IOT COMMUNICATION SECURITY: CHALLENGES AND SOLUTIONS

Paweł Kuraś[1], Patryk Organiściak[1], Bartosz Kowal[1], Veronika Vanivska[1], Krzysztof Demidowski[1], Krzysztof Smalara[1], Piotr Krawiec[2]
[1] Rzeszow University of Technology, Department of Complex Systems, Poland
[2] Rzeszow University of Technology, Machine Learning Student Science Club, Poland
Corresponcende: p.kuras@prz.edu.pl

Abstract

This paper investigates the obstacles and resolutions concerning the security of communication in the Internet of Things (IoT). It commences with a discussion of the remarkable proliferation of internet-connected devices, ranging from personal computers to mobile devices, and now to the era of IoT and IoE. The paper illuminates the impact of IoT on network addresses, leading to the depletion of IPv4 addresses and the necessity for address translation services. Subsequently, the article delves into the risks confronted by IoT systems, encompassing physical and digital assaults, unauthorized access, system failures, as well as diverse forms of malicious software. The significance of IoT security in industrial and agricultural systems is underscored. Finally, the paper concludes by presenting strategies to combat these risks, including antivirus countermeasures, safeguards against Distributed Denial-of-Service (DDoS) attacks, and security considerations in IoT systems for agriculture. In essence, this paper offers valuable insights into the challenges and solutions associated with ensuring the security of IoT communication.

Keywords: IoT, Internet of Things, IoE, Internet of Everything, Network Security

1. INTRODUCTION

The recent years have witnessed a remarkable proliferation of information technology and a surge in the number of Internet-connected devices on a global scale. The period from 1995 to 2000 was dominated by the prevalence of desktop computers, commonly known as personal computers (PCs) (Hannu et al., 2023). Subsequently, from 2000 to 2011, the era of mobile devices and the Bring Your Own Device (BYOD) concept took center stage (Cheerag et al., 2022). This was followed by the era of the Internet of Things (IoT) from 2011 to 2020, which

DOI: 10.5604/01.3001.0054.3829
Received: 29.11.2023 Revised: 10.01.2024 Accepted: 16.01.2024

has now transitioned into the ongoing era of the Internet of Everything (IoE). In the year 2000, the number of devices connected to the worldwide Internet amounted to 200 million (Yufi & Cahaya, 2022). The results of this exponential growth in internet-connected devices are depicted in the example of Polish users in Fig. 1 - with a substantial increase to 10 billion by 2011, and further escalated to 50 billion in 2020 (Marzano et al., 2017). At present, video data traffic accounts for a staggering 80% of all Internet traffic, and along with audio data traffic, it is highly sensitive to latency and packet loss. The convenience of learning and entertainment is primarily facilitated by platforms such as YouTube and Netflix, offering a diverse range of videos and courses (Gama et al., 2021). Companies operating across various locations worldwide leverage videoconferencing to connect their employees, enabling collaborative work (Smith, 2004). The concept of the Internet of Everything encompasses interconnected devices, individuals, data and processes that dynamically interact and influence one another (DaCosta & Henderson, 2013). As we look forward, the future of the Internet is envisaged to be a metaverse, a virtual representation of life wherein individuals and corporations will possess virtual avatars and subsidiaries (Far et al., 2023).

The impact of the Internet of Things has been profound in amplifying the number of networked devices. Smart homes and factories have eagerly embraced IoT devices such as sensors, cameras and control panels (Umair et al., 2021). Consequently, previously underserved areas of the world have witnessed digitization and computerization efforts, leading to the depletion of IPv4 protocol addresses in 2019 (Hughes, 2022). The challenge was addressed through the introduction of NAT/PAT address translation services; however, this posed difficulties for Internet users attempting to access local network services (Ghosh, 2020). In the future, manufacturers will strive to outshine one another in terms of innovation, resulting in the ability to remotely configure every household appliance (Pratheesh et al., 2022). Despite the myriad benefits brought forth by IT technologies and products, they also harbor potential risks, necessitating the implementation of security-related standards and updates through appropriate policies in order to alleviate these concerns.

In today's world, there has been a paradigm shift in the multidimensional approach to security, which is now viewed as a product. In the face of global challenges, there is an urgent need to assess the sense of security and ability to maintain it (Szykuła-Piec & Piec, 2020).

The primary objective of this manuscript is to elucidate the prevailing challenges and potential solutions pertaining to the security of IoT systems. The scope of this work encompasses an in-depth analysis of security issues, including viruses and worms, destructive attacks, denial of service (DoS) attacks, and security considerations within the realm of industrial IoT systems.

Figure 1. Survey about internet usage by Polish users in years 2002–2021, positive answers (Wojciechowska, 2022)

2. INTERNET OF THINGS – DEFINITION, COMPONENTS, AND APPLICATIONS

The term "Internet of Things" (IoT) was first introduced in 1999 (Ashton, 2009). It pertains to distinctively identified devices that are interconnected via a computer network, enabling the gathering, exchange and processing of information (Mukhopadhyay & Suryadevara, 2014). The concept of IoE (Internet of Everything) encompasses the inclusion of processes and individuals within the Internet of Things, with their interdependence and dynamic nature (DaCosta & Henderson, 2013). The constituents of the Internet of Things comprise control panels, cameras, sensors, as well as actuators (such as gates, doors, windows, radiators, fans and air conditioners). For these elements, it is necessary to establish schedules and regulations that govern their operations, for instance, regulating the actuators based on the prevailing time and the data acquired from the sensors (Rayes & Salam, 2022).

The Internet of Things (IoT) plays a pivotal role in numerous areas such as smart cities (Pawłowicz et al., 2019), industrial operations, medical monitoring, smart homes, autonomous vehicles, Personal Area Network devices, and the management of gas and electricity transmission systems (Li et al., 2020). Its functionalities include controlling urban traffic lights through data from intersection cameras (Tchuitcheu et al., 2020), monitoring factory machinery for maintenance needs (Parpala et al., 2020), tracking patient health parameters in real time (Sangeethalakshmi et al., 2023), automating the remote operation of home appliances (Gunge & Yalagi, 2016), aiding decision-making in self-driving cars using environmental sensors (Bautista, & Mester, 2023), managing personal gadgets like smartwatches and Bluetooth headsets from smartphones (Takiddeen & Zualkernan, 2019), and also regulating the performance of energy transmission networks (Sanchez-Sutil & Cano-Ortega, 2021).

3. SECURITY VULNERABILITIES IN INTERNET OF THINGS (IOT) ARCHITECTURE

In the realm of Internet of Things (IoT) systems, a spectrum of security vulnerabilities exists. Physical threats involve the alteration or destruction of devices, potentially leading to the introduction of malicious configurations, such as unauthorized network ports activation (Dul et al., 2023). Such destruction can be accidental or deliberate, often resulting from local natural disasters (Jakubczak, 2022). Digital vulnerabilities are manifold, encompassing malware, exploits, Denial of Service (DoS) attacks, and strategic multi-phased directional attacks aimed at device hijacking and confidentiality breaches (Milosevic et al., 2016). This category extends to information manipulation where data integrity is compromised for financial or disruptive purposes.

Unauthorized intrusions in IoT systems typically become manifested through 'man-in-the-middle' attacks (Cekerevac et al., 2017), either passive (eavesdropping) or active (forging communications). Additionally, session hijacking (Humaira et al., 2020) and network eavesdropping are prevalent (Liao et al., 2018) where attackers surreptitiously gather data about network characteristics. System failures, another critical concern (Ahmad et al., 2018), arise from loss of power (Synowiec, 2019), communication (Krupanek & Bogacz, 2018) or essential services, often due to suboptimal hardware and software choices (Chen et al., 2016), external disruptions, or adverse environmental conditions (Gómez et al., 2017), with functionality generally resuming once these issues are resolved (Synowiec, 2019).

Software-related issues also pose significant risks, including inadequate configurations (Baker, 2021), coding errors (Makhshari & Mesbah, 2021), weak or static passwords, absence of multi-factor authentication (Yu et al., 2020), and lack of data encryption (Dul et al., 2023). Moreover, external catastrophes and conflicts, such as natural disasters and hybrid warfare tactics targeting communication infrastructures and energy supplies, can lead to extensive damage to network and power infrastructure, further exacerbating the security challenges in IoT systems (Jakubczak, 2022).

3.1. MALWARE – DEFINITION AND TYPES

Malware, a term that comprises a variety of malicious software, notably worms (spreading using the network architecture) and viruses (spreading via infected media), operates covertly to perform harmful actions unbeknownst to the user (Zieliński, 2018). These attacks are generally non-targeted, affecting all vulnerable devices rather than specific ones. Their impact includes altering, damaging or stealing data (Wangen, 2015). In the Internet of Things (IoT) systems, the interception or modification of data from a single sensor can lead to significant damage due to the interconnected nature of these systems where the output of various sensors might depend on the data from the corrupted one (Husamuddin

& Qayyum, 2017). The proliferation of malware has been graphically depicted in Fig. 2, which presents annual detections of new malware worldwide from 2015 to May 2019, reflecting a steady increase over the years.

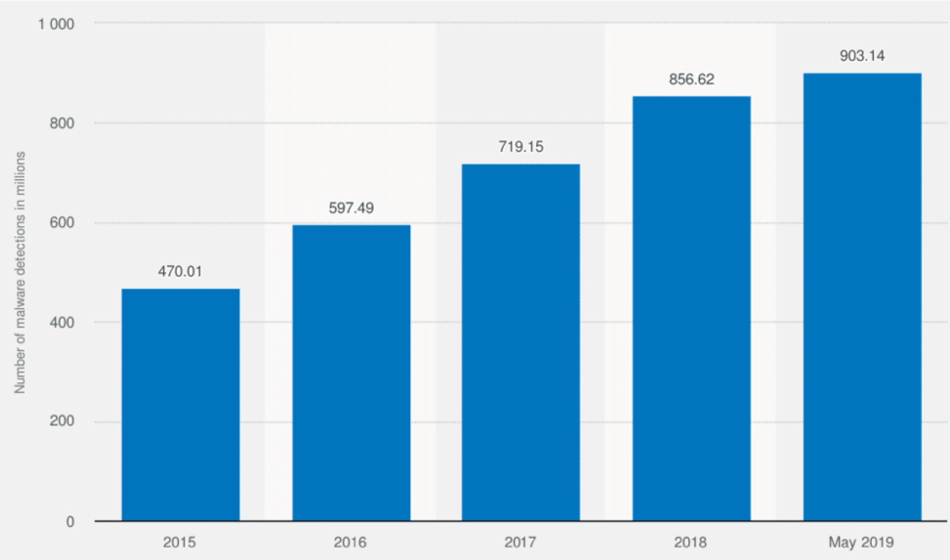

Figure 2. Annual detections of new malware worldwide from 2015 to May 2019 – in millions (Cantrell, 2022)

3.1.1. COMPUTER VIRUSES AND COMPUTER WORMS

Macro viruses, a subset of viruses that affect text documents, are notably difficult to detect due to their resistance to standard access control protections and their ability to propagate through email communications (Bontchev, 1998). Their universality poses a serious risk to various hardware platforms and multiple versions of text applications, underscoring the need for advanced protection mechanisms within text editing software. Viruses are made of distinct components: the payload, which carries out the intended functions of the virus; the trigger, the code that seeks the right conditions to activate the virus; and the infection code, or the infection vector, which is responsible for the virus replication. The virus lifecycle includes a dormancy phase, propagation phase, activation phase and execution phase, each representing different stages of virus activity from inactivity to the execution of harmful actions (Szappanos, 2002).

There are two primary classifications of viruses: simple and compressed ones. Simple viruses are single-segment codes that are generally less harmful and more easily detectable due to their static nature. Compressed viruses, on the other hand, are capable of spreading to other objects and inflicting significant damage during the host's operation (Gupta et al., 2022). Their modus operandi includes searching for specific file types, compressing them, inserting their code, decompressing the files, and then executing the infected files. Viruses may employ self-encryption, polymorphism and metamorphism to conceal themselves, complicating their detection. Infection vectors are diverse, including files, RAM, disk boot sectors and macros within application files, such as those found in text editors (Serazzi & Zanero, 2003).

While computer viruses are software that spreads via infected media, computer worms are malicious software that spreads using the network infrastructure. Computer worms are highlighted as a particularly destructive standalone form of malware that exploits system vulnerabilities independently of a host file. These worms not only strain infrastructure resources but also facilitate the transfer of additional malware and can lead to the compromise of sensitive user data and settings (Smith et al., 2009).

3.1.2. OTHER ATTACK METHODOLOGIES

The change in malware tactics is reflected in Fig. 3, which shows a decline in the number of attacks on non-standard ports to 9% in 2021, suggesting an adaptation in attack methodologies. The malware taxonomy also includes Trojan horses (Denning, 1988), exploits (Miller, 2008), keyloggers (Singh & Choudhary, 2021), rootkits (Kim et al., 2012), backdoors (Zhang & Paxson, 2000), flooders (Sim, 2018), spammers (Song et al., 2011), adware (Gao et al., 2019), bots/zombies (Choo, 2007), logic bombs (Dusane & Pavithra, 2020), portable codes (Rad et al., 2012), autorooters (Pang et al., 2004) and downloaders (Rossow et al., 2013). This diverse array of malware types, as depicted in Fig. 4, indicates that backdoor attacks are currently the most common ones, dominating the landscape of cybersecurity threats and reinforcing the critical need for multifaceted security defenses.

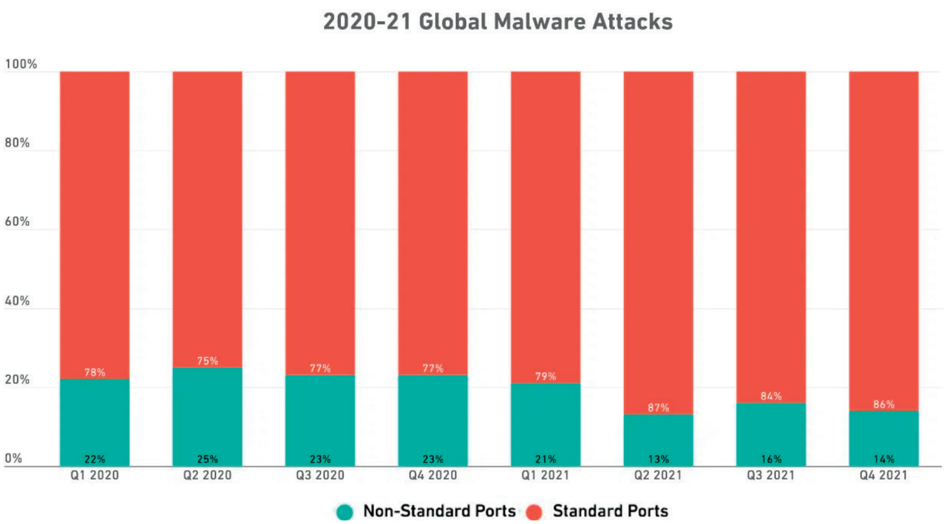

Figure 3. The number of attacks on non-standard ports dropped to 9% in 2021 (Comparitech, 2023)

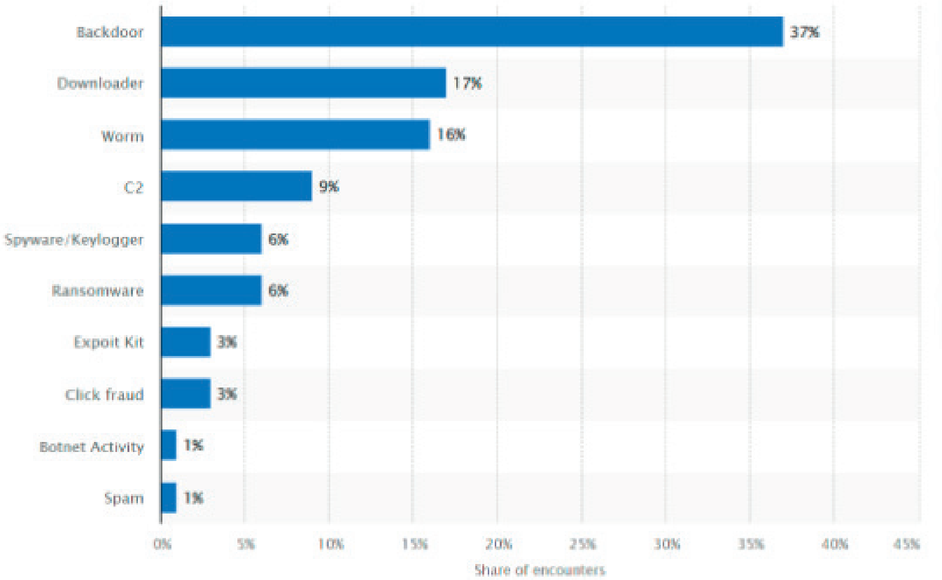

Figure 4. Backdoor attacks lead in number (Petrosyan, 2023)

3.2. DESTRUCTIVE ATTACKS

In the field of cybersecurity, destructive attacks are those that aim to incapacitate electronics or infrastructure of a system via direct physical assault. Utilizing high-energy electrical pulses to damage electronic circuitry is the most common tactic (Moran, 2012). Such methods were not only theoretical concerns but have had real-world applications (Jakubczak, 2022), as evidenced by Fig. 5, which depicts the bombing of critical infrastructure in regions of Ukraine during the autumn of 2022. Adversaries may exploit the power supply network to introduce destructive electrical pulses, thereby overwhelming and damaging electronic devices (Moran, 2012). Electromagnetic pulses, although more costly, offer a high-impact alternative, potentially disabling electronics across vast areas when deployed via military-grade technology or nuclear explosions (Szubrycht & Szymański, 2005).

Destructors are key instruments in such attacks, designed to deliver destructive currents into the electrical grid, with some being capable of releasing up to 300 megajoules of energy (Świętochowski, 2018). To mitigate such threats, Uninterruptible Power Supplies (UPS) systems of various types and configurations are deployed. These systems range from offline to online, with the latter providing seamless power continuity in the event of grid failure. Despite these defenses, the sustained integrity of a power supply of a system remains a critical challenge in view of sophisticated destructive attacks (Alqinsi et al., 2018).

Figure 5. Regions of Ukraine where critical infrastructure was bombed in autumn 2022 (Lukiv, 2022)

3.3. DENIAL OF SERVICE ATTACKS

A Denial of Service (DoS) attack aims to exhaust critical system resources, thus disabling computer systems or services. These resources include computational power, memory, disk storage and network bandwidth. DoS attacks fall into three categories: targeting limited network resources, destroying physical network infrastructure, or disrupting network configuration. A Distributed Denial of Service (DDoS) attack is an escalated assault that uses a network of compromised machines to flood a target with traffic, rendering services inaccessible to intended users (Protasowicki, 2018). Key DDoS attack techniques involve SYN packets that exhaust server resources and ICMP ECHO requests that generate overwhelming traffic (Gupta et al., 2016). Execution of such attacks requires malware, knowledge of system vulnerabilities, and the ability to scan and exploit unprotected computers (Kumar & Jain, 2023). Notable tools for DDoS include Trinoo (Dittrich, 1999), TFN, TFN2K, and Stacheldraht (Nagpal et al., 2015). Fig. 6 provides a statistical representation of the distribution of DDoS attacks across different countries in 2018, illustrating the global scale and targeted nature of these cyber threats.

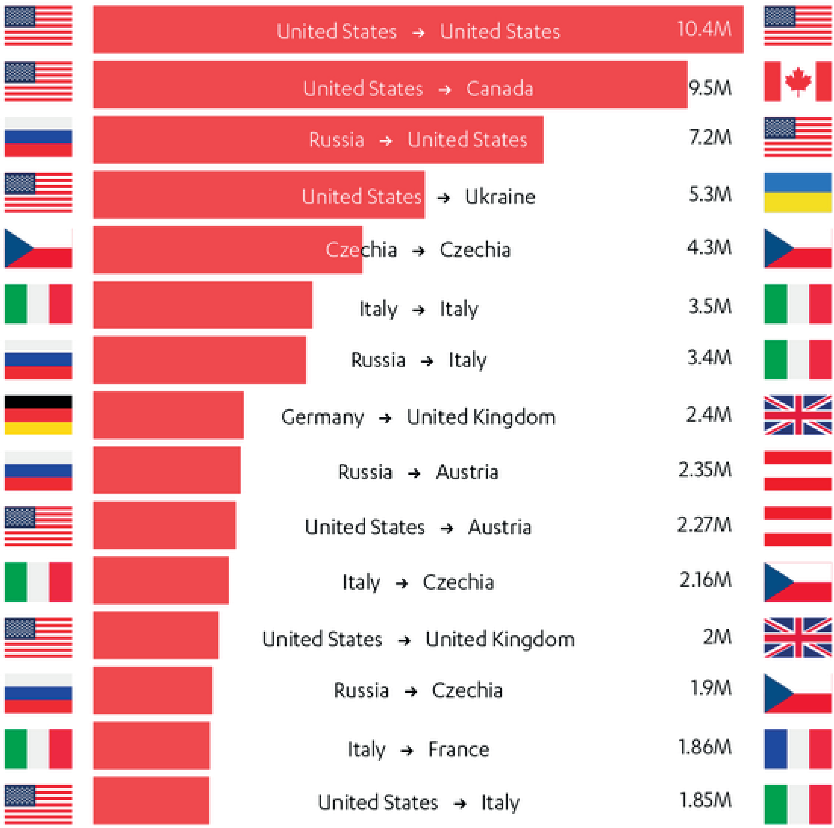

Figure 6. Breakdown of the number of DDoS attacks between countries in 2018 (Michael, 2019)

4. SECURITY ISSUES IN SELECTED IOT BRANCHES

Within the range of industrial domains, the integration of Internet of Things (IoT) technologies is becoming increasingly prevalent. These sectors include agriculture (Stočes et al., 2016), automotive industry (Ghosh et al., 2022), finance (Khanboubi et al., 2019), construction (Gamil et al., 2020), education (Szabłowski, 2023), healthcare (Kwiatkowska, 2016), manufacturing, mining (Szozda, 2017), and retail (Krysiński, 2016). IoT devices deployed across these fields are instrumental in the systematic collection, transmission and processing of information. They also play a critical role in data storage and the execution of artificial intelligence (AI) algorithms for enhanced decision-making (Rathee, 2020). Evidence of this widespread IoT utilization is underscored in Fig 7.

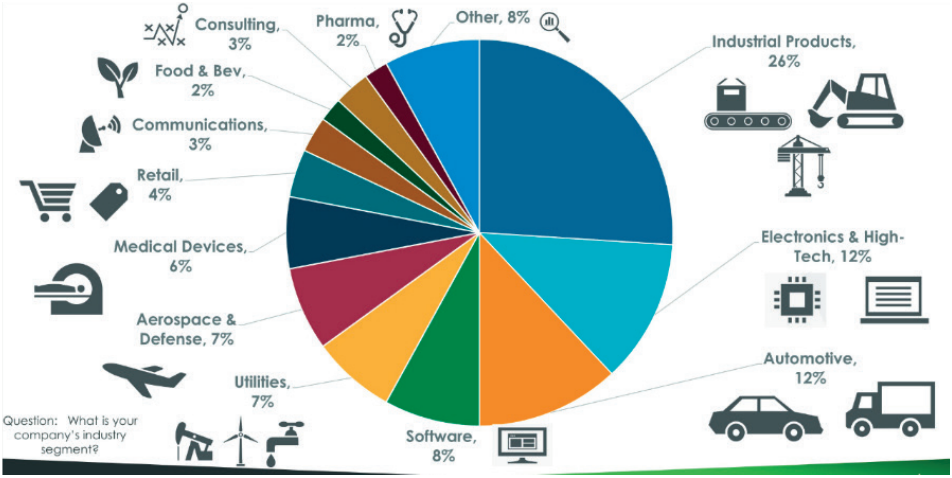

Figure 7. Results of the user survey for ThingWorx, PTC's industrial IoT platform (Immerman, 2022)

4.1. INDUSTRAL IOT (IIOT)

In the industrial Internet of Things (IoT) landscape, an amalgamation of advanced technologies is essential for operational efficiency. This includes machine-to-machine communication for data exchange (Walczak et al., 2012), artificial intelligence for autonomous decision-making (Kuraś et al., 2023), and real-time monitoring systems for network security (Strzałka et al., 2021). The infrastructure is bolstered by distributed computing resources, including cloud storage, and is further enhanced by robotics for tasks like assembly and resource harvesting (El-Sayed, 2017). Predictive maintenance algorithms and Big Data analytics are critical for equipment monitoring and data analysis (Rysz, 2020). However, this technological sophistication renders Industrial IoT systems vulnerable to various cyber threats. Communication interception between controllers and actuators can lead to data leaks (Herzberg & Kfir, 2019), while sensor manipulation might cause system disruptions (Zhu et al., 2011). Actuator compromise can affect manufacturing processes (Perner et al., 2016), and IoT management systems are susceptible to attacks like DDoS and software exploitation (Protasowicki, 2018).

Vulnerabilities in communication protocols can lead to unauthorized system access and data theft, and power supply system attacks can disrupt device functionality (Matejkowski & Szmyd, 2023). Moreover, vulnerabilities in communication or management protocols can be exploited to gain privileged system access, install backdoors, or facilitate data theft (Bator et al., 2023). Attacks executed via direct console access can cause the commandeering of additional devices within the company's network (Zaddach, 2013). Power supply systems are not immune, with attacks manipulating battery level readings leading to rapid energy depletion or disorganized equipment operation, either through physical damage or malware introduction (Case, 2016). Additionally, the uniformity of devices within large enterprise IoT networks presents a risk of botnet formation, potentially leading to extensive DDoS attacks. These multifaceted vulnerabilities underscore the imperative for robust security measures within industrial IoT infrastructures, to safeguard against the diverse array of cyber threats inherent in these technologically advanced systems.

4.2. IOT SYSTEMS IN AGRICULTURE

Contemporary agricultural practices increasingly utilize satellite imagery and drone surveillance for crop monitoring. These technologies enable farmers to assess crop conditions and efficiently plan field operations (Nakalembe et al. 2021, Mogilie et al., 2018). Advanced agricultural machinery, equipped with satellite navigation, is semi-autonomous, facilitating precise field cultivation and optimizing the coverage area. Integrated sensors in these machines measure the distribution of fertilizers, seeds and water, enhancing resource efficiency and environmental sustainability (Rahmadian & Widyartono, 2020). Additionally, sensor technology is employed to monitor machinery wear and tear. Crop surveillance extends to camera systems and sensors that gauge soil moisture, temperature and other environmental parameters like rainfall, light intensity and atmospheric CO_2 levels (Lee et al., 2010). Solar-powered multifunctional sensors prove to be particularly effective in these applications (Bogue, 2012). In granaries, stables and barns, sensors play a crucial role in monitoring temperature and humidity levels, essential for optimal storage conditions and animal welfare (Zhang et al., 2016). Motion-activated video surveillance systems with audio deterrents are also used to protect crops from wildlife (Jeon et al., 2019).

The expansive nature of agricultural lands necessitates efficient data transmission protocols. LoRaWAN, with its long-range capabilities (up to 15 km) and low throughput, is well-suited for connecting field sensors to central stations (Davcev et al., 2018). Power efficiency is crucial due to the limited availability of power sources in agricultural settings. The Hub and Spoke network topology is adopted, where data is collected from sensors by a hub and transmitted to the control panel, often on a scheduled, energy-saving cycle, such as hourly one (Singh et al., 2020). Farm security comprises both physical measures, like fencing and video surveillance, and discreet deployment of sensors and IoT devices (Baranwal & Pateriya, 2016). Redundancy in sensor deployment ensures reliability, allowing rapid anomaly detection if a sensor is compromised (Shen & Wu, 2011). While agricultural machinery is advancing towards automation, it is recommended that these systems provide data and recommendations to operators rather than fully autonomous operation, ensuring human oversight in decision-making processes related to navigation and field operations (Stočes et al., 2016).

5. CHALLENGES AND SOLUTIONS TO CYBERTHREATS IN IOT

The economic impact of computer system downtime is multifaceted, encompassing halted employee productivity, disrupted service provision, and the need for specialized system restoration expertise (Oostenbrink, 2015). This complexity is exemplified in Fig. 8, which illustrates the average losses incurred by a company fully reliant on cloud services after just one hour of system failure. The rapidly evolving IoT landscape presents significant security challenges. The continuous release of new solutions by various manufacturers causes delayed and fragmented security standard adoption. The wide array of devices, each collecting sensitive data, amplifies the potential impact of cyber-attacks.

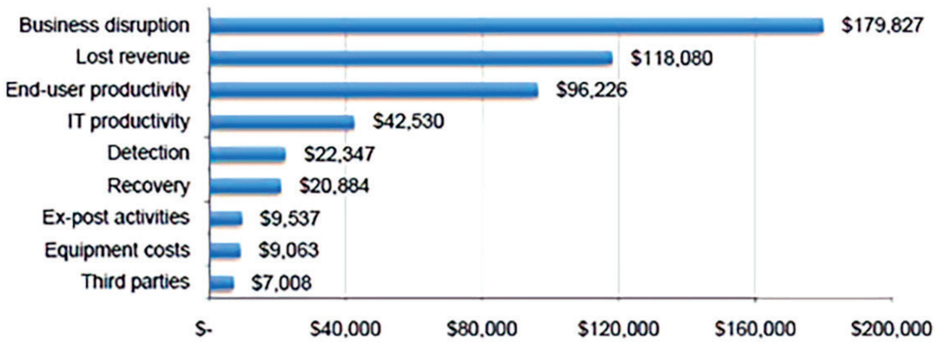

Figure 8. Average losses after 1 hour of failure for a company fully dependent on cloud services (Cohen, 2019)

Cost-reduction strategies in critical infrastructure management have led to the integration of low-cost IoT solutions, raising national security concerns. The diversity of hardware platforms necessitates varied development approaches, often at the expense of security (De Felice & Petrillo, 2018). Partial upgrades in IoT devices further compromise security, necessitating policy adaptations. The lack of clearly defined security responsibilities, coupled with inadequate legislation and standards, exacerbates these challenges (Stoll & Breu, 2012). Competitive market pressures often lead to compromises in security subsystems due to cost-cutting measures.

Furthermore, the IT and cybersecurity sectors face a talent shortfall (Paidant, 2023), complicating the management of the diverse IoT environment. In industrial settings, the integration of legacy equipment with modern IoT devices exposes new security gaps (Rosas et al., 2017). The prioritization of productivity over security in business models (Adamkiewicz, 2005), complex supply chains and the selection of flawed IT solutions due to insufficient knowledge among personnel further heighten security risks. Enterprise security, spanning physical, information and production aspects, are challenged by the mass production of IoT devices, often resulting in oversimplified security measures. The necessity of staff training is emphasized, as untrained personnel are vulnerable to social engineering attacks (Zwilling et al., 2022).

5.1. COMBATING THREATS

Standard virus countermeasures in cybersecurity involve the detection, identification and elimination of viruses, with the aim of restoring the system to its pre-infection state. This process is typically executed by commercial antivirus software (Chen & Carley, 2004). The primary defense mechanism includes the deployment of a dedicated firewall at the Internet entry point and the utilization of a blocking server. This server, running a streamlined operating system, analyzes network traffic and tests suspicious processes in a sandbox environment. The configuration of the server and response protocols are managed by network administrators (Tudosi et al., 2023). In cases of post-infection digital resilience, response actions are initiated upon detection of suspicious activity by antivirus software. This involves transmitting infection reports to an analysis unit, which then formulates and disseminates a remediation plan to local network administrators and infected hosts.

Given the different nature of the worms, as this type of malware uses the network infrastructure to spread, worm containment strategies encompass a variety of approaches, including signature-based detection, content examination of worm commands, blocking of anomalous connections, and payload analysis within network packets. Proactive Worm Containment (PWC) leverages a security management station to dynamically configure firewalls and routers (Jhi et al., 2010). Additionally, network-based protection employs sensors both locally and remotely to detect irregular activities, with a correlation server analyzing these alerts to confirm worm attacks.

DDoS attack mitigation involves real-time detection and filtering of attack traffic, coupled with post-event investigations to identify and neutralize the source. Comprehensive system protection extends beyond internal measures to include physical security of power supply networks, requiring collaboration with electricity suppliers and stringent control of network equipment at distribution points (Da Silva Cardoso et al., 2018). To counteract electromagnetic interference, adherence to standards like ISO is crucial. This includes strategic placement of cables, grounding of distribution points, and maintaining minimum installation distances for various types of cables and devices to mitigate the impact of electromagnetic emissions from common office equipment (Boteanu et al., 2019).

6. SUMMARY AND THE FUTURE OF IOT

The Internet of Things (IoT), now evolving into the Internet of Everything (IoE), represents a paradigm shift in technological integration across diverse sectors. This transformation encapsulates a comprehensive network where not only traditional computing devices but also everyday objects are interconnected, facilitating the collection, processing and analysing of data. This expansive network permeates various domains, including manufacturing, agriculture, healthcare and banking. The proliferation of IoT devices, which now extend to IoE, occurs in both private and public sectors, including private enterprises, government offices and critical infrastructures. These devices, ranging from standard computers to mobile devices, often serve dual purposes, catering to both professional and personal uses. This ubiquity of IoT/IoE technologies introduces significant security challenges, as their unregulated infiltration creates vulnerabilities within organizational systems (Pietrek & Skelnik, 2023). The competitive landscape in the IoT/IoE industry, marked by a multitude of manufacturers vying for market dominance, often results in cost-cutting measures that compromise information security. The absence of a distinct demarcation between IoT security, information security and physical access security further complicates the establishment of robust protective measures (Gołębiewska et al., 2022). Hastily developed standards and the need for continual adaptation of security protocols reflect the dynamic nature of this field (Słota-Bohosiewicz, 2019). Moreover, the focus on operational efficiency and functionality often leads business owners to overlook critical security considerations (Wiercioch, 2022). This prioritization presents a stark contrast to the escalating risks associated with the expanding IoT/IoE landscape. As this sector continues to grow, the integration of comprehensive and adaptive security strategies is becoming increasingly vital to safeguard the integrity of both private and public digital infrastructures.

Funding

This research received no external funding.

REFERENCES

1. Adamkiewicz, S.L., (2005). *The correlation between productivity and the use of information security controls in small businesses*. The George Washington University.
2. Adriani, Y., Asyifa, C., (2022). The Use of Technological Devices: A Descriptive Study of Students in University. *International Conference on Science and Technology (ICOSTECH)*. doi: 10.1109/icostech54296.2022.9829086
3. Ahmad, S., Badwelan, A., Ghaleb, A. M., Qamhan, A., Sharaf, M., (2018). Analyzing critical failures in a production process: Is industrial IoT the solution? *Wireless Communications and Mobile Computing*, 1–12.

4. Alqinsi, P., Edward, I.J.M., Ismail, N., Darmalaksana, W., (2018). IoT-Based UPS monitoring system using MQTT protocols. In: *2018 4th International Conference on Wireless and Telematics (ICWT)*, pp. 1–5.
5. Ashton, K., (2009). That 'internet of things' thing. *RFID Journal*, 22(7), 97–114.
6. Baker, F.C., (2021). *Inadequacy of Existing Security Management Frameworks in Addressing Internet of Things (IoT) Cybersecurity-Related Risks*. Doctoral dissertation. Northcentral University.
7. Baranwal, T., Pateriya, P.K., (2016). Development of IoT based smart security and monitoring devices for agriculture. In: *2016 6th International Conference-Cloud System and Big Data Engineering (Confluence)*, pp. 597–602.
8. Bator, M., Przystasz, J., Serafin, M., (2023). Security of the DNSSEC protocol and its impact on online privacy protection. *Advances in Web Development Journal*, 1(1), 20.
9. Bautista, C., Mester, G., (2023). Internet of Things in Self-driving Cars Environment. *Interdisciplinary Description of Complex Systems: INDECS*, 21(2), 188–198.
10. Bogue, R., (2012). Solar-powered sensors: a review of products and applications. *Sensor Review*, 32(2), 95–100.
11. Bontchev, V., (1998). Macro virus identification problems. *Computers & Security*, 17(1), 69–89.
12. Boteanu, A., Răstoceanu, F., Rădoi, I., Rusea, C., (2019, October). Modeling and simulation of electromagnetic shielding for IoT sensor nodes case. In: *2019 International Conference on Speech Technology and Human-Computer Dialogue (SpeD)*, pp. 1–6.
13. Cantrell, K., (2022, September 15). *Half of the malware detected in 2019 was classified as zero-day threats, making it the most common malware to date*. https://www.cynet.com/blog/half-of-the-malware-detected-in-2019-was-classified-as-zero-day-threats-making-it-the-most-common-malware-to-date/.
14. Case, D.U., (2016). Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*, 388(1-29), 3.
15. Cekerevac, Z., Dvorak, Z., Prigoda, L., Cekerevac, P., (2017). Internet of things and the man-in-the-middle attacks–security and economic risks. *MEST Journal*, 5(2), 15–25.
16. Cheerag, K., Sindhwani, N., Chaudhary, A., (2022). Analysing the Impact of Cyber-Threat to ICS and SCADA Systems. *International Mobile and Embedded Technology Conference (MECON)*, Noida, India, pp. 466–470. doi: 10.1109/MECON53876.2022.9752425
17. Chen, D., Cong, J., Gurumani, S., Hwu, W. M., Rupnow, K., Zhang, Z., (2016). Platform choices and design demands for IoT platforms: cost, power, and performance tradeoffs. *IET Cyber-Physical Systems: Theory & Applications*, 1(1), 70–77.
18. Chen, L.C., & Carley, K.M., (2004). The impact of countermeasure propagation on the prevalence of computer viruses. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 34(2), 823–833.
19. Choo, K.K.R., (2007). Zombies and botnets. *Trends & issues in crime and criminal justice*, no. 333. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi333.

20. Cohen, G., (2019). *Downtime, outages and failures – understanding their true costs*. https://www.evolven.com/blog/downtime-outages-and-failures-understanding-their-true-costs.html.
21. Comparitech (2023). *Malware statistics in 2023: Frequency, impact, cost & more*. https://www.comparitech.com/antivirus/malware-statistics-facts/.
22. Da Silva Cardoso, A.M., Lopes, R.F., Teles, A.S., Magalhães, F.B.V., (2018, April). Real--time DDoS detection based on complex event processing for IoT. In: *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pp. 273–274.
23. DaCosta, F., & Henderson, B., (2013). *Rethinking the Internet of Things: a scalable approach to connecting everything*, Springer Nature, p. 192.
24. Davcev, D., Mitreski, K., Trajkovic, S., Nikolovski, V., Koteli, N., (2018, June). IoT agriculture system based on LoRaWAN. In: *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*, pp. 1–4.
25. De Felice, F., Petrillo, A., (2018). *Human factors and reliability engineering for safety and security in critical infrastructures. Decision Making, Theory, and Practice*. Springer, Cham.
26. Denning, P.J., (1988). *Computer viruses*. No. NASA-CR-184680.
27. Dittrich, D., (1999). *The DoS Project's 'trinoo' distributed denial of service attack tool*. University of Washington, 10.
28. Dul, M., Gugała Ł., Łaba K., (2023). Protecting web applications from authentication attacks. *Advances in Web Development Journal*, 1(1).
29. Dusane, P.S., Pavithra, Y., (2020). Logic Bomb: An Insider Attack. *International Journal*, 9(3).
30. Gama, E.S., de Araujo, L., Immich, R., Bittencourt, L.F., (2021). Video Streaming Analysis in Multi-tier Edge-Cloud Networks. In: *8th International Conference on Future Internet of Things and Cloud (FiCloud)*, Rome, Italy, pp. 19–25. doi: 10.1109/FICLOUD49777.2021.00011
31. El-Sayed, H., Sankar, S., Prasad, M., Puthal, D., Gupta, A., Mohanty, M., & Lin, C.T., (2017). Edge of things: The big picture on the integration of edge, IoT and the cloud in a distributed computing environment. *IEEE Access*, 6, 1706–1717.
32. Far, S.B., Rad, A.I., Bamakan, S.M.H., & Asaar, M.R., (2023). Toward Metaverse of everything: Opportunities, challenges, and future directions of the next generation of visual/virtual communications. *Journal of Network and Computer Applications*, 103675. DOI:10.1016/j.jnca.2023.103675
33. Gamil, Y.A., Abdullah, M., Abd Rahman, I., Asad, M.M., (2020). Internet of things in construction industry revolution 4.0: Recent trends and challenges in the Malaysian context. *Journal of Engineering, Design and Technology*, 18(5), 1091–1102.
34. Gao, J., Li, L., Kong, P., Bissyandé, T.F., & Klein, J., (2019). Should you consider adware as malware in your study?. In: *2019 IEEE 26th International Conference on Software Analysis, Evolution and Reengineering (SANER)*, pp. 604–608.
35. Ghosh, J., (2020). Corporate networking with advance routing, switching and security. In: *2020 IEEE 1st International Conference for Convergence in Engineering (ICCE)*, pp. 311–314.

36. Ghosh, R.K., Banerjee, A., Aich, P., Basu, D., Ghosh, U., (2022). Intelligent IoT for Automotive Industry 4.0: Challenges, Opportunities, and Future Trends. In: *Intelligent Internet of Things for Healthcare and Industry*, 327–352.
37. Gołębiowska, A., Such-Pyrgiel, M., Prokopowicz, D., (2022). Post-pandemic reality and the security of ict, big data, industry 4.0, social media portals and the internet. *Journal of Modern Science*, 49(2).
38. Gunge, V.S., Yalagi, P.S., (2016). Smart home automation: a literature review. *International Journal of Computer Applications*, 975(8887–8891).
39. Gupta, S., Cherukuri, A.K., Subramanian, C.M., Ahmad, A., (2022). Comparison, analysis and analogy of biological and computer viruses. In: *Intelligent Interactive Multimedia Systems for e-Healthcare Applications*, 3–34.
40. Gómez, J.E., Marcillo, F.R., Triana, F.L., Gallo, V.T., Oviedo, B.W., Hernández, V.L., (2017). IoT for environmental variables in urban areas. *Procedia Computer Science*, 109, 67–74.
41. Herzberg, A., Kfir, Y., (2019). The leaky actuator: A provably-covert channel in cyber physical systems. In: *Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy,* pp. 87–98.
42. Hughes, L.E., (2022). The Depletion of the IPv4 Address Space. In: *Third Generation Internet Revealed: Reinventing Computer Networks with IPv6*, pp. 119–146.
43. Humaira, F., Islam, M.S., Luva, S.A., Rahman, M.B., (2020). A Secure Framework for IoT Smart Home by Resolving Session Hijacking. *Glob. J. Comput. Sci. Technol*, 20(2), 9–20.
44. Husamuddin, M., Qayyum, M., (2017). Internet of Things: A study on security and privacy threats. In: *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, pp. 93–97.
45. ISO 690.
46. ISO 690.
47. Jaakkola, H., Henno, J., Mäkelä, J., (2023). *Computers in Education*. doi: 10.23919/MIPRO57284.2023.10159980
48. Jakubczak, W., (2022). Globalna skala wykorzystania działań hybrydowych przez federację rosyjską. *Zeszyty Naukowe Pro Publico Bono*, 1 (1): 83–105. DOI: 10.5604/01.3001.0016.1962
49. Jhi, Y.C., Liu, P., Li, L., Gu, Q., Jing, J., Kesidis, G., (2010). PWC: A proactive worm containment solution for enterprise networks. *Security and Communication Networks*, 3(4), 334–354.
50. Khanboubi, F., Boulmakoul, A., Tabaa, M., (2019). Impact of digital trends using IoT on banking processes. *Procedia Computer Science*, 151, 77–84.
51. Kim, S., Park, J., Lee, K., You, I., Yim, K., (2012). A Brief Survey on Rootkit Techniques in Malicious Codes. *J. Internet Serv. Inf. Secur.*, 2(3/4), 134–147.
52. Krupanek, B., Bogacz, R., (2018). Węzły końcowe systemów Internetu Rzeczy. *Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej*, 59, 111–116.
53. Krysiński, M., (2016). Internet rzeczy – innowacyjne narzędzie dla firm. *Ekonomiczne Problemy Usług*, 122(1), 279–288.

54. Kumari, P., Jain, A.K., (2023). A comprehensive study of DDoS attacks over IoT network and their countermeasures. *Computers & Security*, 127, 103096.
55. Kuraś, P., Organiściak, P., Kowal, B., & Łukasik, E., (2023). Using machine learning techniques to reduce pairwise comparison matrix inconsistencies. In: Šperka, R., Suchánek, P., Duháček Šebestová, J., Dolák, R. et al. (eds.). *4th International conference on Decision making for Small and Medium-Sized Enterprises. Conference Proceedings*. Karviná: Silesian University in Opava, School of Business Administration in Karviná, pp. 122–131.
56. Kwiatkowska, E.M., (2016). Internet rzeczy. Czy będą nas leczyć komputery? *Internetowy Kwartalnik Antymonopolowy i Regulacyjny (iKAR)*, 5(6), 19–32.
57. Lee, W.S., Alchanatis, V., Yang, C., Hirafuji, M., Moshou, D., Li, C., (2010). Sensing technologies for precision specialty crop production. *Computers and electronics in agriculture*, 74(1), 2–33.
58. Li, S., Xu, L. D., Zhao, S. (2015). The internet of things: a survey. Information systems frontiers, 17, 243–259.
59. Liao, C.H., Shuai, H.H., Wang, L.C., (2018). Eavesdropping prevention for heterogeneous Internet of Things systems. In: *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1–2.
60. Lukiv, J., (2022). *Ukraine War: Power and water supply hit across Ukraine in "massive" Russian missile strikes*. https://www.bbc.com/news/world-europe-63454230.
61. Makhshari, A., Mesbah, A., (2021). IoT bugs and development challenges. In: *2021 IEEE/ACM 43rd International Conference on Software Engineering (ICSE)* (pp. 460–472).
62. Marzano, L., Hollis, C., Cipriani, A., Malhi, G.S., (2017). Digital technology: coming of age?. *Evidence-based Mental Health,* 20, 97. doi: 10.1136/EB-2017-102821
63. Matejkowski, D., Szmyd, P., (2023). Online identity theft detection and prevention methods. *Advances in Web Development Journal*, 1(1), 12.
64. Michael, M., (2019). *Attack Landscape H2 2018: Attack traffic increases fourfold - F-secure blog*, https://blog.f-secure.com/attack-landscape-h2-2018/.
65. Miller, C., (2008). Virtual worlds, real exploits. *Network Security*, 2008(4), 4–6.
66. Milosevic, J., Sklavos, N., Koutsikou, K., (2016). Malware in IoT software and hardware. In: *Workshop on Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE'16)*, Barcelona, Spain.
67. Mogili, UR., Deepak, BB.V.L., (2018). Review on application of drone systems in precision agriculture. *Procedia Computer Science*, 133, 502–509.
68. Moran, S., (2012). The basics of electric weapons and pulsed-power technologies. *Leading Edge*, 7(4), 50.
69. Mukhopadhyay, S.C., Suryadevara, N.K., (2014). *Internet of things: Challenges and opportunities*. Springer International Publishing, pp. 1–17.
70. Nagpal, B., Sharma, P., Chauhan, N., Panesar, A., (2015, March). DDoS tools: Classification, analysis and comparison. In: *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 342–346.

71. Nakalembe, C., Becker-Reshef, I., Bonifacio, R., Hu, G., Humber, M.L., Justice, C.J., ... & Sanchez, A., (2021). A review of satellite-based global agricultural monitoring systems available for Africa. *Global Food Security*, 29, 100543.
72. Oostenbrink, J., (2015). *Financial impact of downtime decrease and performance increase of IT services*. Bachelor's thesis. University of Twente.
73. Paidant. (2023). *The Tech Talent Shortage: Navigating the challenges and solutions*. https://www.linkedin.com/pulse/tech-talent-shortage-navigating-challenges-solutions-paidant/.
74. Pang, R., Yegneswaran, V., Barford, P., Paxson, V., Peterson, L., (2004). Characteristics of internet background radiation. In: *Proceedings of the 4th ACM SIGCOMM conference on Internet measurement*, pp. 27–40.
75. Parpala, R.C., Iacob, R., (2017). Application of IoT concept on predictive maintenance of industrial equipment. In: *MATEC Web of Conferences*, Vol. 121.
76. Pawłowicz, B., Salach, M., Trybus, B., (2019). Smart city traffic monitoring system based on 5G cellular network, RFID and machine learning. In: *Engineering Software Systems: Research and Praxis*, pp. 151–165.
77. Pawłowicz, B., Salach, M., Trybus, B., (2019, February). Infrastructure of RFID-based smart city traffic control system. In Conference on Automation. Cham: Springer International Publishing, pp. 186–198.
78. Petrosyan, A., (2023). *Malware: Most common attack types 2021*. https://www.statista.com/statistics/271037/distribution-of-most-common-malware-file-types/.
79. Pietrek, G.W., Skelnik, K., (2023). Cybersecurity and the scope of designing information security systems in the organization. *Journal of Modern Science*, 51(2), 141–173. https://doi.org/10.13166/jms/166583
80. Pratheesh Kumar, S., Dinesh, R., Raja, V., & Karthikeyan, S., (2022). Study and Development of Remote Control Appliances in DailyLife. In: *Materials, Design and Manufacturing for Sustainable Environment: Select Proceedings of ICMDMSE 2022*. Singapore: Springer Nature Singapore, pp. 205–219.
81. Protasowicki, I., (2018). Wpływ zagrożenia atakami DoS/DDoS na bezpieczeństwo teleinformatycznej infrastruktury krytycznej. *Modern Management Review*, vol. XXIII, 25 (1/2018), pp. 131–139.
82. Rad, B.B., Masrom, M., Ibrahim, S., (2012). Opcodes histogram for classifying metamorphic portable executables malware. In: *2012 International Conference on e-Learning and e-Technologies in Education (ICEEE)*, pp. 209–213.
83. Rathee, G., Garg, S., Kaddoum, G., Choi, B.J., (2020). Decision-making model for securing IoT devices in smart industries. *IEEE Transactions on Industrial Informatics*, 17(6), 4270–4278.
84. Rayes, A., Salam, S., (2022). The things in IoT: Sensors and actuators. In: *Internet of Things from Hype to Reality: The Road to Digitization*. Cham: Springer International Publishing, pp. 63–82.
85. Rosas, J.A.D., Brito, V., Brito Palma, L., Barata, J., (2017). Approach to adapt a legacy manufacturing system into the IoT paradigm. *International Journal of Interactive Mobile Technologies (iJIM)*, 11(5).

86. Rossow, C., Dietrich, C., Bos, H., (2013). Large-scale analysis of malware downloaders. In: Detection of Intrusions and Malware, and Vulnerability Assessment: *9th International Conference, DIMVA 2012*, Heraklion, Crete, Greece, July 26–27, 2012, Revised Selected Papers 9. Springer Berlin Heidelberg, pp. 42–61.
87. Rysz, S. J., (2020). Security of personal data. Part I – The specificity of determinants of personal identity in the 21st century. *Zeszyty Naukowe SGSP*, 75, 223–237.
88. Sanchez-Sutil, F., Cano-Ortega, A., (2021). Smart regulation and efficiency energy system for street lighting with LoRa LPWAN. *Sustainable Cities and Society*, 70, 102912.
89. Sangeethalakshmi, K., Preethi, U., Pavithra, S., (2023). Patient health monitoring system using IoT. *Materials Today: Proceedings*, 80, 2228–2231.
90. Serazzi, G., Zanero, S., (2003). Computer virus propagation models. In: *International Workshop on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 26-50.
91. Shen, W., Wu, Q., (2011). Exploring redundancy in sensor deployment to maximize network lifetime and coverage. In: *2011 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pp. 557–565.
92. Sim, G., (2018). Defending against the malware flood. *Network Security*, (5), 12–13.
93. Singh, A., Choudhary, P., (2021). Keylogger detection and prevention. *Journal of Physics: Conference Series*, Vol. 2007, No. 1, p. 012005).
94. Singh, R.K., Aernouts, M., De Meyer, M., Weyn, M., Berkvens, R., (2020). Leveraging LoRaWAN technology for precision agriculture in greenhouses. *Sensors*, 20(7), 1827.
95. Słota-Bohosiewicz, A., (2019). Wpływ Internetu rzeczy na bezpieczeństwo człowieka. *Journal of Modern Science*, 41(2), 189–208. https://doi.org/10.13166/jms/111177
96. Smith, A.D., (2004). Strategic leveraging of videoconferencing and web-enabled conferencing in an information-rich environment. *International Journal of Services and Standards*, 1(2), 206-227.
97. Smith, C., Matrawy, A., Chow, S., Abdelaziz, B., (2009). Computer worms: Architectures, evasion strategies, and detection mechanisms. *Journal of Information Assurance and Security*, 4, 69–83.
98. Song, J., Shimamura, J., Eto, M., Inoue, D., Nakao, K., (2011). Correlation analysis between spamming botnets and malware infected hosts. In: *2011 IEEE/IPSJ International Symposium on Applications and the Internet*, pp. 372–375.
99. Stoll, M., Breu, R., (2012). Information security measurement roles and responsibilities. In: *Emerging trends in computing, informatics, systems sciences, and engineering*. New York: Springer New York, pp. 11–23.
100. Stočes, M., Vaněk, J., Masner, J., Pavlík, J., (2016). Internet of things (IoT) in agriculture-selected aspects. *Agris on-line Papers in Economics and Informatics*, 8(1), 83–88.
101. Strzałka, D., Gerka, A., Kowal, B., Kuraś, P., Leopold, G., Lewicz, M., Jaworski, D., (2021), The Support System for Anomaly Detection with Application in Mainframe Management Process. *Modern Management Based on Big Data II and Machine Learning and Intelligent Sys[tems III: Proceedings of MMBD 2021 and MLIS 2021*, 341, 96.
102. Synowiec, A., (2019). Wykorzystanie Internetu rzeczy w zarządzaniu inteligentnym miastem. *Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie*, 34, 155–166.

103. Szabłowski, S., (2023). Aspekty dydaktyczne internetu rzeczy. *Dydaktyka Informatyki*, vol.. 18 (2023), pp. 176–184.
104. Szappanos, G., (2002). Are there any polymorphic macro viruses at all? (… and what to do with them). In: *Proceedings of the 12th International Virus Bulletin Conference*.
105. Szozda, N., (2017). Znaczenie Internetu rzeczy w planowaniu przepływów produktów i informacji w łańcuchu dostaw. *Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach*, (315).
106. Szubrycht, T., Szymański, T., (2005). Broń elektromagnetyczna jako nowy środek walki w erze informacyjnej. *Zeszyty Naukowe Akademii Marynarki Wojennej*, 46,3 (162), 121–134.
107. Szykuła-Piec, B., Piec, R., (2020). Costs of Security Understood as a Service Product Abstract. *Zeszyty Naukowe SGSP*, Special Issue (1), 159–170.
108. Świętochowski, N., (2018). The History and Use of Electromagnetic Weapons. *Historia i Polityka*, 33(26), 123–136.
109. Takiddeen, N., & Zualkernan, I., (2019, June). Smartwatches as IoT edge devices: A framework and survey. In: *2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC)*, pp. 216–222.
110. Tchuitcheu, W.C., Bobda, C., Pantho, M.J.H., (2020). Internet of smart-cameras for traffic lights optimization in smart cities. *Internet of Things*, 11, 100207.
111. Thakur, K., Ali, M.L., Jiang, N., Qiu, M., (2016). Impact of cyber-attacks on critical infrastructure. In: *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, pp. 183–186.
112. Tudosi, A.D., Graur, A., Balan, D.G., Potorac, A.D., (2023). Research on Security Weakness Using Penetration Testing in a Distributed Firewall. *Sensors*, 23(5), 2683.
113. Umair, M., Cheema, M.A., Cheema, O., Li, H., Lu, H., (2021). Impact of COVID-19 on IoT adoption in healthcare, smart homes, smart buildings, smart cities, transportation and industrial IoT. *Sensors*, 21(11), 3838.
114. Walczak, D., Wrzos, M., Radziuk, A., Lewandowski, B., Mazurek, C., (2012). Machine-to-Machine communication and data processing approach in Future Internet applications. In: *2012 8th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP)*, pp. 1–5.
115. Wangen, G., (2015). The role of malware in reported cyber espionage: a review of the impact and mechanism. *Information*, 6(2), 183–211.
116. Wiercioch, K., (2022). *Wojna informacyjna jako element wojny hybrydowej*. Bachelor thesis: Cracow: Jagiellonian University.
117. Wojciechowska, K., (2022). *Jak wygląda internet po 30 Latach w Polsce?* https://isportal.pl/jak-wyglada-internet-po-30-latach-w-polsce/.
118. Yu, D., Zhang, L., Chen, Y., Ma, Y., Chen, J., (2020). Large-scale IoT devices firmware identification based on weak password. *IEEE Access*, 8, 7981–7992.

119. Zaddach, J., Kurmus, A., Balzarotti, D., Blass, E.O., Francillon, A., Goodspeed, T., ... & Koltsidas, I., (2013). Implementation and implications of a stealth hard-drive backdoor. In: *Proceedings of the 29th annual computer security applications conference*, pp. 279–288.

120. Zhang, Y., & Paxson, V., (2000). Detecting backdoors. In: *9th USENIX Security Symposium (USENIX Security 00)*.

121. Zhang, Y., Chen, Q., Liu, G., Shen, W., Wang, G., (2016). Environment parameters control based on wireless sensor network in livestock buildings. *International Journal of Distributed Sensor Networks*, 12(5), 9079748.

122. Zhu, B., Joseph, A., & Sastry, S., (2011). A taxonomy of cyber attacks on SCADA systems. In: *2011 International conference on internet of things and 4th international conference on cyber, physical and social computing*, pp. 380–388.

123. Zieliński, A., (2018). Cyberbezpieczeństwo-problem globalny. *Przegląd Telekomunikacyjny – Wiadomości Telekomunikacyjne*, 10, 864–869.

124. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H.N., (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1), 82–97.