Interdisciplinary Description of Complex Systems 23(3), 240-249, 2025

CHALLENGES IN RESPONDING TO RANSOMWARE INCIDENTS IN CLOUD CONNECTED IOT ENVIRONMENTS

Dávid János Fehér*

Óbuda University, Doctoral School on Safety and Security Science
Budapest, Hungary

DOI: 10.7906/indecs.23.3.5
Regular article

Received: 20 February 2024.
Accepted: 1 July 2024.

ABSTRACT

The rise of IoT technologies has exponentially increased the return on investment from the ransomware threat vector side. This study addresses the cybersecurity challenges in reacting to security incidents of complex cloud connected IoT solutions, mainly focusing on ransomware incidents. It highlights the diverse and interconnected nature of IoT systems, which creates a complex landscape of attack surfaces for ransomware. The centralization of risks exacerbates these challenges due to cloud or multi-cloud integration, necessitating robust security measures and comprehensive incident response strategies. The need for holistic security approaches, encompassing endpoint, network, and multi-cloud defenses, to mitigate ransomware risks effectively is rising, and the complexities of incident response in such integrated systems are more emphasized, focusing on the coordination required across various stakeholders for effective management and recovery. The study advocates for adaptive, layered security solutions and a nuanced understanding of the interconnected technological landscape to enhance resilience against ransomware threats in cloud-connected IoT environments.

KEY WORDS

ransomware, cybersecurity, incident response, cloud, IoT

CLASSIFICATION

ACM: C.2.1, C.2.3, H.1.1, H.5.1, H.5.3

JEL: L86

*Corresponding author, η: david.janos.feher@gmail.com; -;
Népszínház street 8, Budapest, 1081, Hungary

INTRODUCTION

Automating cloud incident response for business continuity and recovery post-ransomware attacks, especially in cloud connected IoT environments, is critical for rapidly mitigating operational disruptions and safety risks in real-time operational systems. Rapid and effective incident response is essential in industries where continuity is paramount. Security best practices and recommendations emphasize the importance of proactive security measures, including anticipatory security and security by design, in combating the evolving nature of ransomware threats. Due to ransomware attacks, insurance or legal involvement often becomes critical as organizations aim to recuperate losses and manage potential liabilities. These cyber incidents typically result in operational disruptions and substantial financial consequences. Engaging in the insurance and legal dimensions involves navigating complex claims processes, scrutinizing policy coverage, and addressing legal issues arising from data breaches or non-compliance with regulations [1-12].

EMERGING TECHNOLOGIES FOLLOWED BY THREATS

The chart in Figure 1 analyzes Google search trends, highlighting the growing global interest regarding ransomware, specifically variants such as Wannacry. The trendlines reveal a significant rise in ransomware searches, simultaneously, the ascending trajectory of IoT-related searches reflects its expanding usage. This parallel increase suggests an evolving landscape where the proliferation of IoT systems will be likely to become increasingly attractive targets for ransomware threat actors, posing new challenges in cybersecurity and system resilience. According to the presented chart, the WannaCry ransomware incident stands out as the most notable in terms of public awareness and search trends. This ransomware achieved unprecedented notoriety, due to its targets and victims [13]. In contrast, ransomware, such as Ryuk, despite its significant impact on Windows servers, faces challenges in recognition and identification within search trend analysis. This ambiguity arises partly because ‘Ryuk’ shares its name with a character from a popular anime series, complicating the attribution of search trends specifically to the ransomware [14]. The chart also shows trendlines for ransomware and IoT, and it has been observed that a majority of ransomware attacks predominantly target Windows-based devices [15]. This can be attributed to the widespread usage of Windows among general users and the specific vulnerabilities within the Windows operating system that have been exploited by various ransomware attacks [16]. The intersection of increasing IoT usage and the prevalence of ransomware targeting Windows systems highlights an evolving cybersecurity landscape, where the proliferation of connected devices could potentially lead to new vulnerabilities and attacks [17].

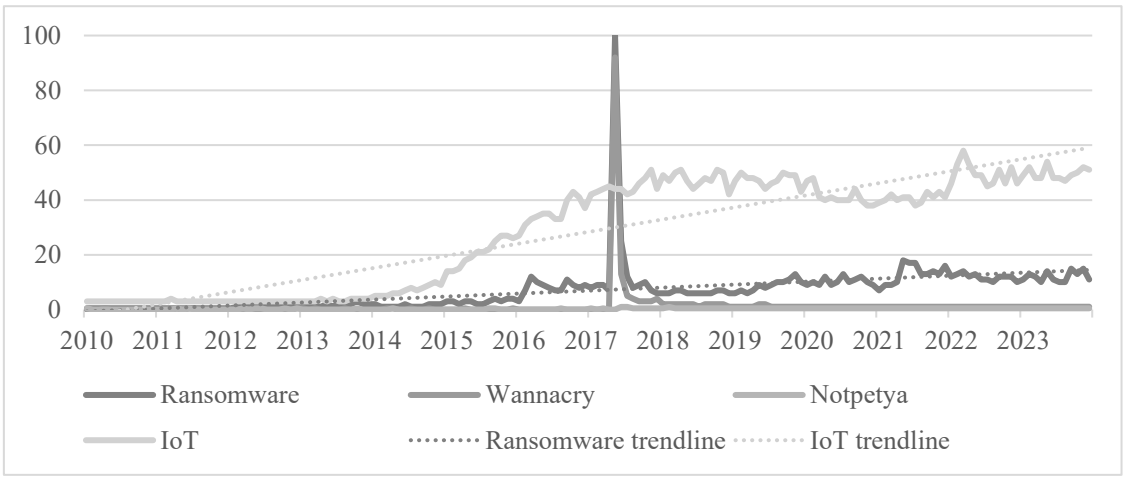

Figure 1. Google Search Trends of Ransomware related words and IoT search word [18].

There is a noticeable trend of declining Windows hosts as various alternative systems gain prominence due to the increasing adoption of Android, Linux, cloud-based platforms, IoT systems, and Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) offerings [19, 20]. Concurrent with this diversification is the exponential growth in data generation and accumulation. This escalation in data volume inherently enhances the value of these systems as targets for cyber threats, including ransomware and data breaches, making robust cybersecurity measures more crucial than ever [21]. As these emerging technologies continue to evolve and store larger quantities of sensitive data, they represent increasingly attractive targets for malicious actors, underscoring the need for enhanced security protocols and vigilant monitoring of these varied and expanding digital environments.

In the current economic climate, organizations are increasingly prioritizing cost efficiency and exploring avenues for expense reduction [22]. This trend is particularly evident in adopting the IoT and Industry 4.0 solutions, which enable companies to leverage data-driven insights for cost optimization [23]. These technological solutions facilitate the collection of extensive data sets, providing detailed insights into various aspects of business operations and thereby identifying potential areas for cost savings [24]. However, this expansion in data collection and the consequent increase in data storage and processing systems introduce new vulnerabilities. As organizations amass more significant quantities of data and develop more complex systems to manage and analyze this information, they inadvertently create additional targets for cyber threats, particularly ransomware attacks. The proliferation of data repositories and the complexity of the systems required to handle them exponentially increase the potential attack surfaces for malicious actors [21]. Furthermore, integrating IoT devices in business processes, while beneficial for operational efficiency, also contributes to the expanded threat landscape. These devices can lack robust security measures, making them susceptible to exploitation by ransomware attackers seeking to infiltrate broader network systems [25, 26].

Thus, while IoT technologies offer significant cost optimization and operational efficiency advantages, they also necessitate a more comprehensive approach to cybersecurity. Businesses must balance the benefits of data-driven decision-making with the increased risk of cyber threats, ensuring adequate protection measures are in place to safeguard their expanding digital infrastructure.

IOT ATTACK SURFACES

Integrating IoT technologies with cloud computing exponentially expands and diversifies potential attack surfaces [5]. This proliferation of connected devices, each a potential vector for intrusion, presents a significant challenge in securing systems against ransomware. Despite the concerted efforts by vendors, implementers, and operation teams to ensure secure environments, the commitment to security often encompasses a limited timeframe and limited available resources to resolve these issues. This is reflected in the Service Level Agreements (SLAs) that specify windows for addressing vulnerabilities and specific aspects to prioritize vulnerabilities based on their estimated criticality [27]. While structured to mandate timely responses, these SLAs do not guarantee the resolution of all security issues, the responsibility for updating and patching applications, a crucial aspect of maintaining security, typically fails on improper vulnerability and patch management procedures, and due to the required change windows in production environments [28].

Many IoT protocols utilize IPv4, while more recent executions use IPv6 [29], aligning their operational frameworks closely with conventional information technology (IT) systems. This IP-based orientation signifies that these solutions function similarly to a broad spectrum of IT solutions, utilizing standardized communication protocols for data transmission and networking [28]. Furthermore, IoT systems do not usually exist in isolation; instead, they are integral components of a larger, more intricate architectural landscape, which strongly rely on

IP. This landscape encompasses a diverse array of solutions, services, and platforms, each contributing to the overall functionality and efficiency of the system [30]. This integration results in complex, multi-layered structures where various elements, such as cloud computing platforms, firewalls, virtual machines, databases, data analytics tools, and various software and hardware components, interplay to facilitate advanced industrial and consumer applications. Ensuring seamless integration and communication across various components while maintaining robust security protocols is essential in these interconnected environments, and the scalability of these systems must be addressed to accommodate the ever-increasing number of connected devices and the corresponding data volume [30, 31].

Message Queuing Telemetry Transport (MQTT) is a lightweight and simple messaging protocol used by IoT systems [1]. As part of this protocol, the publish/subscribe pattern is in use to decouple the message receiver from the message sender, so the communication participants are not aware of each other's IPs and protocols, but they still have IP addresses. MQTT with TLS can solve data in transit issues, if it is properly implemented during the whole traffic end to end, as shown in Figure 2. Google Cloud supports MQTT over TLS in the Google Cloud Platform ecosystem with dedicated MQTT Pub/Sub connectors [33, 34].

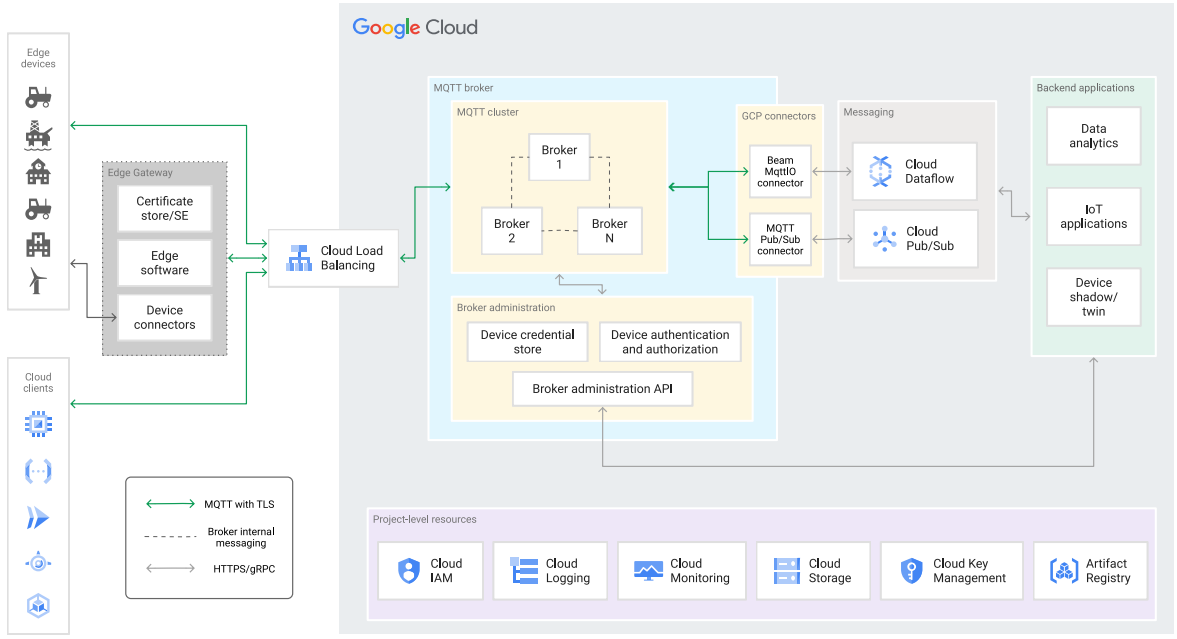

Figure 2. Standalone MQTT broker architecture on Google Cloud [33].

The integration with cloud computing introduces additional layers of complexity and risk. Cloud platforms, while offering scalability and efficiency, can become centralized points of vulnerability in the event of a ransomware attack. A successful breach of cloud infrastructure can have far-reaching consequences, affecting all connected devices and systems. This risk necessitates implementing robust cloud security measures, including data encryption, access control, and regular security assessments. As cloud environments become increasingly integral to IoT ecosystems, ensuring their security becomes mandatory in preventing and mitigating ransomware attacks. Meanwhile proper segregation and zero-trust will be required as the improvements in computing powers will pose new challenges to encryption in the future [5, 35, 36].

The heterogeneity of these devices, coupled with their varying degrees of security robustness, creates a patchwork of potential vulnerabilities. The interconnectivity inherent in IoT systems magnifies the number of attack vectors, and in special cases this interconnectedness means that the compromise of a single device can lead to a domino effect, where the breach can propagate across the network, potentially reaching cloud-based systems [1]. This interconnected nature

requires a shift from a traditional perimeter-based security approach to a more holistic, layered defense strategy with multiple guardrails, and countermeasures in place, from physical level to application level. It should also include proactive monitoring and real-time threat detection and response mechanisms to quickly identify and mitigate potential ransomware attacks before they spread through the network and cause significant damage [5, 25].

Given the varied nature of devices and systems, a one-size-fits-all baseline approach to security could be more effective, but specific customized security measures tailored to each device or system-specific characteristics and vulnerabilities can help to protect against ransomware. The dynamic nature of IoT environments, where devices are continually added, removed, or updated, calls for continuous monitoring for new vulnerabilities, regular updates and preparedness to respond to emerging threats swiftly.

INCIDENT RESPONSE COMPLEXITIES

The intricate nature of integrated systems, characteristic of modern technological environments, introduces significant complications in identifying and swiftly responding to ransomware incidents [37].

A comprehensive approach to incident response in these scenarios is well encapsulated by the National Institute of Standards and Technology (NIST) Special Publication 800-61, which outlines the Incident Response Lifecycle [38]. This framework provides a structured methodology for managing and responding to cybersecurity incidents. As shown in Figure 3, it contains phases such as preparation, detection and analysis, containment, eradication and recovery.

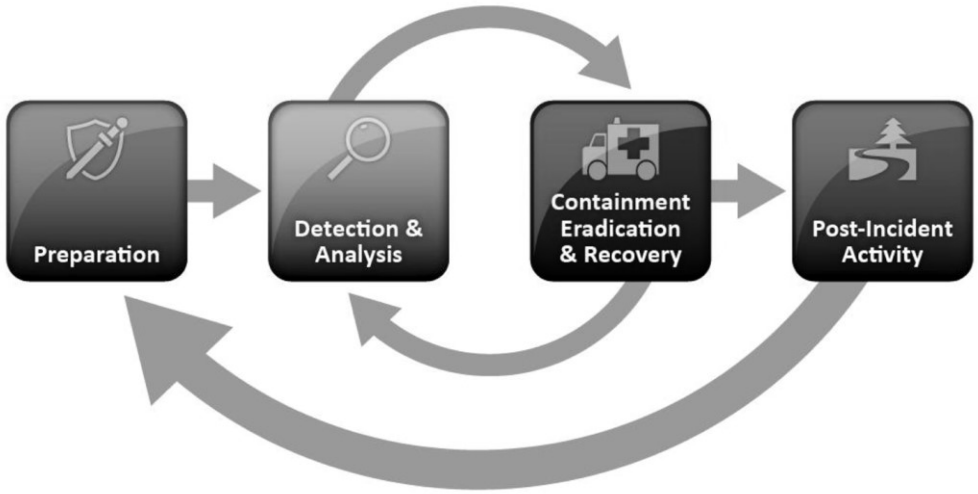

Figure 3. Incident Response Lifecycle, NIST SP 800-61 [38].

Identification, Assessment, and Integration Challenges

In cyber incident response, one of the primary obstacles faced is the precise detection and evaluation of a ransomware intrusion within the diverse ecosystems of IoT, where the plethora of devices and their extensive deployment can obscure the immediacy and origin of an attack. Addressing these challenges necessitates implementing a sophisticated and well-tailored asset management process and properly configured logging and monitoring in place with advanced analytical instruments, as well as the expertise of seasoned cybersecurity professionals who can interpret and respond to the nuances of network traffic and behavior patterns. Due to the diverse log sources, handling the proper logs without creating too much noise and unnecessary cost is a great challenge, but even if the logs are properly handled, the created false positives can be a burden for the analysis teams. Properly implemented and used machine learning and

artificial intelligence-supported solutions can provide great advances for better alerting and incident response. In cloud environments without proper FinOps practices, log ingestion, log stores with locked retention periods, and SIEM and SOAR solutions with pay-as-you-go pricing can cause significant cost implications. The key is proper discovery, integration, and proper guardrails from all perspectives [8, 10, 25, 39, 40]. Responding to incidents can be complex with critical IoT systems, as shutting down critical IoT systems for false positives would cause more harm than good, for example in critical manufacturing systems or in critical smart city or smart building elements, where the human factor is already there as a source of anomaly [41-44].

Cross-functional Teams

Effective incident response in cloud connected IoT environments requires the collaboration of cross-functional teams, which connects different teams with cybersecurity experts, information technology professionals, and operational technology specialists. Integrating diverse expertise enables a holistic approach to incident management, ensuring that each facet of the response is informed by specialized knowledge. Cybersecurity experts contribute their acumen in threat analysis and mitigation, IT professionals offer insights into the network architecture and data flow, and operational technology specialists provide an understanding of the control systems and their integration with business operations. Collectively, these professionals orchestrate a synergistic response that addresses an incident's technical and operational ramifications, thereby fortifying the resilience of the organizational cyber-physical landscape [9, 37, 45].

Restoration and Recovery Processes

In the aftermath of cybersecurity breaches, restoring and rehabilitating compromised systems becomes paramount, especially within the highly integrated domains of business-critical IoT systems. Recovery processes in such complex landscapes necessitate meticulous strategizing to circumvent further perturbations, with consideration for systems underpinning operational technology, where the cost of downtime and penalties of SLAs escalate quickly. A methodical, phased approach is often employed to reinstate critical systems with minimal operational interruption. This strategy underscores the significance of maintaining data integrity and implementing effective backup solutions or resilient system architectures with immutable storage at the required places. The most important part is to define the proper recovery time objective (RTO) and recovery point objective (RPO) for these systems and create the restoration and business continuity plans accordingly, as keeping up extra backups and extra fast recovery systems is expensive [9, 37, 45, 46].

Coordination and Communication in Response Efforts

Once the ransomware hits, the clock starts ticking, and the race against time begins. The interconnected nature of IoT environments means that ransomware can proliferate beyond a singular point of compromise, potentially cascading through numerous connected nodes and different types of servers in a network, which are managed by different teams and departments. The lack of efficient communication can have a high cost, thereby necessitating a synergistic and well-orchestrated response effort. The NIST Special Publication 800-61 advocates proper incident response flows and coordinators to be in place. This response calls for a concerted approach among a spectrum of stakeholders – IT professionals, cloud service providers, IoT-specific subject matter experts, and operational technology teams with the involvement of dedicated coordinator teams. Well-documented communication pathways and well-conceived incident response protocols are indispensable. These protocols and runbooks should delineate explicit roles and responsibilities, assuring that all entities can act promptly and synchronized according to a consolidated response plan [9, 37, 45].

Training and Preparedness

Regular training and preparedness exercises are essential to ensure that all team members understand their roles and responsibilities in the event of a ransomware attack. This includes technical response strategies, crisis management, and decision-making processes. Regular instructional and simulation exercises are indispensable in equipping team members with the requisite knowledge and competencies to navigate the multifaceted challenges of ransomware attacks. These educational endeavors extend beyond the mere impartation of technical response tactics; they encompass the broader gamut of crisis management, including the cultivation of decision-making acumen under duress. Through such comprehensive training programs, personnel across various functional roles are schooled in the nuances of their specific duties during a cybersecurity incident, fostering a state of readiness that transcends routine operations [9, 37, 45].

Big picture

As Figure 4 illustrates, incident response is a huge ever-changing picture with recurring steps for polishing its processes to make it better, faster, and more resilient, and to decrease the resolution time and the damage caused by an incident. Having a comprehensive view is key for proper incident response, so this chapter gives a bird's eye view of incident response steps and the mutual influence between them.

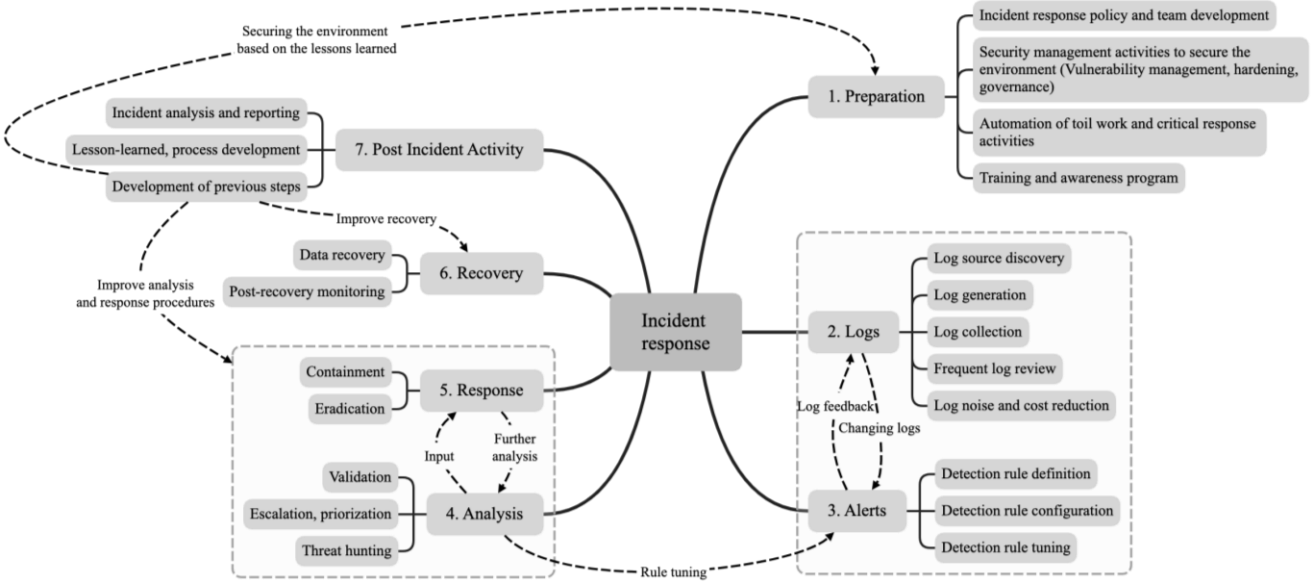

Figure 4. Incident response steps with highlighted mutual influence between them.

Effective response to ransomware in cloud-connected IoT environments demands a proactive, comprehensive, and collaborative approach [9, 37, 38, 45].

CONCLUSION

In conclusion, this article highlights the criticality of a robust incident response strategy for ransomware attacks in cloud-connected IoT environments. It emphasizes the growing complexity of these environments and the escalating risks posed by sophisticated cyber threats. The discussion underscores the necessity of integrating advanced security measures, cross-functional teamwork, and continuous training within these ecosystems. Effective response and recovery strategies must be adaptable, encompassing both technical and operational aspects. A resilient and comprehensive approach is key to safeguard against and mitigate the impacts of ransomware in an increasingly interconnected digital world.

REFERENCES

[1] Yaqoob, I., et al.: *The rise of ransomware and emerging security challenges in the Internet of Things*.
Computer Networks **129**(Part 2), 444-458, 2017,
http://dx.doi.org/10.1016/j.comnet.2017.09.003,

[2] Al-Hawawreh, M., et al.: *Targeted Ransomware: A New Cyber Threat to Edge System of Brownfield Industrial Internet of Things*.
IEEE Internet Things Journal **6**(4), 7137-7151, 2019,
http://dx.doi.org/10.1109/JIOT.2019.2914390,

[3] Axon, L., et al.: *Ransomware as a Predator: Modelling the Systemic Risk to Prey*.
Digital Threats: Research and Practice **4**(4), 1-38, 2023,
http://dx.doi.org/10.1145/3579648,

[4] Mthunzi, S.N.; Benkhelifa, E.; Bosakowski, T.; Ghedira Guegan, C. and Barhamgi, M.: *Cloud computing security taxonomy: From an atomistic to a holistic view*.
Future Generation Computer Systems **107**, 620-644, 2020,
http://dx.doi.org/10.1016/j.future.2019.11.013,

[5] Surya, L.: *Security challenges and strategies for the IoT in cloud computing*.
International Journal of Innovations in Engineering Research and Technology **3**(9), 2394-3696, 2016,

[6] Zahra, S.R. and Chishti, M.A.: *Ransomware and internet of things: A new security nightmare*.
9th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE, Noida, 2019,
http://dx.doi.org/10.1109/CONFLUENCE.2019.8776926,

[7] Snedaker, S.: *Business Continuity and Disaster Recovery Planning for IT Professionals*.
Elsevier Science, 2007,
http://dx.doi.org/10.1016/B978-1-59749-172-3.X5000-2,

[8] Cook, A.; Maglaras, L.; Smith, R. and Janicke, H.: *Managing incident response in the industrial internet of things*.
International Journal of Internet Technology and Secured Transactions **8**(2), 251-276, 2018,
http://dx.doi.org/10.1504/IJITST.2018.093336,

[9] Thompson, E.C.: *Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents*.
Apress, New York, 2018,
http://dx.doi.org/10.1007/978-1-4842-3870-7,

[10] Enciso Bernal, A.; Martínez Monterrubio, S.M.; Parra Fuente, J.; González Crespo, R. and Verdú, E.: *Methodology for computer security incident response teams into IoT strategy*.
KSII Transactions on Internet and Information Systems **15**(5), 1909-1928, 2021,
http://dx.doi.org/10.3837/tiis.2021.05.018,

[11] Sándor, B. and Rajnai, Z.: *Cyber Security Analysis of Smart Buildings from a Cyber Security Architecture Point of View*.
Interdisciplinary Description of Complex Systems 21(2), 141-147, 2023,
http://dx.doi.org/10.7906/indecs.21.2.2,

[12] Albini, A. and Rajnai, Z.: *General architecture of cloud*.
Procedia Manufactruring **22**, 485-490, 2018,
http://dx.doi.org/10.1016/j.promfg.2018.03.074,

[13] Ghafur, S., et al.: *A retrospective impact analysis of the WannaCry cyberattack on the NHS*.
NPJ Digital Medicine **2**, No. 98, 2019,
http://dx.doi.org/10.1038/s41746-019-0161-6,

[14] Goettl, C.: *Is ransomware winning?*
Cyber Security: A Peer-Reviewed Journal **5**(1), 51-65, 2021,
http://dx.doi.org/10.69554/ICWU7894,

[15] Bansal Urvashi, E.: *A review on ransomware attack*.
2nd International Conference on Secure Cyber Computing and Communications. IEEE, Jalandhar, 2021,
http://dx.doi.org/10.1109/ICSCCC51823.2021.9478148,

[16] StatCounter Glob Stats: *Operating System Market Share Worldwide*.
https://gs.statcounter.com/os-market-share, accessed 20th January 2024,
[17] Razaulla, S., et al.: *The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions*.
IEEE Access **11**, 40698-40723, 2023,
http://dx.doi.org/10.1109/ACCESS.2023.3268535,
[18] Google: *Google Trends*.
https://trends.google.com/trends/explore?date=all&q=Wannacry,notpetya,ransomware,iot&hl=hu, accessed 21st January 2024,
[19] StatCounter Glob Stats: *Operating System Market Share Worldwide*.
https://gs.statcounter.com/os-market-share, accessed 20th January 2024,
[20] Fehér, D.J. and Sándor, B.: *Cloud SaaS Security Issues and Challenges*.
13th International Symposium on Applied Computational Intelligence and Informatics. IEEE, Timisoara, 2020,
http://dx.doi.org/10.1109/SACI46893.2019.9111529,
[21] Fadziso, T.; Thaduri, U.R.; Dekkati, S.; Ballamudi, V.K.R. and Desamsetti, H.: *Evolution of the cyber security threat: an overview of the scale of cyber threat*.
Digitalization & Sustainability Review **3**(1), 1-12, 2023,
[22] Odintsov, S.D.; Oikonomou, V.K.; Giannakoudi, I.; Fronimos, F.P. and Lymperiadou, E.C.: *Recent Advances in Inflation*.
Symmetry **15**(9), No. 1701, 2023,
http://dx.doi.org/10.3390/sym15091701,
[23] Tomazzoli, C.; Scannapieco, S. and Cristani, M.: *Internet of things and artificial intelligence enable energy efficiency*.
Journal of Ambient Intelligence and Humanized Computing **14**, 4933-4954, 2023,
http://dx.doi.org/10.1007/s12652-020-02151-3,
[24] Isazadeh, A.; Ziviani, D. and Claridge, D.E.: *Global trends, performance metrics, and energy reduction measures in datacom facilities*.
Renewable and Sustainable Energy Reviews **174**, No. 113149, 2023,
http://dx.doi.org/10.1016/j.rser.2023.113149,
[25] Humayun, M.; Jhanjhi, N.Z.; Alsayat, A. and Ponnusamy, V.: *Internet of things and ransomware: Evolution, mitigation and prevention*.
Egyptian Informatics Journal **22**(1), 105-117, 2021,
http://dx.doi.org/10.1016/j.eij.2020.05.003,
[26] Sándor, B. and Rajnai, Z.: *Evaluating the Interoperability of IoT devices and Cloud Environments in Intelligent Building Systems*. In Hungarian.
Biztonságtudományi Szemle **5**(3), 47-61, 2023,
[27] Chan, C.K.; Chandrashekhar, U.; Richman, S.H. and Vasireddy, S.R.: *The role of SLAs in reducing vulnerabilities and recovering from disasters*.
Bell Labs Technical Journal **9**(2), 189-203, 2024,
http://dx.doi.org/10.1002/bltj.20035,
[28] Cybellium: *Mastering Patch Management*.
Cybellium Ltd, 2023,
[29] Microsoft: *IoT Technologies and Protocols, Azure*.
https://azure.microsoft.com/en-us/solutions/iot/iot-technology-protocols, accessed 20th January 2024,
[30] Lea, P.: *Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security*.
Packt Publishing, 2018,
[31] Szikora, P.: *The Role of the Tools and Methods of Implementation in Information System Efficiency*.
Association of Educational Sciences, Budapest, 2009,
[32] –: *What is MQTT? - MQTT Protocol Explained - AWS*.
https://aws.amazon.com/what-is/mqtt, accessed 20th January 2024,

[33] –: *Standalone MQTT broker architecture on Google Cloud*. https://cloud.google.com/architecture/connected-devices/mqtt-broker-architecture, accessed 21st January, 2024,
[34] –: *MQTT to Pub/Sub template*. https://cloud.google.com/dataflow/docs/guides/templates/provided/mqtt-to-pubsub, accessed 21st January2024,
[35] Rubóczki, E. and Rajnai, Z.: *Moving towards cloud security*. Interdisciplinary Description of Complex Systems **13**(1), 9-14, 2015, http://dx.doi.org/10.7906/indecs.13.1.2,
[36] Szikora, P. and Lazányi, K.: *The end of encryption? The era of quantum computers*. In.: Kovács, T.A.; Nyikes, Z. and Fürstner, I., eds.: Security-Related Advanced Technologies in Critical Infrastructure Protection. NATO Science for Peace and Security Series C: Environmental Security. Springer, Dordrecht, pp.61-72, 2022, http://dx.doi.org/10.1007/978-94-024-2174-3_5,
[37] Ozer, M., et al.: *Cloud incident response: Challenges and opportunities*. International Conference on Computational Science and Computational Intelligence. IEEE, Las Vegas, 2020, http://dx.doi.org/10.1109/CSCI51800.2020.00015,
[38] Cichonski, P.; Millar, T.; Grance, T. and Scarfone, K.: *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*. http://dx.doi.org/10.6028/NIST.SP.800-61r2,
[39] Itodo, C.; Varlioglu, S. and Elsayed, N.: *Digital forensics and incident response (DFIR) challenges in IoT platforms*. 4th International Conference on Information and Computer Technologies. IEEE, Hawaii, pp.199-203, 2021, http://dx.doi.org/10.1109/ICICT52872.2021.00040,
[40] Storment, J.R. and Fuller, M.: *Cloud FinOps*. O'Reilly Media, Newton, 2023,
[41] Pető, R.: *Security of Smart City*. Interdisciplinary Description of Complex Systems **17**(1-A), 13-19, 2019, http://dx.doi.org/10.7906/indecs.17.1.3,
[42] Lazányi, K. and Danaj, A.: *Critical Threat of Critical Infrastructures: The Human Factor*. In.: Kovács, T.A.; Nyikes, Z. and Fürstner, I., eds.: Security-Related Advanced Technologies in Critical Infrastructure Protection. NATO Science for Peace and Security Series C: Environmental Security. Springer, Dordrecht, pp.1-11, 2022, http://dx.doi.org/10.1007/978-94-024-2174-3_1,
[43] Bederna, Z.; Rajnai, Z. and Szadeczky, T.: *Business strategy analysis of cybersecurity incidents*. Land Forces Academy Review **26**(2), 139-148, 2021, http://dx.doi.org/10.2478/raft-2021-0020,
[44] Sándor, B. and Rajnai, Z.: *Smart Buildings and IoT: A Comprehensive Review of Global Practices*. In Hungarian. Biztonságtudományi Szemle **5**(2), 33-46, 2023,
[45] Ozkaya, E.: *Incident Response in the Age of Cloud: Techniques and best practices to effectively respond to cybersecurity incidents*. Packt Publishing Ltd., 2021,
[46] Petrenko, S.: *Developing an Enterprise Continuity Program*. River Publishers; 2021, http://dx.doi.org/10.1201/9781003337881.