulation, and fraudulent activities within the IoT ecosystem. It involves verifying the identity of users, devices, and services before granting access or allowing transactions. To ensure authenticity, various authentication methods can be implemented, such as two-factor authentication, biometric authentication, and public-key infrastructure (PKI). Two-factor authentication requires users to provide two forms of identification, making it harder for unauthorized users to gain access. Biometric authentication utilizes unique physical characteristics like fingerprints or facial recognition for identification. PKI uses cryptographic keys to verify the identity of parties involved in transactions, providing a robust method for ensuring authenticity.

DOI: 10.17148/IARJSET.2023.107126

By adhering to these security requirements and principles, IoT system developers and administrators can significantly reduce the risks posed by potential security threats and create a more secure and trustworthy IoT ecosystem.

IV. IOT APPLICATIONS

1. **Smart homes:** IoT devices have made it possible for homeowners to have greater control over their living spaces, leading to energy savings, increased security, and improved comfort.[3] Smart thermostats, lighting systems, security cameras, and other connected devices work together to create a seamless and interconnected environment.
2. **Healthcare:** IoT has brought significant advancements in remote patient monitoring and telemedicine [1,8]. Wearable health trackers and remote monitoring systems allow healthcare professionals to gather real-time data on patients' health conditions, enabling timely intervention and better management of chronic conditions.
3. **Industrial IoT:** I0T has transformed the industrial landscape by enabling real-time monitoring and predictive maintenance of equipment and machinery. This leads to increased operational efficiency, reduced downtime, and cost savings.
4. **Transportation sector:** IoT has facilitated the development of connected vehicles and smart transportation systems. Vehicle-to-vehicle communication and smart infrastructure improve road safety and traffic management, enhancing the overall transportation experience.

V. SECURITY ISSUES IN IOT

Security issues in IoT (Internet of Things) are a significant concern due to the large number of interconnected devices and the potential impact of attacks on these systems. Here are some common security issues related to IoT:

1. **Denial of Service (DoS) Attack:** A DoS attack aims to overwhelm a system's resources, such as memory, CPU, or bandwidth, causing legitimate users to be denied access to network services. Attackers achieve this by flooding the network with a high volume of traffic, rendering the system unresponsive or ineffective. [21,22]
2. **Replay Attack:** A replay attack involves capturing and storing legitimate data exchanged during a communication session. The attacker then replays or resends this data to deceive the system into thinking it is coming from a trusted source, leading to unauthorized actions or compromising the security of the system. [18,22]
3. **Password Guessing Attack:** This attack involves attempting to guess a user's password by systematically trying various combinations until the correct one is found. Weak or easily guessable passwords are particularly vulnerable to this type of attack.

Example: A hacker targets an IoT device with a default or weak password. By systematically trying common passwords or using a brute-force attack, the hacker successfully gains access to the device, allowing them to control it or compromise the entire IoT network it's connected to. [17,20,22]

Spoofing Attack: In a spoofing attack, an attacker impersonates a trusted entity by falsifying information or network parameters. By doing so, the attacker gains the trust of the system or its users, allowing them to perform unauthorized actions.

4. **Data Confidentiality:** IoT devices often collect and transmit sensitive data, such as personal information, location data, and health-related data. Ensuring data confidentiality is crucial to prevent unauthorized access or data leaks that could lead to privacy violations and identity theft.
5. **Authentication and Authorization:** IoT devices and services require robust authentication and authorization mechanisms to ensure that only legitimate users and devices have access to sensitive data and functionalities. Weak authentication can lead to unauthorized access and potentially malicious control of devices.
6. **Integrity of Data:** Maintaining data integrity is critical in IoT applications. Tampered data could lead to incorrect decisions or actions being taken based on faulty information, especially in critical applications like healthcare and industrial control.
7. **Physical Security:** In many IoT deployments, physical access to devices is possible. Attackers gaining physical access can tamper with devices, extract sensitive data, or implant malicious hardware.[13]
8. **Resource Constraints:** Many IoT devices operate with limited resources, including processing power, memory, and energy. Implementing strong security measures within these constraints can be challenging.
9. **Secure Firmware and Software Updates:** Ensuring secure over-the-air updates for IoT devices is crucial to patch vulnerabilities and address security issues. However, implementing a reliable update mechanism without introducing new risks can be complex.
10. **Insider Attack:** An insider attack occurs when a legitimate entity with authorized access to the system deliberately or accidentally compromises the system's security. This could be an employee, contractor, or anyone with privileged access to the IoT infrastructure. [4,12]

DOI: 10.17148/IARJSET.2023.107126

Mitigating these security issues requires a combination of technical measures and best practices:

- Implementing robust access control mechanisms to restrict unauthorized access to devices and systems.
- Encrypting data transmission to ensure confidentiality and integrity.
- Deploying intrusion detection systems to detect and respond to unusual or malicious activities.
- Regularly updating and patching devices and software to address known vulnerabilities.
- Using strong authentication methods, such as two-factor authentication, to prevent unauthorized access.
- Educating users about security best practices and the potential risks associated with IoT devices.

It's essential for IoT developers, manufacturers, and users to prioritize security and privacy to ensure a safer and more reliable

IoT ecosystem. As IoT technology continues to evolve, addressing these security challenges will remain crucial to its widespread adoption and success.

EXAMPLES OF IOT ATTACK

An example of Trespass attack, hacking a door lock.

An attacker uses a vulnerability in the door lock's firmware to gain unauthorized access. By exploiting the weakness, the attacker bypasses the authentication mechanism, effectively unlocking the door without a valid key or passcode [1]. This allows the intruder to gain entry to a secure facility or property, posing a significant security threat.

VI. SECURITY CHALLENGES AND SOLUTIONS

The Internet of Things (IoT) has brought about numerous benefits, but it also comes with its fair share of challenges. Here are some of the key challenges faced by IoT and potential solutions to address them:

1. **Security and Privacy:** The proliferation of IoT devices has introduced new cyber security challenges, as many of these devices lack robust security measures. This vulnerability has led to an increasing number of cyber-attacks, compromising user data, and even affecting critical infrastructure. To address these concerns, implementing strong encryption and authentication mechanisms is crucial to secure the communication between IoT devices and networks. Additionally, timely software updates and security patches should be provided to address known vulnerabilities promptly. Privacy is another significant concern in the IoT landscape. With the massive amount of data generated by IoT devices, there is a risk of unauthorized data collection and usage, which can infringe on users' privacy rights. Privacy-by-design principles should be adhered to during the development of IoT devices and services. [9,11] This approach ensures that privacy considerations are integrated into the design process, allowing for data anonymization or pseudonymization whenever possible. Transparent data collection and usage policies are essential to gain users' trust and confidence in the IoT ecosystem.

SOLUTION: Strong encryption and authentication mechanisms: Implementing robust encryption protocols, such as AES (Advanced Encryption Standard), ensures that data transmitted between IoT devices and networks remains confidential and protected from unauthorized access. Additionally, strong authentication methods, such as two-factor authentication (2FA) or biometric authentication, add an extra layer of security to prevent unauthorized access to IoT devices and services.

Regular software updates and security patches: IoT devices should receive timely software updates and security patches from manufacturers to address known vulnerabilities and stay protected against emerging threats. Automated update mechanisms can ensure that devices remain up-to-date with the latest security fixes.

Privacy-by-design principles: Adopting privacy-by- design principles ensures that privacy considerations are integrated into every stage of IoT device development. This includes minimizing data collection to only essential information, anonymizing or pseudonymizing data wherever possible, and providing users with granular control over their data. [17,19,22]

Real-World Example: Smart Home Security Systems

In the realm of smart homes, companies like Ring (owned by Amazon) and Nest (owned by Google) implement strong encryption and authentication mechanisms to secure communication between their IoT devices (e.g., smart doorbells, cameras) and the cloud servers. This ensures that users' video feeds and other sensitive data remain protected from unauthorized access.

DOI: 10.17148/IARJSET.2023.107126

2. Interoperability: The lack of interoperability among IoT devices and systems remains a persistent challenge. Incompatibility between different devices and communication protocols can hinder seamless data exchange and cooperation between devices from various manufacturers. This issue becomes more critical as the number and diversity of IoT devices continue to grow.

To promote interoperability, the adoption of open standards and protocols becomes crucial. Open standards ensure that IoT devices can communicate and work together, regardless of their origin or manufacturer. [4,9] By adhering to common standards, companies can avoid vendor lock-in and create a more open and competitive IoT market.
Moreover, IoT platforms that provide middleware services can act as a bridge between different devices and protocols, enabling interoperability and facilitating data exchange. Such platforms can simplify the integration process and encourage collaboration between various IoT stakeholders.

SOLUTION: Open standards and protocols: Encouraging the adoption of open standards and communication protocols allows IoT devices from different manufacturers to communicate seamlessly. Popular open standards in IoT include MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol), and OPC UA (Open Platform Communications Unified Architecture).

IoT platforms as middleware: IoT platforms can act as middleware to bridge the gap between devices with different communication protocols. These platforms provide translation services and data normalization, allowing devices to understand and communicate with each other effectively. [17,19,22]

Real-World Example: Smart Cities
Various cities around the world are embracing IoT to build smart city infrastructure. In this context, open standards and protocols are utilized to enable interoperability between diverse devices and systems. For instance, Singapore's "Smart Nation" initiative promotes the use of open standards for data sharing across various urban services, such as transportation, waste management, and energy.

3. Scalability: The scalability of IoT infrastructure is a pressing concern, especially with the exponential growth of IoT devices. The sheer volume of data generated by these devices can overload networks and data processing systems if not managed effectively.

Cloud computing and edge computing are two solutions that address the scalability challenge. Cloud computing allows data to be stored and processed in remote data centers, reducing the burden on individual devices and enabling efficient data analysis. [15] On the other hand, edge computing involves processing data locally on IoT devices or gateway devices, closer to the data source. This approach reduces data transfer to the cloud, improves real-time analytics capabilities, and minimizes network congestion.

Furthermore, decentralized architectures, such as blockchain, offer potential benefits in terms of scalability and data integrity. Blockchain's distributed nature ensures that data is stored and verified across a network of nodes, enhancing reliability and reducing the risk of a single point of failure.

SOLUTION: Cloud computing and edge computing: Cloud computing enables IoT devices to offload data processing and storage to remote data centers, reducing the burden on individual devices. Edge computing, on the other hand, allows data processing to occur locally on IoT devices or gateways, reducing latency and data transfer to the cloud.

Decentralized architectures like blockchain: Blockchain technology can be used in IoT to create a decentralized and tamper-resistant network of devices. This approach can improve scalability, security, and reliability, as it eliminates the need for a central authority and reduces the risk of single points of failure.

Real-World Example: Industrial IoT (IIoT) Applications
In industrial settings, IoT technologies are applied to monitor and manage complex processes. Edge computing is utilized to process critical data locally on industrial machines, reducing latency and ensuring real-time insights. This is implemented in industries like manufacturing and oil and gas, where timely data analysis is essential for optimizing production processes and preventing downtime. [17,19,22]

4. Power Management: The majority of IoT devices rely on battery power, making power management a critical concern. Prolonging the battery life of these devices is essential to reduce maintenance efforts and enhance user convenience.

DOI: 10.17148/IARJSET.2023.107126

Low-power hardware design is a fundamental approach to minimize power consumption in IoT devices. Energy- efficient components, such as microcontrollers and sensors, can reduce power requirements without compromising functionality.[16,19] Additionally, power-efficient communication protocols, like Bluetooth Low Energy (BLE) or Zigbee, can enable devices to communicate with minimal energy expenditure.

Power harvesting techniques offer an innovative solution to replenish or supplement device batteries. Technologies like solar panels, kinetic energy harvesting (from motion), or thermal energy harvesting (from temperature differentials) can help extend the operational life of IoT devices by harnessing energy from the environment.

SOLUTION: Low-power hardware design: IoT devices should be designed with energy-efficient components, microcontrollers, and sensors that consume minimal power during operation. Hardware optimization can significantly extend the battery life of IoT devices.

Energy-efficient communication protocols: Choosing communication protocols like Bluetooth Low Energy (BLE) or Zigbee, which have lower power requirements, helps minimize energy consumption during data transmission.

Power harvesting techniques: By integrating power harvesting technologies, such as solar panels, piezoelectric materials, or thermoelectric generators, IoT devices can harvest energy from the environment, reducing or eliminating the need for battery replacements. [17,19,22]

Real-World Example: Wearable Devices
Wearable IoT devices, such as fitness trackers and smartwatches, rely on power management techniques to extend battery life. By using low-power hardware and energy-efficient communication protocols, these devices can operate for extended periods without requiring frequent recharging.

5. Data Management and Analytics: With the vast amount of data generated by IoT devices, efficient data management and analytics become essential to derive meaningful insights and facilitate informed decision-making.
Edge computing plays a crucial role in managing IoT- generated data.[17] By performing data processing and analysis locally on the device or gateway, edge computing reduces the amount of data that needs to be sent to the cloud. This approach not only eases network congestion but also enables real-time analytics, which is vital in time-sensitive applications.

Leveraging big data analytics tools and machine learning algorithms is another effective means of extracting valuable insights from IoT data. These tools can identify patterns, trends, and anomalies in the data, allowing businesses to optimize operations, predict maintenance needs, and enhance overall efficiency.

SOLUTION: Edge computing: Performing data processing and analysis at the edge of the network allows IoT devices to respond quickly to local events, reducing the amount of data sent to the cloud. This approach also enhances real-time analytics capabilities, critical for time-sensitive applications.

Big data analytics and machine learning: Leveraging big data analytics tools and machine learning algorithms enables organizations to derive valuable insights from the massive volumes of IoT-generated data. These insights can drive decision-making, predict trends, and optimize operations. [17,19,22]

Real-World Example: Environmental Monitoring
In environmental monitoring applications, IoT devices collect data on air quality, water levels, and weather conditions. Edge computing is employed to perform initial data processing locally, filtering out non-critical data, and sending only relevant information to central data repositories for further analysis. This reduces the volume of data transmitted and optimizes data management.

6. Regulatory and Ethical Challenges: As IoT adoption outpaces the development of adequate regulations, there are concerns about data governance, user privacy, and ethical data practices.

To address these challenges, governments and regulatory bodies must collaborate with industry stakeholders to establish clear guidelines and standards for IoT security, privacy, and data handling. Compliance with these regulations ensures that IoT companies prioritize user safety and data protection. In addition to regulatory efforts, companies should adopt ethical data practices and be transparent with users about how their data is being collected, used, and shared. Implementing ethical data policies builds trust with consumers and fosters a positive perception of IoT technologies. [13,17]

DOI: 10.17148/IARJSET.2023.107126

SOLUTIONS: Collaborative regulatory efforts: Governments, regulatory bodies, and industry stakeholders should collaborate to develop and enforce clear guidelines and standards for IoT security, data privacy, and ethical data practices. Regular audits and compliance checks can ensure adherence to these standards.

Ethical data practices and transparency: Companies must adopt ethical data collection, storage, and usage practices. They should provide transparent privacy policies, informing users about the data collected, how it will be used, and with whom it will be shared. [17,19,22]

Real-World Example: European Union's General Data Protection Regulation (GDPR)
In response to concerns about data privacy and protection, the European Union implemented GDPR to regulate the collection and processing of personal data, including data collected by IoT devices. Companies operating within the EU must adhere to GDPR's guidelines, ensuring greater transparency and respect for users' privacy rights.

7. Reliability and Quality Assurance: In critical applications such as healthcare, transportation, and industrial settings, IoT device failures can have severe consequences. Ensuring the reliability and performance of IoT devices is of paramount importance.

Rigorous testing and quality assurance processes should be followed during the development and manufacturing of IoT devices. [7] Thorough testing helps identify and rectify issues before deployment, reducing the likelihood of malfunctions or vulnerabilities.

Moreover, continuous monitoring and predictive maintenance can improve the reliability of IoT devices. By collecting real-time data on device performance and health, organizations can detect potential problems early on and implement preventive measures, minimizing downtime and costly failures.

Solutions: Rigorous testing: Conducting comprehensive testing throughout the development lifecycle helps identify and resolve issues early on. Testing should encompass functionality, performance, security, and stress testing to ensure the reliability of IoT devices.

Continuous monitoring and predictive maintenance: Implementing continuous monitoring systems allows organizations to track the health and performance of IoT devices in real-time. Predictive maintenance leverages data analytics to predict device failures and schedule maintenance proactively, reducing downtime and enhancing reliability. [17,19,22]

Real-World Example: Predictive Maintenance in Transportation
Transportation companies, such as airlines and railway operators, use IoT sensors to monitor the condition of their assets (e.g., aircraft engines or train components). Predictive maintenance algorithms analyze the sensor data to predict potential failures, allowing companies to schedule maintenance proactively, reduce downtime, and enhance reliability.

8. Cost Constraints: Cost is a significant factor influencing the widespread adoption of IoT solutions. Especially in certain industries or regions, budget limitations can hinder IoT deployment.

Standardization is a key strategy to reduce the production cost of IoT devices. When the industry adopts common standards for hardware components and communication protocols, manufacturers can achieve economies of scale, leading to cost reductions.

SOLUTIONS: Standardization and economies of scale: Promoting standardization in IoT hardware components and communication protocols allows manufacturers to produce devices more efficiently and cost-effectively. Widespread adoption of common standards also creates economies of scale, further reducing production costs.

Financial incentives and subsidies: Governments, industry associations, or organizations can offer financial incentives or subsidies to businesses and consumers to offset the initial costs of adopting IoT technologies. This approach encourages wider adoption, especially in industries where the benefits of IoT are significant. [17,19,22]

Real-World Example: Smart Agriculture
In the agricultural sector, farmers face cost constraints when implementing IoT solutions. However, government initiatives in various countries offer subsidies or financial incentives to encourage farmers to adopt IoT technologies for precision farming, water management, and livestock monitoring. These incentives help offset the initial investment and promote the adoption of IoT in agriculture

DOI: 10.17148/IARJSET.2023.107126

VII. CONCLUSION

The paper primarily focuses on the security aspects of IoT technology, emphasizing the different types of attacks that IoT systems may encounter, such as DOS, password guessing, replay, and insider attacks. Authentication is identified as the first line of defence for securing IoT systems, and the paper delves into various authentication approaches used in IoT, including one-time passwords, ECC-based mutual authentication, ID-based authentication, certificate-based authentication, and blockchain-based solutions. The researchers compare recent authentication protocols and note that many of them rely on encryption cryptography to ensure security.

In their future work, the plan to enhance the security of IoT environments by proposing secure and efficient IoT authentication schemes. This highlights their dedication to advancing the protection of user data and preventing potential security breaches in IoT systems. By continually exploring and developing new authentication methods, the researchers aim to bolster the overall security of IoT technology, providing safer and more reliable IoT ecosystems for users and industries alike.

REFERENCES

[1] Security Issues in the Internet of Things (IoT): A Comprehensive Study (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017
[2] Review Article Internet of Things Security: Challenges and Key Issues IEEE.
[3] Security in Internet of Things: Issues, Challenges and Solutions Hanan Aldowah1(&), Shafiq Ul Rehman2, and Irfan Umar1
[4] M. Abomhara and G. M. Køien, “Security and privacy in the internet of things: Current status and open issues,” in Privacy and Security in Mobile Systems (PRISMS), International Conference on. IEEE, 2014, Pp. 1–8.
[5] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, “A vision of iot: Applications, challenges, and opportunities with China perspective,” IEEE Internet of Things journal, vol. 1, no. 4, pp. 349–359, 2014.
[6] M. M. Hossain, M. Fotouhi, and R. Hasan, “Towards an analysis of Security issues, challenges, and open problems in the internet of things,” In Services (SERVICES), 2015 IEEE World Congress on. IEEE, 2015, Pp. 21–28.
[7] L. Da Xu, W. He, and S. Li, “Internet of things in industries: A survey,” IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233–2243, 2014.
[8] Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: A survey on enabling technologies, protocols, and applications, IEEE Communications Surveys Tutorials 17 (4) (2015)
[9] Aditya, M. Sharma, S. C. Gupta, an internet of things based smart surveillance and monitoring system using arduino, in: 2018 International Conference on Advances in Computing and Communication Engineering (ICACCE), 2018, pp. 428–433. doi:10.1109/ICACCE.2018.8441725
[10] G. Chu, N. Apthorpe, N. Feamster, Security and privacy analyses of internet of things childrens toys, IEEE Internet of Things Journal (2018) 1–1doi:10.1109/JIOT.2018.2866423.
[11] S. Prabhakar, “Network security in digitalization: attacks and defence,” International Journal of Research in Computer Applications and Robotics, vol. 5, no. 5, pp. 46–52, 2017.
[12] Y. Javed, A. S. Khan, A. Qahar, and J. Abdullah, “Preventing DoS attacks in IoT using AES,” Journal of Telecommunication, Electronic and Computer Engineering, vol. 9, no. 3–11, pp. 3–11, 2017.
[13] H. C. A. van Tilborg and S. Jajodia, Encyclopedia of Cryptography and Security, Springer US, Boston, MA, 2011.
[14] M. Conti, N. Dragoni, and V. Lesyk, “A survey of man in the middle attacks,” IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2027–2051, 2016.
[15] H. C. Hasan, F. N. Yusof, and M. Daud, “Comparison of authentication methods in internet of things technology,” International Journal of Computer and Systems Engineering, vol. 12, no. 3, pp. 231–234, 2018.
[16] M. Azrour, Y. Farhaoui, and M. Ouanan, “Cryptanalysis of farash et al.’s SIP authentication protocol,” International Journal of Dynamical Systems and Differential Equations, vol. 8, no. 1/2, 2018.
[17] S. Panchiwala and M. Shah, “A comprehensive study on critical security issues and challenges of the IoT world,” Journal of Digital Information Management, vol. 2, no. 4, pp. 257–278, 2020.
[18] R. Z. Naeem, S. Bashir, M. F. Amjad, H. Abbas, and H. Afzal, “Fog computing in internet of things: practical applications and future directions,” Peer-to-Peer Networking and Applications, vol. 12, no. 5, pp. 1236–1262, 2019.
[19] Mahmoud, T. Yousuf, F. Aloul, I. Zualkernan, Internet of things (iot) security: Current status, challenges and prospective measures, in: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), 2015, pp. 336–341. doi:10.1109/ICITST.2015.7412116.
[20] E. Leloglu, A review of security concerns in internet of things, Journal of Computer and Communications 5 (1) (2017) 121–136. doi:10.4236/jcc.2017.51010.
[21] Ad Hoc Networks 32 (2015) 17 – 31, internet of Things security and privacy: design methods and optimization.
[22] M. Azrour J. mabrouk A. Guezzaz Internet of things challenges and solutions, key issues 2021.