# БЕЗБЕДНОСНИТЕ РАНЛИВОСТИ И ПРЕДИЗВИЦИ НА IOT ТЕХНОЛОГИИТЕ THE SECURITY VULNERABILITIES AND CHALLENGES ON THE IOT TECHNOLOGIES

# БЕЗБЕДНОСНИТЕ РАНЛИВОСТИ И ПРЕДИЗВИЦИ НА IOT ТЕХНОЛОГИИТЕ

# THE SECURITY VULNERABILITIES AND CHALLENGES ON THE IOT TECHNOLOGIES

Rexhep Mustafovski[1], Aleksandar Risteski[2], Tomislav Shuminoski[3]
[1, 2, 3]Ss. Cyril and Methodius University, Faculty of Electrical Engineering and Information Technologies,
Rugjer Boshkovikj, Karpos 2 bb, 1000 Skopje, Republic of North Macedonia

[1] rexhepmustafovski@gmail.com [2] acerist@feit.ukim.edu.mk
[3] tomish@feit.ukim.edu.mk

## АПСТРАКТ

Овој труд ја нагласува важноста на IoT технологиите во денешниот свет, истакнувајќи го нивниот трансформативен потенцијал и значајните безбедносни предизвици со кои се соочуваат поради брзиот технолошки напредок. Се разгледуваат целите, пречките и аспирациите поврзани со безбедноста на IoT, како и различните видови напади и контрамерки со цел подобрување на безбедноста и приватноста. Дополнително, студијата ја нагласува клучната улога на IoT во зголемувањето на енергетската ефикасност и поддршката на одржливиот развој преку паметни мрежи, обновливи енергетски системи и иницијативи за паметни градови. Се истражуваат идните насоки и предизвици, со фокус на зајакнување на безбедноста на IoT и поттикнување на нивната употреба во еколошки одржливи апликации. Наодите ја истакнуваат неопходноста од прилагодување на IoT технологиите за безбедна употреба во различни мрежи, обезбедувајќи безбедност на корисниците и сигурност на мрежите.

**Клучни зборови:** *IoT технологии, безбедносни предизвици, енергетска ефикасност, одржлив развој, паметни мрежи, контрамерки.*

## ABSTRACT

This paper emphasizes the importance of IoT technologies in today's world, highlighting their transformative potential and the significant security challenges they encounter due to rapid technological progress. It examines the security objectives, obstacles, and aspirations of IoT, reviewing various attack types and countermeasures aimed at enhancing security and privacy. Furthermore, the study underscores the crucial role of IoT in boosting energy efficiency and fostering sustainable development through smart grids, renewable energy systems, and smart city initiatives. Future directions and challenges are explored, with a focus on strengthening IoT security and encouraging its adoption in environmentally sustainable applications. The findings highlight the necessity of adapting IoT technologies for secure usage across various networks, ensuring both user safety and network reliability.

**Keywords:** *IoT technologies, security challenges, energy efficiency, sustainable development, smart grids, countermeasures.*

## 1 INTRODUCTION

The IoT technologies integrated with other components in the environment can be useful for the users for analysis or further use of them for decision making processes. The use of IoT technologies can give advantages to the users providing them effectiveness and efficiency in everyday life by making them more successful and efficient in the work and professions that they do. As we can overview different literature, is noticed that that the number of IoT technology that will be used in the future will increase alerts that companies will be forced to implement more secure IoT devices and gadgets and provide secure communications and sharing data via more secured channels [1], [2], [3], [5], [6]. This study aims to concern the steps and methods that will be taken by the attackers to minimize the security of the devices and gadgets that can compromise the communications and the information sharing. This paper reviews and defines the different types of attacks and threats that can be faced by the IoT technologies and introduces the steps that can be used to countermeasure and overcome those types of threats successfully. Moreover, there are some suggestions and guidelines for future steps and directions for overcoming the threat challenges [1], [13], [14], [15], [16]. The integration of IoT technologies into different environmental elements presents significant opportunities for improving decision-making processes. These technologies are applicable across various sectors, leading to greater efficiency and effectiveness in both everyday life and professional tasks. However, as the adoption of IoT increases, so do the concerns about security vulnerabilities and associated risks. This paper examines these challenges and suggests countermeasures to tackle them, particularly focusing on their impact on energy efficiency (EE) and sustainable development (SD) [33], [34].

## 2 IOT TECHNOLOGY OVERVIEW

From the first introduction of this kind of technology until now with the development of IoT technology we can see that they are integrated and connected with different types of components which offer different prototypes and systems that can be used for: smart houses, smart cities, smart energy systems, smartphones, tablets, internet connected cars, different wearable devices and gadgets, wireless sensor networks and other useful systems in our everyday lives [17], [18], [19]. The IoT technology devices and gadgets can increase the massive economic and financial opportunities for various applications in the field of military, healthcare, different industries, companies or corporates, educational system, banking system and in many other fields and systems [20], [21], [22]. Since the changed methodology of living, the way of life in the past, the integration of components and devices reduce the operational complexity, make lower costs and increase the market time [1], [2], [3]. Always the IoT devices and gadgets as the part of traditional IoT security technology their main task or duty is concentrating more in operational and maintenance of end-to-end connectivity of devices and IoT environments to interact, login, send or receive data and information [23], [24], [25], [26]. Data or information leaks are the main things that make the community very unreliable to trust in networks, so that's why security of the IoT technology in general is very important [27], [28]. Some of the threats or attacks that the IoT technology can face are: botnet, denial of service (DoS), remote recording, ransomware, social engineering, man in the middle, identity and data theft and advanced persistent threats and etc. The Internet of Things (IoT) is now essential for improving energy efficiency and promoting sustainable development. By linking devices, sensors, and systems, IoT allows for the real-time gathering, analysis, and management of data, which helps optimize resource use and minimize environmental impact. IoT is crucial in contemporary energy systems, supporting smart grids, the integration of renewable energy, and the development of energy-efficient infrastructure [33], [34].

Key contributions of IoT in this context include:

- Energy Monitoring and Optimization: IoT allows for accurate tracking of energy use and effective load balancing, which helps to reduce waste and lower costs.
- Renewable Energy Management: IoT facilitates the integration of renewable energy sources such as solar and wind into the grid by forecasting energy production and consumption.
- Smart Cities and Buildings: IoT technologies enhance urban living by optimizing lighting, heating, and cooling systems to decrease energy consumption.

- Sustainable Development Goals (SDGs): IoT supports global initiatives aimed at achieving SDGs by fostering resource efficiency, lowering carbon emissions, and improving urban sustainability [35], [36], [37].

While the Internet of Things (IoT) has the potential to transform energy and sustainability, its adoption is hindered by challenges like interoperability, scalability, and security issues. Addressing these concerns calls for innovative solutions and strong governance [35], [36], [37].

**Table 1** Applications and Benefits of IoT in Energy Efficiency and Sustainable Development [33], [34], [35], [36], [37]

| Aspect | Description | Examples |
|---|---|---|
| **Energy Monitoring** | IoT sensors track real-time energy consumption to identify inefficiencies and optimize usage. | Smart meters, industrial energy management. |
| **Smart Grids** | IoT enables real-time communication between energy providers and consumers, balancing supply and demand. | Load management, fault detection. |
| **Renewable Integration** | Facilitates seamless incorporation of solar and wind energy into grids through predictive analytics. | IoT-enabled solar panels, wind turbine monitoring. |
| **Energy-Efficient Buildings** | IoT automates HVAC systems, lighting, and appliances to reduce energy wastage. | Smart thermostats, motion-sensitive lighting. |
| **Environmental Monitoring** | Tracks air quality, water usage, and waste management, contributing to sustainability efforts. | IoT-based pollution sensors, water leak detection. |
| **Smart Cities** | IoT systems optimize urban services such as transportation, waste collection, and utilities. | Smart traffic lights, connected streetlights. |
| **Advantages** | Reduces energy waste, integrates renewables, improves urban sustainability, and lowers operational costs. | Reduced carbon emissions, optimized resources. |
| **Challenges** | Security vulnerabilities, interoperability issues, and high implementation costs. | Data breaches, lack of standard protocols. |
| **Future Trends** | AI-driven energy management, blockchain for energy trading, IoT for circular economy practices. | Peer-to-peer energy sharing, predictive maintenance. |

### 2.1 IoT Technology Architecture

The IoT technology architecture is given in Fig. 1 below [2], [3], [4].

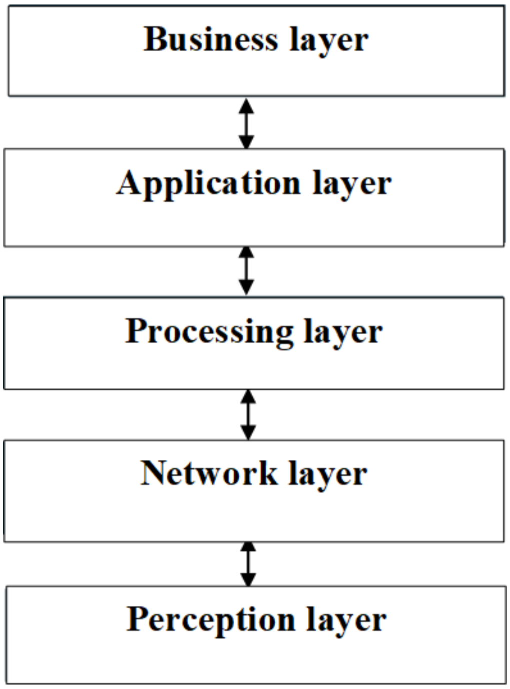

**Figure 1** IoT architecture layers [3]

As we can see from the Fig. 1 the IoT architecture layers consists of 5 layers such as: perception layer, network layer, processing layer, application layer and business layer [1], [2], [3]. The first layer of the architecture is the perception layer which also is known as the physical layer of the architecture, and it consists of sensors or gadgets that collect and sense data or information about the environment [2], [3]. They are used to detect different physical parameters or recognize other smart objects in the environment where then the data or information is sent to further analysis and storage of data or information. The second layer of the architecture is the network layer that serves as a connection or link between the hardware and application layers, allowing the devices or gadgets to communicate with each other. The third layer of the architecture is the processing layer which is also known as middleware layer. It's constructed on top of the network layer and has Application Programming Interface (API) that can be used to easily create and configure applications. This layer also offers different services that can be accessed on. The fourth and the last layer of IoT architecture is the business layer that is the key point of all IoT systems. This layer is integrating and promoting the whole evolution of IoT applications and services. This layer also is used to protect and secure the user privacy, which in the IoT technology is the most crucial part [3], [5], [6], [7], [8], [9], [10]. These components work together to foster advancements in energy systems and sustainability initiatives, including smart grids and energy-efficient buildings [33], [34], [35].

### 2.2 The use of IoT technology in the everyday life

The IoT technology has become crucial component of the people routine and everyday life activities. With the fast evolution of this kind of technology the IoT systems are becoming susceptible to different security, privacy and agreement issues and risks, which can affect everything starting from applications to invisible medium of communication [29], [30], [31]. To secure this kind of technology and systems many security results must be implemented on IoT system domains which should be based on functions and protocols. With the evolution of the IoT systems they give the opportunity to be used and implemented in different fields and areas [31].

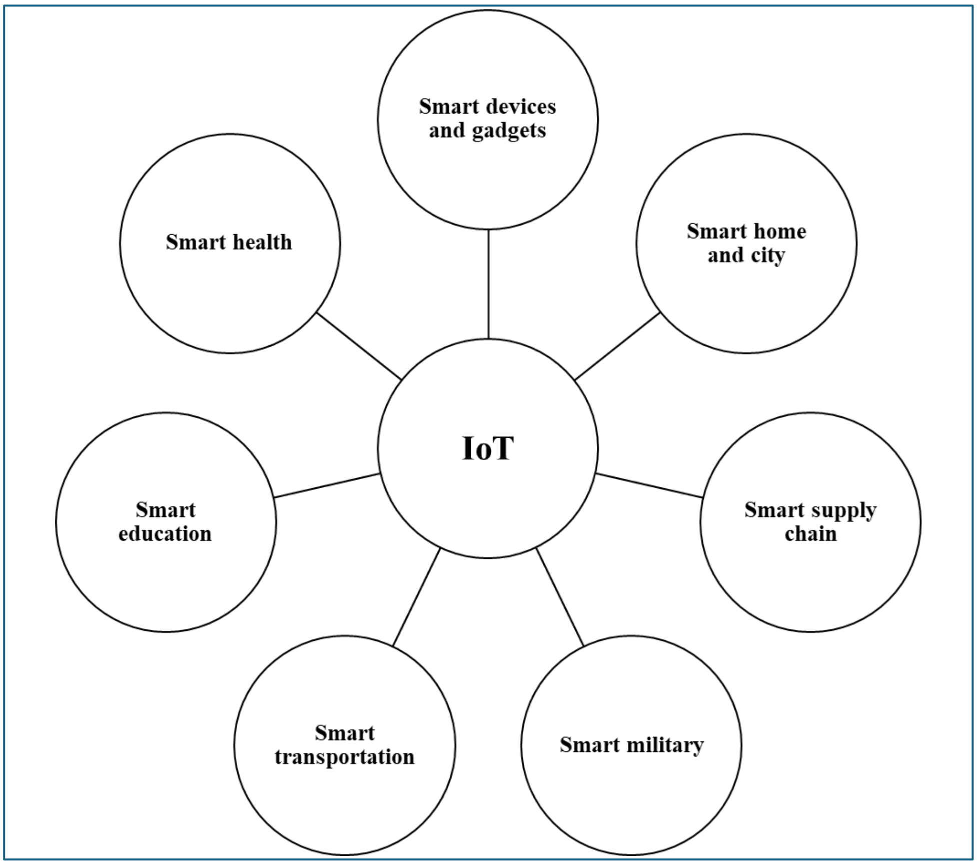

**Figure 2** Fields and areas of application of IoT technology [2], [3]

### 2.3. IoT Applications in Energy Efficiency and Sustainable Development

The Internet of Things (IoT) plays a crucial role in the worldwide effort to enhance energy efficiency and promote sustainable development. By utilizing interconnected devices, IoT solutions help optimize energy consumption, encourage the use of renewable energy sources, and enable more intelligent resource management [35], [36], [37]. Here are some specific applications in energy efficiency and sustainable development:

- **IoT in Energy Efficiency:**
  1. Smart Grids: IoT-enabled smart grids are transforming energy distribution by enabling real-time communication between energy providers and consumers. Sensors integrated into the grid track energy usage, forecast demand spikes, and identify faults, which helps maintain stable and efficient energy delivery. For example, smart grids can automatically redirect energy during outages or periods of high demand, reducing downtime and minimizing energy waste. Example: In Europe, IoT-based grids have played a crucial role in incorporating renewable energy sources such as solar and wind, effectively balancing energy supply and demand [33], [34].
  2. Energy-Efficient Buildings: The use of IoT sensors and automation systems is crucial for enhancing the energy efficiency of buildings. Smart HVAC systems can modify heating, cooling, and ventilation based on how many people are present, while IoT-enabled lighting systems adjust energy consumption by reacting to natural light levels

or room occupancy. These technologies help minimize energy waste and decrease operational costs, leading to more sustainable infrastructure. Example: In office buildings, smart thermostats and motion-sensitive lighting have achieved energy savings of up to 30% [35], [36].

3. Renewable Energy Management: IoT technology facilitates the effective monitoring and management of renewable energy systems. Solar panels and wind turbines outfitted with IoT sensors deliver real-time performance insights, forecast energy production, and pinpoint maintenance requirements. By examining weather trends and energy needs, IoT optimizes the incorporation of renewable sources into the energy grid. Example: In Denmark, IoT-driven systems oversee wind energy generation, promoting grid stability and lessening dependence on fossil fuels [37].
4. IoT devices gather and analyze data on energy consumption, offering valuable insights to help optimize usage patterns. With advanced analytics, demand response strategies can be implemented, allowing consumers to modify their energy usage during peak periods in return for incentives. This approach not only alleviates pressure on the grid but also promotes energy-efficient practices. For instance, IoT-enabled demand response programs in the U.S. have successfully lowered peak energy demand by as much as 10% [33], [34].

- **IoT in Sustainable Development:**
    1. Smart Cities: IoT solutions are essential for developing smart cities, where technology enhances urban services and encourages sustainable living. From smart traffic management systems that alleviate congestion to connected waste collection systems that optimize resource usage, IoT improves the quality of life while lessening environmental impact. Example: Barcelona's IoT-enabled streetlights and waste management systems have significantly cut down on energy and resource consumption [35], [36].
    2. Precision Agriculture: IoT fosters sustainable farming practices through precision agriculture. Sensors track soil moisture, weather conditions, and crop health, enabling farmers to use water and fertilizers more effectively. This not only increases crop yields but also reduces the environmental damage caused by overusing resources. Example: IoT-driven irrigation systems in India have decreased water usage by 20-30% while enhancing crop productivity [37].
    3. Environmental Monitoring: IoT systems are vital for monitoring environmental factors like air quality, water levels, and carbon emissions. These systems deliver real-time data to policymakers and organizations, allowing them to take proactive steps to tackle environmental issues. Example: IoT air quality sensors installed in major cities such as London have guided policies aimed at lowering pollution levels [36], [37].
    4. Resource Optimization and Circular Economy: The Internet of Things (IoT) plays a crucial role in optimizing resources by monitoring and managing the lifecycle of materials. Within a circular economy model, IoT systems keep track of product usage, facilitate efficient recycling processes, and help minimize waste production. Example: In Japan, IoT-enabled waste tracking systems have significantly boosted recycling rates and decreased reliance on landfills [33], [34].

- **Impact of IoT on Global Sustainability Goals**

The Internet of Things (IoT) plays a crucial role in supporting the United Nations' Sustainable Development Goals (SDGs) by focusing on essential areas like affordable energy (SDG 7), sustainable cities and communities (SDG 11), and climate action (SDG 13). By incorporating IoT into energy management, urban planning, and environmental monitoring, countries can make meaningful progress toward these objectives:

1. Affordable and Clean Energy (SDG 7): IoT-enabled energy systems help lower costs and enhance access to dependable energy sources [33], [34].
2. Sustainable Cities and Communities (SDG 11): IoT innovations transform cities into smarter, more livable spaces by streamlining transportation, utilities, and waste management [35], [36].
3. Climate Action (SDG 13): IoT technologies facilitate real-time tracking and reduction of carbon emissions, aiding in the pursuit of global climate targets [37].

## 3 SECURITY GOALS

IoT technology is a relatively new concept of technology where is a need to define different security goals and aims. To achieve these goals, we must successfully implement an integration of these technologies with the networks infrastructures which will increase the security of the users in the use of IoT technology [16], [17], [20], [21]. Therefore, there is a possibility of additional security risk or threat that arises from the coexistence and integration of these technologies and from the open-source codes, open standards and protocols, which are mainly created for the IoT devices and platforms [23], [27], [29]. The aim of IoT technology is to protect and successfully secure the collected data and information, since the collected data and information from the physical devices or gadgets can gather sensitive user information [1], [2], [3], [11], [12], [13]. This paper refers to protection and security of the data and information collected or stored in IoT system, which will increase the security of the networks and the clouds. This implies that IoT systems need to ensure the confidentiality, integrity, and availability of data and information. This can be achieved through authentication, access control, data and information encryption, data availability and redundancy through back-ups [1].

## 4 LITERATURE REVIEW

Furthermore, the comparative table based on the IoT technology devices and gadgets and their used and implementations from scientific papers [2] and [3] are given:

**Table 2** Comparison of IoT devices based on their applications, benefits, and challenges, providing a structured overview of the key technologies discussed in the papers [2] and [3]

| IoT Technology Devices and Gadgets | Application | Benefits | Challenges | Source |
|---|---|---|---|---|
| Smart Home Devices | Home automation | Enhances security, convenience, and energy efficiency | Vulnerable to hacking, privacy issues | Mihai et al. (2023) [2] |
| Healthcare IoT (Wearable Devices) | Remote health monitoring | Enables real-time health tracking and diagnostics | Privacy concerns, data security risks | Felcia Bel & Sabeen (2022) [3] |
| Industrial IoT Devices (IoT) | Industrial automation, smart manufacturing | Improves productivity, real-time monitoring | Network and power constraints, security threats | Felcia Bel & Sabeen (2022) [3]; Mihai et al. (2023) [2] |

| | | | | |
|---|---|---|---|---|
| Smart City Devices (Sensors) | Traffic and infrastructure management | Reduces traffic congestion, improves energy usage | Lack of standards, scalability, data integration | Mihai et al. (2023) [2] |
| Smart Grid Devices | Energy distribution | Optimizes energy consumption, integrates renewable energy sources | Data breaches, system complexity | Felcia Bel & Sabeen (2022) [3]; Mihai et al. (2023) [2] |
| Agricultural IoT (Soil Sensors, Drones) | Precision farming | Enhances crop yield, reduces water usage | High cost of devices, need for internet connectivity in rural areas | Mihai et al. (2023) [2]; Felcia Bel & Sabeen (2022) [3] |
| Smart Traffic Systems | Traffic management | Provides real-time traffic data, reduces accidents | Privacy concerns, data accuracy | Mihai et al. (2023) [2] |
| IoT Security Devices (Surveillance Systems) | Security and surveillance | Monitors and prevents unauthorized access | Susceptibility to cyberattacks, privacy breaches | Felcia Bel & Sabeen (2022) [3] |

In the paper of Mihai et al. (2023), the authors emphasize the transformative potential of IoT technology devices and gadgets across various sectors and fields focusing mostly at: healthcare field, agriculture field, and smart cities, highlighting its ability to improve and enhance the efficiency and quality of life over the time passed and also providing to the users efficient use of the technology to shorten some activities that waste the people and community life necessarily. However, they also describe the significant challenges and risks that the IoT technology in this century is facing, particularly in terms of security, scalability, and standardization. The authors Felcia Bel & Sabeen (2022) in their scientific paper are mostly focused on the security risks associated with IoT technology, discussing specific attacks and threats like botnets, DoS, and man-in-the-middle, while also exploring countermeasures that can be taken from the users to enhance and improve the security and the need for improved security frameworks in IoT technology networks.

From this point of view the focus of the IoT technology devices and gadgets development and implementation should be on increasing and enhancing the security of the devices and design of new frameworks that should be implemented in the future to prioritize the safety of the users, services and networks. Furthermore, a comparative table outlining the risks associated with IoT technology based on the papers [2] and [3] is presented.

**Table 3** Comparison of the risks associated with IoT technology, detailing their impact on different applications and industries, as discussed in the papers [2] and [3]

| Risk | Description | Impact | Affected IoT Application | Source |
|---|---|---|---|---|
| Data Privacy | Unauthorized access to personal data collected by IoT devices | Compromised personal information, legal implications | Healthcare IoT, Smart Homes, Wearables | Mihai et al. (2023) [2]; Felcia Bel & Sabeen (2022) [3] |

| | | | | |
|---|---|---|---|---|
| Cyberattacks (e.g., Botnets) | Networks of compromised devices used to execute malicious activities | Disruption of services, theft of sensitive data | Industrial IoT, Smart Homes | Felcia Bel & Sabeen (2022) [3] |
| Denial of Service (DoS) Attacks | Overloading systems with requests, rendering them unavailable | System downtime, financial losses | Smart Cities, Industrial IoT | Felcia Bel & Sabeen (2022) [3] |
| Man-in-the-Middle Attacks | Interception and modification of communication between devices | Loss of data integrity, unauthorized control | Smart Grids, Healthcare IoT | Felcia Bel & Sabeen (2022) [3] |
| Device Vulnerabilities | Exploitation of weaknesses in IoT device firmware and software | Unauthorized access, malware infections | All IoT devices (e.g., smart homes, wearables) | Mihai et al. (2023) [2] |
| Lack of Standardization | No universal security standards for IoT devices | Security loopholes, interoperability issues | Industrial IoT, Smart Cities | Mihai et al. (2023) [2]; Felcia Bel & Sabeen (2022) [3] |
| Scalability Issues | Difficulty in managing large numbers of interconnected devices | Performance bottlenecks, increased attack surface | Smart Cities, Industrial IoT | Mihai et al. (2023) [2] |
| Energy Consumption | IoT devices may require frequent charging or replacement due to high power demands | Decreased device longevity, increased costs | Wearables, Industrial IoT | Mihai et al. (2023) [2] |
| Software Update Risks | Difficulty in securely updating IoT devices remotely | Increased vulnerability to attacks | All IoT devices | Mihai et al. (2023) [2]; Felcia Bel & Sabeen (2022) [3] |

In the scientific paper of Mihai et al. (2023), the authors address the technical and security challenges and risks of IoT technology, including the risks and threats of data privacy and safety breaches, scalability issues, and the lack of standardization, which minimizes the widespread adoption of the IoT technology devices and gadgets. They describe the need for enhanced and improved security measures, frameworks and infrastructure to manage, monitor and configure the increasing number of connected devices in the network. The authors Felcia Bel & Sabeen (2022) in their scientific paper provide and highlight a detailed examination of IoT devices and gadgets security vulnerabilities, such as botnet and DoS attacks, describing the crucial need for advanced or improved countermeasures that may be as encryption protocols and learning-based methods to protect IoT networks and communication mediums.

This comparison highlights the need for enhanced countermeasures through encryption protocols, new methods for network protection, and frameworks to improve IoT technology integration. Focusing on interoperability and the incorporation of artificial intelligence or machine learning will further strengthen these efforts [2], [3].

## 5 FUTURE SECURITY DIRECTIONS AND CHALLENGES

This section of the paper outlines several countermeasures proposed by the authors, supported by the findings from sources [2] and [3], addressing key security challenges. These countermeasures are based on the strategies and future directions highlighted in the referenced works, with a focus on practical solutions that can be developed and implemented in the near future.

**Table 4** Comprehensive overviews of the countermeasures proposed by the authors of the scientific paper, also that are grounded in the research from the provided papers [2] and [3]

| IoT Security Risk | Proposed Countermeasure | Description | Source |
|---|---|---|---|
| Data Privacy Breach | End-to-end encryption with periodic key updates | Encrypt data at all stages of transmission and update keys regularly to prevent unauthorized access. | Mihai et al. (2023) [2]; Felcia Bel & Sabeen (2022) [3] |
| Botnet Attacks | Implementation of device authentication and intrusion detection systems | Use robust authentication protocols and intrusion detection systems (IDS) to detect and block botnet activities. | Felcia Bel & Sabeen (2022) [3] |
| Denial of Service (DoS) Attacks | Rate limiting and resource isolation | Implement rate limiting to control the number of requests and isolate critical resources to prevent them from being overwhelmed | Felcia Bel & Sabeen (2022) [3] |
| Man-in-the-Middle Attacks | Mutual authentication with session encryption | Use mutual authentication protocols along with encrypted sessions to ensure the integrity of communication between devices. | Felcia Bel & Sabeen (2022) [3]; Mihai et al. (2023) [2] |
| Device Vulnerabilities | Regular software/firmware updates and security patches | Ensure all IoT devices have regular software/firmware updates to patch vulnerabilities and mitigate risks. | Mihai et al. (2023) [2] |
| Lack of Standardization | Development of universal IoT security standards | Propose universal security standards and certification requirements for IoT devices across industries. | Mihai et al. (2023) [2]; Felcia Bel & Sabeen (2022) [3] |
| Scalability Issues | Use of blockchain for decentralized security management | Implement blockchain technology for decentralized management of IoT security, which can handle large-scale deployments securely. | Mihai et al. (2023) [2] |

| | | | |
|---|---|---|---|
| Energy Constraints | Low-power cryptographic algorithms and energy-efficient protocols | Utilize lightweight cryptographic algorithms and protocols designed for devices with limited power resources. | Felcia Bel & Sabeen (2022) [3] |
| Software Update Risks | Secure remote updating mechanisms with authentication and encryption | Ensure remote updates are authenticated and encrypted to prevent unauthorized modifications during the update process. | Mihai et al. (2023) [2]; Felcia Bel & Sabeen (2022) [3] |
| Physical Security Risks | Tamper-evident packaging and physical protection of critical devices | Employ tamper-evident seals and physical hardening techniques to protect IoT devices from tampering or theft. | Mihai et al. (2023) [2]; Felcia Bel & Sabeen (2022) [3] |

In the paper of Mihai et al. (2023), the authors focus on the need for improved security measures that must be used and be implemented in IoT technology systems due to issues such as data breaches, unauthorized access and device vulnerabilities. The authors [2] and [3] describe the importance of designing and developing universal standards, frameworks and regular software updates to address or overcome these risks and threats. The authors Felcia Bel & Sabeen (2022) in the paper focused on analyzing specific IoT technology security challenges and vulnerabilities such as: botnet attacks or DoS attacks, with proposing solutions that can be used as: encryption, authentication protocols, and intrusion detection systems to mitigate these threats or risks.

## 6 CONCLUSION

In the last ten years, the rapid growth of IoT research and development has demonstrated its potential to transform various sectors, ranging from education to advanced scientific fields. However, this expansion has also made IoT devices, systems, and gadgets vulnerable to numerous risks and threats, underscoring the urgent need to tackle these vulnerabilities and establish strong security measures. This paper highlights the vital role of IoT technology while also recognizing the challenges and risks it encounters, especially concerning security and privacy. The study offers a thorough review of IoT's security objectives, challenges, and goals, along with an in-depth analysis of different attacks, threats, and countermeasures. It outlines future directions and challenges aimed at enhancing IoT security, addressing both existing and emerging threats. By focusing on the development and implementation of robust security frameworks and universal standards, IoT technologies can reach their full potential without jeopardizing user safety, privacy, or system integrity. In addition to tackling security issues, this paper emphasizes the dual role of IoT in promoting energy efficiency and supporting sustainable development. By integrating IoT into essential areas like smart grids, renewable energy systems, and smart cities, it has the potential to revolutionize both technology and ecology. To achieve this vision, future initiatives should aim to incorporate IoT technologies into broader sustainability frameworks, ensuring that technological progress aligns with ecological advancement. With the right strategies in place, IoT can become a key element of a secure, energy-efficient, and sustainable future.

## 7 REFERENCES

[1] Ioannis Andrea, Chrysostomos Chrysostomou and George Hadjichristofi, Internet of Things: Security Vulnerabilities and Challenges, The 3rd IEEE ISCC 2015 International Workshop on Smart City and

Ubiquitous Computing Applications, Cyprus, 2015.

[2] Mihai, A., Mănăilă, Ş. C., & Dumitraşcu, A. S., Internet of Things – Overview, Database Systems Journal, Vol. XIV, No. 1/2023.

[3] Felcia Bel, H.J., & Sabeen, S., A Survey on IoT Security: Attacks, Challenges, and Countermeasures, Webology, 19(1), 2022.

[4] Sahibzada Saadoon Hammad, Ditsuhi Iskandaryan and Sergio Trilles, An unsupervised TinyML approach applied to the detection of urban noise anomalies under the smart cities environment, Internet of Things 23, 2023.

[5] Akbar Telikani, Asadollah Shahbahrami, Jun Shen, Georgi Gaydadjiev and Jerry Chun-Wei Lin, An edge-aided parallel evolutionary privacy-preserving algorithm for Internet of Things, Internet of Things 23, 2023.

[6] Zainab Noor, Sadaf Hina, Faisal Hayat and Ghalib A. Shah, An intelligent context-aware threat detection and response model for smart cyber-physical systems, Internet of Things 23, 2023.

[7] Anam Nawaz Khan, Atif Rizwan, Rashid Ahmad, Qazi Waqas Khan, Sunhwan Lim and Do Hyeun Kim, A precision-centric approach to overcoming data imbalance and non-IIDness in federated learning, Internet of Things 23, 2023.

[8] Hossein Pourrahmani, Adel Yavarinasab, Amir Mahdi Hosseini Monazzah and Jan Van herle, A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the Blockchain, Internet of Things 23, 2023.

[9] Mireya Lucia Hernandez-Jaimes, Alfonso Martinez-Cruz, Kelsey Alejandra Ramírez-Gutiérrez and Claudia Feregrino-Uribe, Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures, Internet of Things 23, 2023.

[10] Marco Marcozzi, Orhan Gemikonakli, Eser Gemikonakli, Enver Ever and Leonardo Mostarda, Availability evaluation of IoT systems with Byzantine fault-tolerance for mission-critical applications, Internet of Things 23, 2023.

[11] Hassaan Malik, Tayyaba Anees, Muhammad Faheem, Muhammad Umar Chaudhry, Aatka Ali and Muhammad Nabeel Asghar, Blockchain and Internet of Things in smart cities and drug supply management: Open issues, opportunities, and future directions, Internet of Things 23, 2023.

[12] Marc Vila, Maria-Ribera Sancho, Ernest Teniente and Xavier Vilajosana, Critical infrastructure awareness based on IoT context data, Internet of Things 23, 2023.

[13] Ihab Nassra and Juan V. Capella, Data compression techniques in IoT-enabled wireless body sensor networks: A systematic literature review and research trends for QoS improvement, Internet of Things 23, 2023.

[14] Miguel Gayo-Abeleira, F.J. Rodríguez, Carlos Santos, Ying Wu, Yanpeng Wu, Juan C. Vasquez and Josep M. Guerrero, Design and implementation of multiprotocol framework for residential prosumer incorporation in flexibility markets, Internet of Things 23, 2023.

[15] Dazhi Gao, Rongyang Li, Lingfeng Mao, Hongbo Wang and Huansheng Ning, Dynamic cooperation and mutual feedback network for shield machine, Internet of Things 23, 2023.

[16] Arturo Barriga, José A. Barriga, María José Moñino and Pedro J. Clemente, IoT-based expert system for fault detection in Japanese Plum leaf-turgor pressure WSN, Internet of Things 23, 2023.

[17] Lubna, Naveed Mufti, Sadiq Ullah, Abubakar Sharif, Muhammad Waqas Nawaz, Ahmed Alkhayyat, Muhammad Ali Imran and Qammer H. Abbasi, IoT enabled vehicle recognition system using inkjet-printed windshield tag and 5G cloud network, Internet of Things 23, 2023.

[18] G. Cano-Quiveu, P. Ruiz-de-Clavijo-Vazquez, M.J. Bellido, J. Juan-Chico and J. Viejo-Cortes, IRIS: An embedded secure boot for IoT devices, Internet of Things 23, 2023.

[19] Pierfrancesco Bellini, Luciano Alessandro Ipsaro Palesi, Alberto Giovannoni and Paolo Nesi, Managing complexity of data models and performance in broker-based Internet/Web of Things architectures, Internet of Things 23, 2023.

[20] Ibrar Yaqoob, Khaled Salah, Raja Jayaraman and Mohammed Omar, Metaverse applications in smart cities: Enabling technologies, opportunities, challenges, and future directions, Internet of Things 23, 2023.

[21] Tomas Lagos Jenschke, Marcelo Dias de Amorim and Serge Fdida, Nearby connections strategies:

Features, usage, and empirical performance evaluation, Internet of Things 23, 2023.

[22] Alejandro Peñuelas-Angulo, Claudia Feregrino-Uribe and Miguel Morales-Sandova, Revocation in attribute-based encryption for fog-enabled internet of things: A systematic survey, Internet of Things 23, 2023.

[23] Gleiston Guerrero-Ulloa, Ariel Fernandez-Loor, Francisco Moreira, Paulo Novais, Carlos Rodríguez-Domínguez and Miguel J. Hornos, Validation of a development methodology and tool for IoT-based systems through a case study for visually impaired people, Internet of Things 23, 2023.

[24] Rob van Kranenburg1 and Alex Bassi, IoT Challenges, Communications in Mobile Computing 2012, SpringerOpen Journal, 2012.

[25] Iqra Rafiq, Anzar Mahmood, Sohail Razzaq, S. Hassan M. Jafri and Imran Aziz, IoT applications and challenges in smart cities and services, The Journal of Engineering, The Institutio of Engineering and Technology, 2023.

[26] Ramya Prakash, JyotiNeeli and Manjunatha S., A survey of security challenges, attacks in IoT, E3S Web of Conferences 491, 04018 (2024), 2024.

[27] AbdelRahman H. Hussein, Internet of Things (IOT): Research Challenges and Future Applications, International Journal of Advanced Computer Science and Applications (IJACSA), 2019.

[28] Prof. Mohamed M. El Hadi, Overview of the IoT that meeting societal challenges, Scientific Articles, Sadar Academy for Management Sciences, July 2022.

[29] Ghazaleh Shirvani and Saeid Ghasemshirazi, Towards Sustainable IoT: Challenges, Solutions, and Future Directions for Device Longevity, Conference'17, July 2017, Washington, DC, USA, 2017.

[30] Falguni Jindal, Rishabh Jamar and Prathamesh Churi, Future and Challenges of Internet of Things, International Journal of Computer Science & Information Technology (IJCSIT) Vol 10, No 2, April 2018, 2018.

[31] Deekshaa Khanna and Ankit Sharma, Internet of Things Challenges and Opportunities, International Journal For Technological Research In Engineering Volume 6, Issue 12, August- 2019.

[32] Ball, C. S., & Degischer, D., IoT implementation for energy system sustainability: The role of actors and related challenges, Utilities Policy, 90, 101769, 2024.

[33] Jaber, M., Intelligent IoT for Sustainable Development Goals: Sensing with the Communication Network, Queen Mary University of London, 2024.

[34] Renda, A., & Laurer, M., IoT4SDGs: What can the digital transformation and IoT achieve for Agenda 2030?, Hitachi & CEPS, 2024.

[35] Malik, H., Anees, T., & Asghar, M. N., Blockchain and IoT in smart cities and drug supply management, Internet of Things Journal, 2024

[36] Lagos Jenschke, T., Amorim, M. D., & Fdida, S., Nearby connections strategies: Features, usage, and empirical performance evaluation, Internet of Things Journal, 2024.

[37] Biggar, D. R., & Hesamzadeh, M. R., Merchant investment in electricity transmission networks, Utilities Policy, 90, 101796, 2024.