*Nanotechnology Perceptions*
*ISSN 1660-6795*
*www.nano-ntp.com*

# Privacy And Security Issues In Iot Systems

**Himanshu Bhamare[1] , Dr.Amarsinh Vidhate[2], Dr. Puja Padiya[3]**

*[1]Postgraduate Student, Department of Computer Engineering, Ramrao Adik Institute Of Technology, D. Y. Patil Deemed to be University,*
*Nerul, Navi Mumbai, 400706.*
*[2]Professor, Department of Computer Engineering, Ramrao Adik Institute Of Technology, D. Y. Patil*
*Deemed to be University,*
*Nerul, Navi Mumbai, 400706.*
*[3]Assistant Professor, Department of Computer Engineering, Ramrao Adik Institute Of Technology, D. Y. Patil*
*Deemed to be University,*
*Nerul, Navi Mumbai, 400706.*
*Email: [1]himanshubhamre417@gmail.com, [2]amar.vidhate@rait.ac.in, [3]puja.padiya05@gmail.com*
*Corresponding Author* : Himanshu Bhamare*

The Internet of Things (IoT) is revolutionizing industries and everyday life by connecting a wide range of devices through the Internet. While IoT enhances convenience and efficiency, it simultaneously presents significant challenges regarding privacy and security. This paper explores IoT systems' primary privacy and security concerns, including data collection, unauthorized access, and cyber threats. It delves into existing solutions such as blockchain, fog computing, and machine learning, which aim to mitigate these challenges. Furthermore, a comparative analysis of different IoT security strategies is presented, emphasizing the need for robust encryption, authentication, and privacy-by-design principles. Ultimately, the paper calls for a collaborative effort among researchers, policymakers, and industry players to secure IoT systems and protect user data effectively.

**Keywords:** IoT components, IoT Security issues, Security protocols, Machine Learning, Blockchain Technology**.**

## 1. INTRODUCTION:

The Internet of Things (IoT) represents a paradigm shift in how technology interacts with the physical world, linking everyday objects to the Internet to create a highly interconnected digital ecosystem. From smart home devices and wearable technology to industrial sensors and smart cities, IoT has enabled remarkable advancements, enhancing convenience, efficiency, and automation. However, with the growing adoption of IoT systems, significant concerns arise regarding data privacy and security. IoT devices, by design, collect and transmit vast amounts of sensitive data, making them potential targets for cyberattacks and raising ethical questions about data ownership and consent.

The global integration of IoT devices has led to a rapid escalation in data collection, which often includes personal, location, and behavioral information. This creates a complex web of privacy concerns, as IoT systems frequently collect data without explicit consent from users, and in many cases, it is unclear how this data is processed, stored, or shared. Moreover, cybersecurity risks in IoT systems are prevalent, with vulnerabilities ranging from device-level hacking and malicious code attacks to network intrusions and denial-of-service (DoS) attacks. These risks not only threaten individual privacy but also compromise critical infrastructures, making the security of IoT systems a priority for policymakers, technologists, and organizations.

This paper aims to explore the multifaceted landscape of privacy and security challenges in IoT systems, focusing on the following key objectives:

1. To analyze the privacy risks associated with the vast scale of data collection in IoT systems and their implications for individuals and society.
2. To examine the security vulnerabilities within IoT devices and networks, with an emphasis on authentication, access control, encryption, and data integrity.
3. To evaluate existing frameworks and technologies designed to mitigate IoT security risks, such as blockchain, fog computing, and machine learning.
4. To provide a comparative analysis of current solutions and discuss future directions for enhancing IoT security and privacy.

## 2. LITERATURE SURVEY:

### 2.1 Overview of IoT: Shaping the Connected World

The Internet of Things (IoT) has fundamentally transformed the way individuals, businesses, and industries interact with technology. IoT refers to the network of interconnected physical devices embedded with sensors, software, and other technologies that enable them to collect and exchange data. These devices range from simple household gadgets to complex industrial systems, and they play a critical role in automating processes, increasing efficiency, and providing real-time data for decision-making.

One of the key advantages of IoT is its ability to seamlessly integrate with various aspects of daily life. Smart homes, wearable technology, healthcare monitoring devices, and industrial IoT applications such as predictive maintenance are only a few examples of how IoT is reshaping the digital landscape. However, this increased connectivity also introduces significant privacy and security risks that require urgent attention.

### 2.2 Defining IoT and Its Components

At its core, IoT involves the connection of previously unconnected devices, allowing them to sense, communicate, and act autonomously or semi-autonomously. The basic structure of an IoT system includes several layers:

- Physical Layer: Comprising the physical devices embedded with sensors and actuators, this layer is responsible for collecting data from the environment. It is considered one of the most vulnerable layers due to the lack of standardized security protocols.
- Network Layer: This layer facilitates data transmission between IoT devices and systems. Communication occurs over various protocols, such as Internet Protocol (IP), and security vulnerabilities at this layer can lead to issues like data interception and eavesdropping.
- Processing Layer: Also referred to as the middleware layer, this component handles the initial processing and analysis of data, ensuring its efficient transfer to the upper layers. Security measures are critical here, as the layer is prone to data injection attacks and malware.
- Application Layer: The highest layer in the IoT architecture, this level supports end-user applications, including smart homes, health monitoring systems, and industrial automation. Security challenges at this layer stem from the openness of applications and the integration of multiple third-party services.

Each of these layers presents its own set of security challenges, which must be addressed to maintain the integrity of the IoT system as a whole.

### 2.3 Growth and Significance of IoT

The exponential growth of IoT in various sectors such as healthcare, transportation, agriculture, and smart cities has made it a critical component of modern digital infrastructure. The global IoT market is expected to continue expanding rapidly, with billions of devices anticipated to be connected in the coming years. This proliferation of devices increases the attack surface for malicious actors and exacerbates concerns regarding data privacy and security.

The significance of IoT lies not only in its ability to enhance convenience and efficiency but also in its potential to revolutionize industries by providing real-time analytics, predictive maintenance, and automation. Despite its advantages, the growth of IoT comes with substantial security challenges, as the heterogeneous nature of IoT devices makes it difficult to implement uniform security measures across the entire ecosystem.

### 2.4 IoT Security Concerns: A Critical Review

As IoT systems continue to expand, so do the security vulnerabilities that accompany them. IoT devices are often deployed with minimal security configurations, making them easy targets for cyberattacks. Several key security concerns have been identified across the different layers of IoT architecture:

- Physical Layer Attacks: These include malicious code incursions, node compromises, and false data injection attacks, all of which exploit the physical accessibility of IoT devices. Attackers may also engage in side-channel attacks and eavesdropping.
- Network Layer Attacks: The network layer is prone to attacks such as routing manipulation, data transit interceptions, and denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks. Such threats can disrupt communication between devices, leading to service outages or the compromise of sensitive data.
- Application Layer Threats: At the application layer, access control violations, data breaches, and malicious code injections are common. The lack of encryption in many IoT systems further exacerbates the risk of data theft.

### 2.5 Privacy Concerns in IoT

Data privacy remains one of the most pressing concerns in IoT. Given that IoT devices collect vast amounts of personal data, including location, behavioural patterns, and sensitive health information, the risk of data misuse and unauthorized access is high. Issues such as user profiling, context-aware privacy violations, and data de-identification are critical privacy challenges that IoT users face.

The absence of standardized privacy frameworks in the IoT ecosystem creates additional risks. Without comprehensive guidelines on how data should be stored, shared, or processed, IoT devices often lack the necessary safeguards to prevent unauthorized data access. This opens the door to user tracking, information mining, and potential breaches of confidential data.

### 2.6 Existing Solutions for IoT Security

Over the years, various security solutions have been proposed to address the growing concerns in the IoT landscape. Some of the most promising approaches include:

- Blockchain Technology: Blockchain provides a decentralized, tamper-proof ledger that enhances the integrity and security of data shared between IoT devices. Its cryptographic techniques make it resistant to data manipulation and unauthorized access.
- Fog Computing: By processing data closer to the source (i.e., at the network edge), fog computing reduces latency and enhances security by limiting the amount of sensitive data transmitted over long distances.
- Machine Learning (ML): ML algorithms have shown promise in detecting anomalous behavior in IoT systems, allowing for the early identification of potential security breaches. ML is also being used to create adaptive security systems that can evolve in response to emerging threats.

### 2.7 Gaps Identified in IoT Security and Privacy

Despite advancements in IoT security, several gaps still exist that hinder the full protection of IoT systems:

1. Lack of Standardization: The absence of uniform security standards across IoT devices and networks creates inconsistencies and vulnerabilities.
2. Inadequate Encryption: Many IoT systems still do not implement end-to-end encryption, leaving data exposed to interception.
3. Device and Network Vulnerabilities: The diversity of IoT devices makes it difficult to enforce strong authentication and access control protocols across the board.

These gaps highlight the urgent need for further research and innovation to address IoT security and privacy challenges comprehensively.

## 3. METHODOLOGY:

This section outlines the approach used to analyze the privacy and security challenges in Internet of Things (IoT) systems and examines existing solutions designed to mitigate these risks. Given the vast and evolving nature of IoT technologies, this paper adopts a comparative analysis framework to evaluate different security strategies, focusing on their effectiveness, scalability, and practicality in real-world applications.

### 3.1 Data Collection and Analysis

The analysis draws on existing literature and case studies that detail the security vulnerabilities present in IoT systems, with particular emphasis on:

- Peer-reviewed research papers discussing IoT architectures, privacy issues, and security measures.
- Industry reports and white papers from technology companies providing insights into IoT deployments and security strategies.
- Regulatory frameworks and guidelines on IoT privacy and security from global organizations such as the International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), and the General Data Protection Regulation (GDPR).

The key sources of information for this research include academic papers that explore various aspects of IoT security, industry best practices for mitigating cyber threats, and technical papers that propose novel solutions such as blockchain integration, machine learning-based detection systems, and fog computing architectures.

### 3.2 Comparative Framework

To systematically evaluate the effectiveness of different security solutions, a comparative analysis framework was employed. The framework assesses each solution based on the following criteria:

- Scalability: Can the solution be implemented across a wide variety of IoT devices and networks, from small consumer applications to large industrial systems?
- Cost-effectiveness: What are the costs associated with implementing and maintaining the solution, and how does this affect its adoption?

- Security Impact: How effectively does the solution mitigate security vulnerabilities such as data breaches, malicious code injections, denial-of-service (DoS) attacks, and privacy violations?
- Resource Constraints: Does the solution take into account the limited processing power and memory of many IoT devices, particularly those in edge computing environments?
- Ease of Integration: How easily can the solution be integrated into existing IoT ecosystems without significant modifications or disruptions?

By applying this comparative framework, the paper evaluates the following key technologies:

1. Blockchain Technology: Blockchain's ability to provide decentralized security and tamper-proof data records was analyzed based on its integration with IoT systems for enhanced data integrity and authentication.
2. Fog Computing: The distributed processing capabilities of fog computing were assessed, especially in terms of its ability to reduce data transit risks by keeping data processing closer to the network edge. Its potential for low-latency response to security threats was also considered.
3. Machine Learning (ML): The use of machine learning algorithms for detecting anomalous behavior in IoT networks was reviewed, particularly focusing on their adaptability to emerging cyber threats and their role in creating dynamic access control systems.

### 3.3 Case Studies and Comparative Analysis

To validate the comparative analysis, case studies of real-world IoT implementations were reviewed. These case studies provided insights into:

- How blockchain has been used in supply chain management to enhance security and transparency**.**
- Fog computing's role in smart cities to manage data traffic efficiently while ensuring privacy protection**.**
- Machine learning applications in healthcare and industrial IoT systems, where predictive analysis helps identify potential security breaches before they occur.

These case studies were selected to represent a diverse range of industries and applications, showcasing the versatility and challenges of each security solution.

## 4. RESULTS:

This section presents the findings of the comparative analysis, focusing on the effectiveness, scalability, and challenges of various security solutions in addressing the privacy and security concerns associated with IoT systems. The analysis draws on case studies and data gathered from existing literature to evaluate each solution's capacity to mitigate the risks that IoT ecosystems face.

### 4.1 Blockchain Technology in IoT Security

Blockchain technology has demonstrated significant potential in enhancing the security of IoT systems by providing a decentralized architecture that reduces reliance on central authorities. The key findings include:

- Data Integrity and Tamper Resistance: Blockchain ensures the integrity of data transmitted between IoT devices by storing data in immutable blocks. This provides tamper-proof records, making it nearly impossible for malicious actors to alter or delete data without detection.
- Decentralized Trust: By removing the need for a centralized trust authority, blockchain reduces vulnerabilities associated with single points of failure, which are common in traditional IoT systems. This is particularly useful in applications like smart contracts for supply chains, where real-time data sharing between stakeholders must be secure.
- Challenges in Scalability: Despite its security advantages, blockchain faces scalability issues in IoT environments due to the processing power and storage requirements involved in validating and maintaining blockchain ledgers. Many IoT devices, especially those with limited computational resources, struggle to support the full blockchain framework.
- Energy Consumption: The high energy consumption associated with blockchain's consensus mechanisms (e.g., Proof of Work) poses challenges for IoT devices operating on limited power**,** making it impractical for certain IoT applications, particularly in low-power environments like wearable technology.

### 4.2 Fog Computing for Distributed IoT Security

Fog computing, which brings processing power closer to the network edge, has proven to be an effective solution for improving latency and security in IoT systems:

- Proximity-Based Security: By processing data at the edge of the network, fog computing reduces the need for sensitive data to travel long distances to centralized cloud servers. This proximity enhances data protection by minimizing the risk of interception during transmission.
- Real-Time Threat Detection: Fog computing enables real-time analysis of security threats. Localized processing allows for faster detection and mitigation of potential attacks, such as distributed denial-of-service (DDoS) attacks, which can cripple IoT networks.
- Scalability and Flexibility: Fog computing's scalable architecture can be tailored to specific IoT applications, making it suitable for both large-scale industrial IoT systems and smaller consumer IoT devices. Its ability to manage heterogeneous device environments adds to its versatility in ensuring secure data exchanges.
- Resource Constraints: While fog computing reduces latency and improves security, its reliance on edge devices with limited processing power poses a challenge. Ensuring real-time threat detection and data encryption at the edge may strain devices that lack adequate computational resources.

### 4.3 Machine Learning for Anomaly Detection and Adaptive Security

Machine learning (ML) has emerged as a powerful tool for enhancing IoT security, particularly in the areas of anomaly detection**,** predictive threat analysis, and dynamic access control:

- Anomaly Detection: ML models excel at identifying anomalous behavior within IoT networks by analyzing patterns of data flow and device activity. This allows for the early detection of cyberattacks, such as unauthorized access attempts or malware infections, before they cause significant damage.
- Adaptive Security: One of the major advantages of ML in IoT security is its ability to adapt to new threats over time. As IoT systems evolve, machine learning algorithms can learn from past security incidents and adjust security protocols accordingly, making them more resilient to emerging threats.
- False Positive Reduction: ML-based systems have been shown to reduce the number of false positive alerts, which are a common issue in traditional security systems. This allows security teams to focus on genuine threats, enhancing the overall efficiency of IoT security measures.
- Computational Overhead: Implementing ML models in resource-constrained IoT environments remains a challenge. ML algorithms often require significant computational power and data processing capabilities, which many IoT devices lack. This limits the widespread deployment of ML-based security solutions in smaller, lower-power IoT devices.

### 4.4 Comparative Analysis:

The table below summarizes the findings of the comparative analysis, illustrating the strengths, limitations, and potential applications of each solution:

**Table 1. Solutions**

| Security Solutions | Strengths | Limitations | Potential Applications |
|---|---|---|---|
| Block Chain Technology | • Data integrity, tamper-proof records<br>• Decentralized trust | • Scalability issues<br>• High energy consumption | • Supply chain management<br>• Smart contracts |
| Fog Computing | • Proximity-based security<br>• Real-time threat detection | • Resource constraints at the edge | • Smart cities<br>• Industrial IoT |

| | | | |
|---|---|---|---|
| Machine Learning | • Anomaly detection<br>• Adaptive to new threats | • High computational requirements | • Healthcare IoT<br>• Autonomous systems |

**Table 2. Comparative Analysis of Discussed Solutions**

| Reference | Findings | Security solutions proposed | Limitations |
|---|---|---|---|
| Kumar & Vidhate, 2023 | Discusses the issue of IoT security and exposure, focusing on data leak and risk at different levels. | Suggests the usage of the blockchain concept for handling large amounts of data in the IoT network and ensuring the data integrity of its components. | High processing costs in blockchain make it challenging to implement the BSM for large IoT networks. |
| Alaskri et al., 2023 | Summarizes major IoT security threats including viruses, breach of security and availability, and DoS.<br>. | Encryption protocols are the first primary solution and will be aiding multi-factor authentication in this case. | Pays most attention to theoretical threats; provides very little evidence regarding the efficiency of implemented measures |
| Veluvarthi et al., 2023 | Discusses more on Various Types of IoT Security Threats at the Physical, Network, and Application Layer while emphasizing on secure protocols.<br>. | Fog computing and Machine Learning based anomaly detection is recommended to improve security. | Scanty references to how such integration might be accomplished in resource-scarce IoT devices |
| Sadhu et al., 2022 | Specifically; it is involved in the identification of risks associated with IoT data primarily at transit and storage levels. | Encourages the use of cloud based encryption and secure access control. | The use of cloud tends to develop latency as well as dependency by edge IoT units. |
| Singh et al., 2023 | Evaluates IoT security using various | Uses blockchain for secure data sharing | High computational demands, which can |

| | | | |
|---|---|---|---|
| | techniques, including blockchain and machine learning for enhanced detection and resilience. | and ML for predictive analysis. | be costly for small-scale IoT systems. |
| Kaur & Raina, 2023 | Discusses IoT threats in smart cities with emphasis on privacy. | Includes ideas on privacy by design frameworks and encryption mechanisms on data security. | Few implementation stories; not a large number of actual case studies but very abstract concepts without proving their efficiency in front line. |
| Kumar et al., 2023 | Discusses IIoT risks and threats with an emphasis on the manufacturing business environment. | Introduces the technique of AI in intrusion detection and the concept of multi-layered encryption. | High resource demands working against feasibility in tight environments of manufacturing industries. |
| Singh et al., 2022 | Evaluates the security threats and issues of IoT before suggesting the adoption of adaptive authentication method. | Raises the need to adopt two-factor authentication as well as managing session. | Largely restricted by feature coverage, with most attention paid to application layer flaws. |
| Gautam et al., 2023 | Pursues the subject of security and privacy in the IoT paying extra attention to network threat tactics, such as a DoS attack. | Supports the use of multiple-protocol security tools and artificial neural networks for threats' identification. | In its current manifestation, it somewhat lacks scalability testing across different IoT platforms and industries. |
| Khader & Eleyan, 2021 | Discusses Surveys DoS/DDoS attacks in IoT and point to considerable network weaknesses. | Proposes intrusion detection systems (IDS) and specifies that network should be divided in segments. | Offers only generic approaches to the problems and does not comment on the issues of scalability and real-time applicability. |
| Chanal & Kakkasageri, 2020 | Discusses the issues characteristic of the application and the | The writer of this article recommends encryption and user | The underlying minimalist practical use as a tool of |

| | | | |
|---|---|---|---|
| | transport layer of IoT security emphasis on privacy. | authentication for protection of the individuals' precious data. | practical applied system analysis. |
| Goyal et al., 2021 | Argues the possible privacy issues that could exist in IoT with a focus in profiling of the users and data mining. | Focuses on providing security in the context and application methods for data anonymization. | Restricted by the absence of a uniform approach towards the method that accomplishes the task of data anonymization. |
| Abughazaleh et al., 2020 | Discusses possible DoS attacks on IoT and their effects on the availability of data. | Suggests the use of intrusion detection system(S) in real time and dynamic usage of access rights to combat DoS attacks. | Almost entirely theoretical, possessing relatively little in the way of actual usage particularly as employed in real-world settings. |
| Bangare & Patil, 2022 | Investigates IoT system vulnerabilities, particularly in healthcare and industrial applications. | Proposes multi-layered encryption and role-based access control (RBAC). | Challenges in scalability across diverse IoT devices; limited testing data on solution effectiveness. |

## 5. DISCUSSION:

The findings from this study underscore the complexity of achieving robust privacy and security in Internet of Things (IoT) ecosystems. Although various technologies, such as blockchain, fog computing, and machine learning (ML), show promise in addressing these challenges, each solution has unique strengths and limitations that impact its practicality and scalability across different IoT applications. The insights gained from the comparative analysis highlight the urgent need for multi-layered security strategies and collaborative efforts to secure IoT systems effectively.

### 5.1 Interpreting Security Solution Efficacy

Each security solution analyzed in this paper contributes a distinct set of advantages and challenges to IoT security:

- Blockchain Technology provides a highly secure and decentralized way of safeguarding IoT data. Its immutability and resistance to tampering make it ideal for applications requiring transparent data sharing among multiple parties. However, blockchain's high processing requirements and energy consumption remain significant barriers, especially for IoT devices with limited resources. Integrating blockchain effectively in resource-constrained IoT environments may require the development of lighter consensus mechanisms or hybrid solutions that combine blockchain with other security frameworks.

- Fog Computing addresses latency and bandwidth issues by enabling local data processing close to the source. This approach not only minimizes data transmission risks but also enhances real-time response capabilities, which are critical in applications such as smart cities and industrial automation. Despite these benefits, the computational constraints at the edge pose challenges for implementing robust encryption and threat detection protocols. Further advancements in low-power edge computing may enhance fog computing's security benefits for a broader range of IoT devices.
- Machine Learning has proven highly effective in anomaly detection and dynamic threat adaptation. ML's ability to identify unusual behavior and predict future risks makes it particularly suitable for high-risk IoT environments like healthcare and autonomous systems. However, ML algorithms require substantial computational power and memory, making their deployment challenging on low-resource IoT devices. Future research could focus on optimizing ML algorithms for lightweight deployment or using cloud-based ML models in combination with edge devices to balance computational demands.

### 5.2 Future Directions and Research Needs

The rapidly evolving nature of IoT technologies calls for continuous innovation in security strategies. The following areas are recommended for future research and development:

- Lightweight Security Algorithms: Developing low-power security algorithms that can operate on constrained IoT devices is essential.
- Hybrid Security Models: Combining multiple security solutions, such as blockchain with fog computing or machine learning with encryption protocols, could yield more effective multi-layered security models. Hybrid models can leverage the strengths of each solution while mitigating their limitations, offering a more comprehensive approach to IoT security.
- Standardized Testing and Compliance Frameworks: The lack of consistent testing and compliance standards across IoT devices presents a significant security risk. Future efforts should aim to establish standardized testing protocols that evaluate IoT devices' compliance with security benchmarks, enabling manufacturers to adopt best practices more easily.
- Privacy-Preserving ML Models: With the growing reliance on machine learning for IoT security, there is a need to develop privacy-preserving ML models. Techniques such as federated learning and differential privacy could allow IoT systems to learn from data without compromising user privacy, which is particularly important in sensitive applications like healthcare.

## 6. CONCLUSION:

The growth of the Internet of Things (IOT) remains one of the most dynamic technologies of the present age since it supplements several industries with connection and automation. However, the integration of IoT has also brought new and difficult questions in the field of protecting the privacy and security of the data as IoT systems also manage, process and transfer a large amount of confidential information. To the above, this paper sought to conduct a comprehensive review of privacy and security in the IoT ecosystem, discuss existing solutions and also examine and compare various technological and regulatory measures in IoT.

The comparative analysis also reveals that some emerging techniques such as blockchain, fog computing, and machine learning present opportunities for improving the security of IoT, such opportunities are bounded by issues to do with scalability, computational requirements, and integration challenges. Self-organized systems ensure a decentralized control of data but require substantial storage, computing and energy to potentially unreliable results depending on the IoT system in question. While fog computing is an effective solution to security and latency because of its ability to process data at the network edge, it has an issue of resource management in the same network. Likewise, the machine learning-based anomaly detection improves the threats identification but at the same time consumes a huge amount of computational power thus limited in IoT environments due to available resources.

## 7. ACKNOWLEDGEMENT:

I would like to express my sincere gratitude to my guide and mentor Dr. A V Vidhate on the topic seminar on Privacy and Security Issues in IoT Systems, who helped me understand all aspects of the topic.

## 7. REFERENCES:

[1] S. Kumar and A. Vidhate, “Issues and Future Trends in IoT Security using Blockchain: A Review,” 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2023, pp. 976-984, doi: 10.1109/IDCIoT56793.2023.10053430.

[2] A. Alaskri, N. A. Salem Ahmed and H. Shaari, “Internet of Things (IoT): survey of most important security risks,” 2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), Benghazi, Libya, 2023, pp. 295-299, doi: 10.1109/MI-STA57575.2023.10169291.

[3] R. Veluvarthi, A. Rameswarapu, K. V. Sai Kalyan, J. Piri and B. Acharya, “Security and Privacy Threats of IoT Devices: A Short Review,” 2023 4th International Conference on Signal Processing and Communication (ICSPC), Coimbatore, India, 2023, pp. 32-37, doi: 10.1109/ICSPC57692.2023.10125863.

[4] Sadhu, Pintu Kumar, Venkata P. Yanambaka, and Ahmed Abdelgawad. 2022. “Internet of Things: Security and Solutions Survey” Sensors 22, no. 19: 7433.

[5] J. A. Beltran, P. Mudholkar, M. Mudholkar, V. Tripathi, C. Valderrama Zapata and M. Lourense, “Security Issues and Challenges in Internet of 27 Things (IoT) System,” 2022 5th

International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 57-60, doi: 10.1109/IC3I56241.2022.10072600.

[6] J. Singh, G. Singh and S. Negi, "Evaluating Security Principals and Technologies to Overcome Security Threats in IoT World," 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2023, pp. 1405-1410, doi: 10.1109/ICAAIC56838.2023.10141083.

[7] S. Kaur and S. Raina, "IOT based Security and Privacy issues in Smart Cities," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2023, pp. 188-191, doi: 10.1109/ICACITE57410.2023.10182995.

[8] R. Kumar, B. Kandpal and V. Ahmad, "Industrial IoT (IIOT): Security Threats and Countermeasures," 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA), Uttarakhand, India, 2023, pp. 829-833, doi: 10.1109/ICIDCA56705.2023.10100145.

[9] S. K. A. Yaklaf, A. S. Elmezughi, S. M. H. Naas and N. B. Ekreem, "Privacy, Security, Trust and Applications in Internet of Things," 2023 IEEE International Conference on Advanced Systems and Emergent Technologies (ICASET), Hammamet, Tunisia, 2023, pp. 01-06, doi: 10.1109/ICASET58101.2023.10150619.

[10] E. Akanksha, A. Javali and Jyoti, "A review on Secutity in Internet of Things," 2022 IEEE World Conference on Applied Intelligence and Computing (AIC), Sonbhadra, India, 2022, pp. 883-887, doi: 10.1109/AIC55036.2022.9848853. 28

[11] K. K. S. Gautam, R. Kumar, R. Yadav and P. Sharma, "Investigation of the Internet of Things (IoT) Security and Privacy Issues," 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2023, pp. 1489-1494, doi: 10.1109/ICIRCA57980.2023.10220814.

[12] Poornima M. Chanal, Mahabaleshwar S. Kakkasageri, (2020). "Security and Privacy in IoT: A Survey." Wireless Personal Communications. 115. 10.1007/s11277-020-07649-9.

[13] Goyal Parul, Ashok kumar sahoo, Tarun Kumar Sharma, Pramod K. Singh (2021). "Internet of Things: Applications, security and privacy: A survey." Materials Today: Proceedings. 34. 752-759. 10.1016/j.matpr.2020.04.737.

[14] P. S. Bangare and K. P. Patil, "Security Issues and Challenges in Internet of Things (IOT) System," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 91-94, doi: 10.1109/ICACITE53722.2022.9823709.