Journal of Intelligent System and Applied Data Science (JISADS)

Journal homepage : https://www.jisads.com

ISSN (2974-9840) Online

THE ROLE OF DEPENDABILITY IN IOT SYSTEMS

Mohammad Ibraigheeth[1*]

[1]*Department of Software Engineering, Bethlehem University, Bethlehem, Palestine, mayyash2010@gmail.com*

ABSTRACT

The advances in the Internet of Things (IoT) have contributed to the automation of various industries by enabling devices and systems to effectively connect and collect data remotely over the internet. This progress has led to the creation of an intelligent society where physical things are becoming increasingly innovative and undoubtedly, the IoT systems will continue to impact real life by providing efficient data collection and sharing. The successful implementation of IoT systems relies on their dependability, which is closely tied to several factors such as their reliability, resilience, and security. This paper explores the crucial role of dependability in IoT system, emphasizing challenges such as real-time analysis, resource constrains, connection redundancy, and quick fault recovery. The paper also provides some strategies for overcoming dependability challenges, such as efficient algorithms, edge computing, prioritization of resources, and AI techniques integration. Additionally, the paper presents a case study of an IoT system that faced dependability problems, highlighting the importance of rigorous testing and redundancy in ensuring reliable IoT deployments. As a result of this research, we suggest that by addressing the challenges related to dependability aspects, stakeholders can unlock the full potential of IoT, empowering industries and individuals with transformative, efficient, and reliable technologies. For future work, a frame work for evaluating and enhancing the IoT dependability will be developed. Several factors will be considered in developing this framework, such as reliability, availability, safety, security, resilience, and fault management. The framework will define a quantifiable metrics to measure these factors.

Keywords: internet of things (IoT), dependability, reliability, resource constrains, failure recovery.

1. INTRODUCTION

Nowadays, the rapid advancement of smart sensor applications enables objects or things in various fields of our life to be addressed, connected, and to collect data about the environment around them. In this context, the "Internet of Things" (IoT) is a paradigm that emerged to manage and organize practical and technical issues [1]. Therefore, IoT deals with different technologies and protocols, such as Internet, mobile communication, and wireless sensor protocols [2]. The evolution of IoT has led to use this paradigm by different applications such as smart home, smart payment, smart lighting, fire detection, monitoring safety, and many other fields [3]. Central to the successful implementation and widespread adoption of IoT systems is the concept of dependability [4].

Dependability in general is a combination of several attributes such as reliability, availability, security, confidentiality, and resilience. Having these attributes enables a user to put trust into and rely on a system [5]. The dependability of an IoT device refers to ability of this device to consistently deliver trusted, accurate and reliable data, while maintaining the integrity and security of data in the face of various challenges and uncertainties. In IoT, dealing with vulnerabilities of a huge number of

heterogeneous devices is a challenge [6,7]. Enhancing dependability enables IoT system to handle several challenges.

A way to realize dependability requirements in IoT systems is by using fog computing [8,9]. Fog computing enables real-time data processing and analysis at the edge [10], which mean that the massive volume of data generated by IoT devices can be processed and analyzed locally and closer to the source of this data (network edges) rather than sending data to centralized cloud or data center. This reduces the data transmission and allows faster decision-making at the edge, enhancing the overall performance of IoT system [11]. Fog computing provides a platform that supports data communication between users, IoT devices and data centers, as well as storage and processing devices. Therefore, a fog-based IoT system can has dependability challenges, such as managing data flow of IoT devices, memory limitation and power constrains [12].

This paper studies the crucial rule of dependability of IoT systems and its implications in different applications. In the following sections, first some factors that affect the IoT system's dependability will be identified, then the challenges that can impact the dependability as well as some solutions for overcoming these challenges will be explored. Then a case study related to IoT system that faced dependability problems will be presented. Finally, a conclusion and future work are described.

2. FACTORS AFFECTING DEPENDABILITY IN IOT SYSTEMS

Dependability allows for continuity (uninterrupted) of system services [13]. In other words, a dependable system should provide mechanisms to tolerate any condition throughout its life cycle. The dependability can be achieved through different factors including reliability, availability, safety and security, resilience, fault management methods, scalability, and other factors [14].

2.1 Reliability

We begin by considering the traditional IoT architecture, characterized by centralized data processing and decision-making. This framework emphasizes the limitations of this approach, particularly in terms of latency and scalability [1].

First, confirm that you have the correct template for your paper size. This template has been tailored for output on the A4 paper size. If you are using US letter-sized paper, please close this file and download the Microsoft Word, Letter file.

System reliability is the probability that system will behave as expected (without failure) over a given period of time (t). The system reliability can be measured through two metrics: mean time between failures (MTBF) and mean time to failure (MTTF). The reliability is measured by MTBF if the system has failure recovery mechanism, while MTTF is used to measure the reliability if there is no failure recovery mechanism [15]. Given R(t) is the reliability function of time:

$$R(t) = e^{-\lambda t} \quad (1)$$

where λ=1/ MTBF if there is recovery mechanism, otherwise λ=1/ MTTF.

Reliability is critical in IoT environment because unreliable data collection, processing, and transmission can cause long delay and data loss which can lead to a loss of confidence in the IoT systems, and therefore reliability is essential for the widespread of these systems [16].

2.2 Availability

The availability attribute in IoT system is directly related to reliability. The availability of an IoT system can be defined as its ability to deliver the required service as long as possible to ensure continuous operation. There are methods that can help to keep the system available, like maintaining a mechanism for faults management [17], and apply some approaches to manage hardware redundancy [18]. The availability can be calculated as follows:

$$Availability = \frac{MTTF}{MTTF+MTTR} \quad (2)$$

where MTTF is mean time to failure, and MTTR is mean time to repair.

2.3 Safety and Security

Safety and security are essential non-functional requirements (NFR) for any IoT system and are considered critical attributes for its dependability [19]. Safety is key attributes in IoT systems to prevent harm to their users or to the IoT environment [20]. IoT's security is related to avoiding security threats [21]. The two attributes are both source of risks and there are affected by each other [22]. Many IoT applications are integrated into safety critical environment, such as smart transportation

and medical healthcare devices. It is essential to mitigate potential risks associated with these situations. Similarly, security protection against unauthorized access and cyber-attacks can help to preserve user privacy and sensitive information

One of major requirements of an IoT system is that safety and security issues are designed to support the dependability of the system. Many attributes could affect the safety and security of IoT systems, such as hardware faults and, human errors, and security attacks [23]. These impediments need to be identified and mitigated.

2.4 Resilience

Resilience is the property of preserving the system's dependability when it encounters changes; thus, it is the ability to deal with failure, predict, tolerate and prevent it [24]. In an IoT system, the devices are connected through a network, and resilience is responsible for keeping the system connected regardless any failure that could affect the network [25]. The IoT system must deal with some constraints related to resources, such as network, memory and battery constraints, to recover from faults and failures as quickly as possible. Therefore, for the IoT system to be resilient, it should provide a fault (and failure) management mechanism. In addition, the system should be survivable in which it should offer continuity throughout managing and recovering the faults.

2.5 Fault and Failure Management

In IoT systems, a failure represents an unexpected behavior, such as data loss due to network connection problems or due memory overflow. To deal with faults, there are four strategies: detection, prediction, mitigation and prevention. Fault detection is the process of verifying the unexpected behavior using various methods, such as statistical machine learning methods [26], while fault prediction applies different techniques to predict probable failure, such as classification and regression techniques. Fault mitigation aim to recover the IoT system from failure, such as applying node load balancing [27] and redundancy techniques [28]. Fault preventions aims to prevent fault occurrence using different approach, replicating data on more than one node.

2.6 Assuring Data Quality and integrity

In IoT system, the collected data should represent the actual system context. For example, in an environment such as Polar Regions, where the climate is always cold, data from temperature sensors with a warm temperature is likely wrong. Therefore, an IoT system should previously know the context and related domain to provide meaningful and trustworthy results that are suitable for accurate decision -making [29].

2.7 Scalability

The IoT system should be scalable to accommodate thousands or even millions of sensors in terms of data transfer, storage, and real time processing [30]. The scalable system needs to provide more computing devices as well as the required hardware infrastructure [31].

2.8 Heterogeneity

The IoT system includes different heterogeneous devices that have different technologies and hardware implementations [32]. The IoT system provides the needed protocols to enable devices to communicate and understand each other. Each communication protocol has its own characteristics and application scenarios. For example, low- power wide- area network (LPWAN) technologies provide low power consumption and long transmission ranges. Examples of LPWAN technologies: Sigfox and NB-IoT [33]. Other examples of IoT communications technologies are: Bluetooth [34], Z-Wave [35], and Zigbee [36]. Furthermore, IEEE 802.11 standards can be adopted in an IoT environment for devices with no battery constraints and for data transmission over short distances [34].

3. CHALLENGES TO DEPENDABILITY IN IOT SYSTEMS

This section presents some of most important challenges of dependability in IoT systems:

3.1 Real-Time Analysis and Resource Constrains

In the IoT environment, dealing with real-time analysis and resource constrains is major challenge. Real-time analysis involves processing data immediately as it received from sensors without significant delay. Furthermore, there is a need address resource constraints such as limited availability of memory and power. IoT devices may have limited resources compared to other traditional devices, as they often designed to be small, inexpensive, and power-efficient. As a result, implementing complex real-time IoT system given some resource constraints can be challenging.

Energy consumption is a major challenge, and more research is needed to implement IoT systems with low power consumption [38]. The IoT requires mechanism of minimizing the power to be spent during the system

operation.

3.2 Connection Redundancy

Connection redundancy is a crucial aspect of ensuring dependable and continuous communication in IoT deployments. The IoT system may involve numerous interconnected devices with different data formats. IoT nodes can be deployed with more than one communication protocol [37]. Disconnections can be prevented using monitoring mechanism that make automatic switching between connection technologies. In other words, each node can transmit and receive data using two or more communication protocols and it can select a protocol with better performance. However, in scenarios with huge number of nodes and connection redundancy mechanisms, it is challenge to deploy without the cost of hardware.

3.3 Quick Fault-Recovery

IoT system needs to detect and recover faults that may occur in its components. It is critical to ensure that the system can detect and recover from faults in real-time. Faults can arise due to hardware failure, software error, human error, or environmental factors.

4. STRATEGIES FOR OVERCOMING IOT DEPENDABILITY CHALLENGES

Some strategies can help to overcome IoT challenges. For example, using efficient and lightweight algorithms can be used to optimize the computational burden on IoT devices.

Other approach that can help to optimize IoT devices communication is applying edge computing to perform data processing near the IoT devices themselves, rather than sending all data to centralized server. The edge devices such as edge or gateway servers can perform data analysis and filtering locally reducing the need for continuous high-bandwidth communication.

Applying prioritization task mechanism allocate resources based on tasks importance as well as scheduling mechanisms that ensure critical tasks get the resources promptly. Furthermore, enable the IoT system to dynamically adjust resource allocation based on task priority and available resources will help the system to respond any changing condition

To overcome the limited-power challenges, it is recommended to use hardware components that are designed for low-power operational environment. For example, using energy-efficient microcontrollers that offer needed computational capabilities will help to minimize power consumption during the IoT system operation. Using energy harvesting techniques (such as solar panels) to power IoT devices can help can help to extend battery life or even eliminate the need for batteries.

Using artificial intelligent (AI) techniques can play vital role in enhancing IoT system dependability. AI techniques can analyze massive amount of data, predict probable failures, and detect security threats, aiding in system optimization and predictive maintenance. Using AI techniques can help in developing decision-making system that can be used to enhance system reliability, ensuring that IoT system can adapt to changes and provide consistent performance.

By combining these strategies, many challenges can be resolved, enabling a more robust and efficient IoT system.

5. CASE STUDY: NEST THERMOSTAT GLITCH

One example of an IoT system that faced problems that affect its dependability is the "Nest Thermostat Glitch" incident that occurred in January 2016 [39]. Nest Labs, a company owned by Google, and specializing in home automation and WiFi-enabled products that can controlled remotely, such as smart thermostats, sensor-driven and smoke detectors [40]. This company experienced a service outage that impacted a large number of their smart thermostats [41].

Nest's smart thermostats allow their users to remotely control their home heating and cooling systems through web service or mobile app. The smart thermostat aims to provide personalized comfort to users and optimized energy usage. This thermostat collects data from sensors and use machine learning techniques to adjust the temperature [42].

On January 13, 2016, an unexpected glitch happened On Nest's servers during a scheduled maintenance update. As a result of this glitch, many Nest thermostats became inaccessible for users. Some thermostats also provide wrong temperature readings, causing problems in heating and cooling systems. This accident affected the dependability of Nest thermostats and led to user dissatisfaction and inconvenience as many users were unable to control their thermostat, and the wrong temperature reading caused energy inefficiency and discomfort in their homes [41].

Nest engineers investigate and address the root cause of the glitch and developed solutions to prevent occurring similar incident in the future to ensure the dependability of their smart system. The nest lab implemented more extensive testing procedures before final deploying their final system. Additionally, they improve the communication protocols to promptly response to any incident and keep user updated related to issues related to their service.

The Nest Thermostat Glitch incident illustrates how even well-established IoT companies can face dependability challenges. This incident showed the importance of rigorous testing, quality assurance, and redundancy in IoT systems. Furthermore, it highlights the necessity of having backup solutions in place to ensure reliable system functionality.

6. CONCLUSION AND FUTURE WORK

The role of dependability in IoT systems is essential to ensure a reliable and secure system. Dependability plays a critical role in building trust, ensuring safety, and enabling the successful implementation of IoT solutions. By addressing the challenges related to reliability, resilience, security, and other dependability aspects, stakeholders can unlock the full potential of IoT, empowering industries and individuals with transformative, efficient, and reliable technologies.

This paper identified factors affecting IoT system dependability, including reliability, availability, safety, security, resilience, fault management, data quality, scalability, and heterogeneity. There are several dependability challenges including real- time processing, limited resources, continuous communication and quick fault recovery. This paper addressed some strategies to overcome these challenges and enhance the dependability such as efficient algorithms, edge computing, prioritization/ scheduling of resources, and using AI techniques. This paper also identified one case study that faced problems that affect its dependability, which is the "Nest Thermostat Glitch" incident. This incident showed how it is necessary to perform rigorous testing, quality assurance, and redundancy before final deployment of the IoT systems, and how it is important to have backup solutions in place to ensure reliable system functionality.

As future work, a framework to evaluate IoT dependability can be developed. This framework should consider several factors to assess the dependability of an IoT system. The framework will define a quantifiable metrics to measure different factors, such as reliability, availability, safety, security, resilience, and fault management. These metrics can be used for evaluating the system's performance. By developing such framework, the IoT system decision makers can assess the dependability, and can take enhancing steps that will lead to more reliable and successful IoT solutions.

In comparison to previous works in the realm of the Internet of Things (IoT), our study delves into the paramount role of dependability in IoT systems. While past research has acknowledged the significance of some factors such as reliability and security in IoT [20-23], our paper extends the discussion to emphasize resilience, real-time analysis, connection redundancy, and swift fault recovery as critical factors influencing dependability. We build upon existing literature by proposing strategic solutions to overcome these challenges, including the integration of efficient algorithms, edge computing, resource prioritization, and the incorporation of artificial intelligence techniques. Notably, our work contributes a valuable case study highlighting the practical implications of dependability issues in an IoT system. This case underscores the necessity for rigorous testing and redundancy measures to ensure the reliability of IoT deployments, an aspect that has not been extensively explored in prior studies. Furthermore, we advocate for the development of a comprehensive framework for evaluating and enhancing IoT dependability in future work. This proposed framework will consider a spectrum of factors including reliability, availability, safety, security, resilience, and fault management, providing quantifiable metrics for a holistic assessment of IoT systems. Our research contends that by addressing these dependability challenges, stakeholders can unlock the full potential of IoT, fostering transformative, efficient, and reliable technologies for both industries and individuals.

REFERENCES

[1] Nižetić, Sandro, et al. "Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future." Journal of cleaner production 274 (2020): 122877.

[2] Kumar, Sachin, Prayag Tiwari, and Mikhail Zymbler. "Internet of Things is a revolutionary approach for future technology enhancement: a review." Journal of Big data 6.1 (2019): 1-21.

[3] Kumar, Mohit, Kalka Dubey, and Rakesh Pandey.

"Evolution of emerging computing paradigm cloud to fog: applications, limitations and research challenges." 2021 11th international conference on cloud computing, data science & engineering (Confluence). IEEE, 2021

[4] L. Bukowski, "System of systems dependability—Theoretical models and applications examples", Rel. Eng. Syst. Saf., vol. 151, pp. 76-92, Jul. 2016.

[5] Avižienis, A., Laprie, J. C., Randell, B., Landwehr, C. (2004): Basic concepts and taxon-omy of dependable and secure computing. IEEE Trans. Dependable Secure Comput.,1(1).

[6] E. Park, A. del Pobil and S. Kwon, "The role of Internet of Things (IoT) in smart cities: Technology roadmap-oriented approaches", Sustainability, vol. 10, no. 5, pp. 1388, May 2018.

[7] P. P. Ray, "A survey on Internet of Things architectures", J. King Saud Univ. Comput. Inf. Sci., vol. 30, no. 3, pp. 291-319, 2018.

[8] S. Verma, Y. Kawamoto, Z. M. Fadlullah, H. Nishiyama and N. Kato, "A survey on network methodologies for real-time analytics of massive IoT data and open research issues", IEEE Commun. Surveys Tuts., vol. 19, no. 3, pp. 1457-1477, 3rd Quart. 2017.

[9] R. Mahmud, R. Kotagiri and R. Buyya, "Fog computing: A taxonomy survey and future directions" in Internet of Everything, Singapore:Springer, 2018.

[10] F. Bonomi, R. Milito, J. Zhu and S. Addepalli, "Fog computing and its role in the Internet of Things", Proc. 1st Ed. MCC Workshop Mobile Cloud Comput. (MCC), pp. 13-16, 2012.

[11] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow and P. A. Polakos, "A comprehensive survey on fog computing: State-of-the-art and research challenges", IEEE Commun. Surveys Tuts., vol. 20, no. 1, pp. 416-464, 1st Quart. 2018.

[12] H. Atlam, R. Walters and G. Wills, "Fog computing and the Internet of Things: A review", Big Data Cogn. Comput., vol. 2, no. 2, pp. 10, Apr. 2018.

[13] L. M. C. E. Martins, F. L. de Caldas Filho, R. T. de Sousa Júnior, W. F. Giozza and J. P. C. L. da Costa, "Increasing the dependability of IoT middleware with cloud computing and microservices", Proc. 10th Int. Conf. Utility Cloud Comput. (UCC Companion), pp. 203-208, Dec. 2017.

[14] J.-H. Cho, S. Xu, P. M. Hurley, M. Mackay, T. Benjamin and M. Beaumont, "STRAM: Measuring the trustworthiness of computer-based systems", ACM Comput. Surv., vol. 51, no. 6, pp. 1-47, Feb. 2019.

[15] C. Maiorano, E. Pascale, L. Bouillaut, P. Sannino, Y. Solorzano, S. Borriello, et al., "MTBF (metric that betrays folk)", Proc. 29th Eur. Saf. Rel. Conf., pp. 6, 2019.

[16] Prasad, S.S., & Kumar, C. 2013. A Green and Reliable Internet of Things. Communications and Network, 5(1B), pp.44-48. Available at: https://doi.org/10.4236/cn.2013.51B011.

[17] Z. Bakhshi and G. Rodriguez-Navas, "A preliminary roadmap for dependability research in fog computing", SIGBED Rev., vol. 16, no. 4, pp. 14-19, 2020.

[18] E. Andrade and B. Nogueira, "Dependability evaluation of a disaster recovery solution for IoT infrastructures", J. Supercomput., vol. 76, no. 3, pp. 1828-1849, Mar. 2020.

[19] Abdulhamid, A.; Kabir, S.; Ghafir, I.; Lei, C. Dependability of The Internet of Things: Current Status and Challenges. In Proceedings of the 2nd International Conference on Electrical, Computer, Communications and Mechatronics Engineering, Malé, Maldives, 16–18 November 2022; pp. 2532–2537. [Google Scholar]

[20] Kumar, R.; Stoelinga, M. Quantitative security and safety analysis with attack-fault trees. In Proceedings of the 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), Singapore, 12–14 January 2017; pp. 25–32. [Google Scholar]

[21] Sasaki, R. A Risk Assessment Method for IoT Systems Using Maintainability, Safety, and Security Matrixes. In Information Science and Applications; Springer: Singapore, 2020; Volume 621, pp. 363–374. [Google Scholar]

[22] Cerf, V.G.; Ryan, P.S.; Senges, M.; Whitt, R.S. Iot safety and security as shared responsibility. Bus. Inform. 2016, 1, 7–19. [Google Scholar] [CrossRef]

[23] Kabir, S.; Gope, P.; Mohanty, S.P. A Security-enabled Safety Assurance Framework for IoT-based Smart Homes. IEEE Trans. Ind. Appl. 2022, 59, 6–14. [Google Scholar] [CrossRef]

[24] C. Tsigkanos, S. Nastic and S. Dustdar, "Towards resilient Internet of Things: Vision challenges and research roadmap", Proc. IEEE 39th Int. Conf. Distrib. Comput. Syst. (ICDCS), pp. 1754-1764, Jul. 2019.

[25] V. Prokhorenko and M. A. Babar, "Architectural resilience in cloud fog and edge systems: A survey", IEEE Access, vol. 8, pp. 28078-28095, 2020.

[26] D. Ratasich, F. Khalid, F. Geissler, R. Grosu, M.

Shafique and E. Bartocci, "A roadmap toward the resilient Internet of Things for cyber-physical systems", IEEE Access, vol. 7, pp. 13260-13283, 2019.

[27] F. H. Rahman, T.-W. Au, S. H. S. Newaz, W. S. Suhaili and G. M. Lee, "Find my trustworthy fogs: A fuzzy-based trust evaluation framework", Future Gener. Comput. Syst., vol. 109, pp. 562-572, Aug. 2020.

[28] Z. Bakhshi and G. Rodriguez-Navas, "A preliminary roadmap for dependability research in fog computing", SIGBED Rev., vol. 16, no. 4, pp. 14-19, 2020.

[29] H. Baqa, N. B. Truong, N. Crespi, G. M. Lee and F. L. Gall, "Quality of information as an indicator of trust in the Internet of Things", Proc. 17th IEEE Int. Conf. Trust Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE), pp. 204-211, Aug. 2018.

[30] S. Verma, Y. Kawamoto, Z. M. Fadlullah, H. Nishiyama and N. Kato, "A survey on network methodologies for real-time analytics of massive IoT data and open research issues", IEEE Commun. Surveys Tuts., vol. 19, no. 3, pp. 1457-1477, 3rd Quart. 2017.

[31] K. Iwanicki, "A distributed systems perspective on industrial IoT", Proc. IEEE 38th Int. Conf. Distrib. Comput. Syst. (ICDCS), pp. 1164-1170, Jul. 2018.

[32] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A survey on enabling technologies protocols and applications", IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347-2376, 4th Quart. 2015.

[33] K. Mekki, E. Bajic, F. Chaxel and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment", ICT Exp., vol. 5, no. 1, pp. 1-7, Mar. 2019.

[34] O. Elijah, T. A. Rahman, I. Orikumhi, C. Y. Leow and M. N. Hindia, "An overview of Internet of Things (IoT) and data analytics in agriculture Benefits and challenges", IEEE Internet Things J., vol. 5, no. 5, pp. 3758-3773, Oct. 2018.

[35] M. B. Yassein, W. Mardini and A. Khalil, "Smart homes automation using Z-wave protocol", Proc. Int. Conf. Eng. MIS (ICEMIS), pp. 1-6, Sep. 2016.

[36] J.-S. Lee, Y.-W. Su and C.-C. Shen, "A comparative study of wireless protocols: Bluetooth UWB ZigBee and Wi-Fi", Proc. IECON 33rd Annu. Conf. IEEE Ind. Electron. Soc., pp. 46-51, Nov. 2007.

[37] G. Signoretti, M. Silva, J. Araujo, I. Silva, D. Silva, P. Ferrari, et al., "A dependability evaluation for OBD-II edge devices: An Internet of intelligent vehicles perspective", Proc. 9th Latin-Amer. Symp. Dependable Comput. (LADC), pp. 1-9, Nov. 2019.

[38] Shakerighadi, Bahram, et al. "Internet of things for modern energy systems: State-of-the-art, challenges, and open issues." Energies 11.5 (2018): 1252.

[39] Zeng, Eric, Shrirang Mare, and Franziska Roesner. "End user security and privacy concerns with smart homes." thirteenth symposium on usable privacy and security (SOUPS 2017). 2017.

[40] Crunchbase website (2023), Nest Lab company, [Online], Available: https://www.crunchbase.com/organization/nest-labs

[41] Bilton, Nick. "Nest thermostat glitch leaves users in the cold." The New York Times 14 (2016).

[42] Park, Toby. "Evaluating the Nest Learning Thermostat-Four field experiments evaluating the energy saving potential of Nest's Smart Heating Control." (2017).

.