Analysis of the Trust and Resilience of Consumer and Industrial Internet of Things (IoT) Systems in the Indian Context

Akaash R. Parthasarathy

Abstract The Internet of Things (IoT) connects every device possessing some element of computer technology or a digital interface. These devices constitute a global interconnected network that bridges the gap between the physical and virtual worlds. Today, there are two major applications for IoT—Consumer Internet of Things (CIoT), concerned with interactions between consumers and IoT devices, and industrial Internet of Things (IIoT), focussed on the utilisation of IoT for designing industrial systems. With the proliferation of IoT devices for myriad applications, it is becoming increasingly important to investigate and understand the factors essential to securing them against external threats. These factors directly influence the design, functionality and the standards and regulations for IoT devices. This paper defines the trust and resilience of IoT systems and provides unambiguous definitions for key factors (security, privacy, safety, recoverability, reliability and scalability) that directly influence the trust and resilience of IoT systems. Based on the results of a survey conducted amongst IoT consumers and experts, this paper ranks each of these factors in the order of their importance in determining the trust and resilience of CIoT and IIoT systems. These rankings are generated using the analytic hierarchy process (AHP) and a pairwise analysis of the collected data.

Keywords Internet of things · Trust and resilience · Security

1 Introduction

The International Telecommunication Union Telecommunication Standardisation Sector (ITU-T) defines the Internet of Things (IoT) "as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" [1]. IoT broadly refers to the worldwide system of

A. R. Parthasarathy (✉)
The Shri Ram School—Aravali, Gurgaon, Haryana 122002, India

K. Khanna et al. (eds.), *Cyber Security and Digital Forensics*,
Lecture Notes on Data Engineering and Communications Technologies 73,
https://doi.org/10.1007/978-981-16-3961-6_21

devices that are connected to the Internet and can communicate and exchange data with each other. Today, IoT connects every device that possesses some element of computer technology or a digital interface. These include devices such as Amazon Echoes, which function as smart speakers and assistants, and fitness bands, which track your activity and monitor your health. IoT is responsible for bridging the gap between the physical and virtual world and has been extensively employed in myriad applications ranging from home automation to facility management.

These applications depend on the collection of data through sensors, which can measure physical quantities in the surrounding environment. IoT devices, composed of a multitude of these sensors, are integrated with powerful IoT platforms capable of organizing and manipulating the collected data to perform specific tasks [2]. For example, using IoT technology, smart lights containing proximity sensors are able to turn on or off when they detect the presence or absence of people nearby. More often than not, IoT devices and platforms are enabled with artificial intelligence (AI) to effectively handle and detect patterns in the enormous amounts of incoming data, allowing for enhanced convenience [3]. Using AI, the same smart lights can learn your sleep and work patterns and automatically adjust the lighting to suit your needs.

Historically, consumer devices, home control systems and industrial machines have been offline and not connected to any network. These entities were inherently secure since they could only be compromised through physical access. At the turn of the century, however, there was a significant explosion in computing power and techniques for data analysis, enabling the shift of security and safety systems to virtual platforms [4]. This shift came with its associated risks, both in terms of data leakages and reductions in the integrity of these systems. The past decade saw the emergence of the concept of IoT, associated with an increase in the connectivity of physical devices with each other and with virtual systems. In fact, Gartner forecasts that over 25 billion connected devices will be in use around the world by 2021 [5]. This ever-rising number of IoT devices, which is expected to soon surpass the number of people on the planet, has brought into question their trust and resilience. The immense scale of implementation and the intricacy of the computer systems involved in developing IoT devices leave them vulnerable to malicious hackers and cyber attacks [6]. Each unsecured endpoint serves as a potential location for attacks that can cripple entire IoT systems.

In 2017, Ronen et al. [7] discovered a vulnerability in the Zigbee protocol for IoT devices, allowing them to develop a self-replicating Zigbee worm to exploit Philips Hue smart lamps. This worm could spread to other lamps based on their wireless connectivity and physical proximity. Their research had large implications since similar attacks could be carried out across entire cities, leading to city-wide blackouts. More recently, in February 2020, it was demonstrated that several Philips Hue smart lamps could be hacked with the assistance of drones.

It is evident that device interoperability, trusted communication and the secure sharing and management of data are key aspects that need to be addressed when

designing and analysing IoT systems. Thus, research into developing standards for and enhancing the resilience of IoT systems has gained considerable traction in recent years.

2 Consumer and Industrial Internet of Things

IoT can be categorically divided into consumer IoT (CIoT) and industrial IoT (IIoT). CIoT is the more widely known variant of IoT and broadly encompasses IoT devices used to meet consumer needs and increase consumer convenience. CIoT is mainly focussed on residential and consumer interactions with IoT devices such as smart home appliances and wearable technology. IIoT, on the other hand, is concerned with using IoT devices for industrial applications such as synchronisation of manufacturing equipment and operation of integrated supply chains. IIoT makes use of a combination of sensor-driven computing, data analytics and intelligent machines to promote the efficiency of industrial processes and increase enterprise productivity [8].

Since IIoT systems involve the transmission of vast amounts of confidential data, unauthorized access to this data has far-reaching impacts. Despite being less popular and prevalent, IIoT has made significant progress towards standardisation with the help of industrial consortiums dedicated to the advancement of machine-to-machine communication and the promotion of open standards for security and interoperability [4]. These standards have continuously been revisited and updated for several years.

CIoT devices are independently developed by smart device and application providers through the use of traditional interfaces, which emphasise usability and functionality over trust and resilience [9]. Mechanisms to ensure security, privacy and safety are often incorporated solely on the basis of present consumer needs without appropriate planning for subsequent integrations. These concerns arise due to the absence of well-documented standards for CIoT systems, and as a result of the fact that CIoT devices are marketed directly to consumers with limited knowledge of security protocols. For example, in September 2019, a couple's smart home was compromised by a hacker, who took control of their cameras, played disturbing music and manipulated the heat levels in their house by accessing the Google Nest thermostat. This is just one of the many attacks that have been carried out on CIoT systems.

With the widespread adoption of both CIoT and IIoT devices, it is becoming increasingly important to investigate the issues and challenges related to their trust and resilience. The impact of the various characteristics of trust and resilience on the buying and adoption decisions of consumers and industries is of great significance.

3 Literature Survey

Recently, much research has been conducted in order to identify the security and privacy risks associated with IoT devices. Atlam and Wills [10] analysed the security, privacy and safety requirements for IoT systems. They reviewed the challenges faced in IoT security and privacy and presented a case study revolving around the security threats affecting smart cities. Additionally, they provided details regarding the implementation of security and privacy by design and listed the types of cyber and physical attacks that can affect IoT systems. Papp et al. [11] wrote a primer on hacking the hardware and software of IoT systems, where they analysed the most commonly employed methods and scientific research on IoT hacking.

Prior research has focussed on the development of malware to test the resilience of IoT systems. A few of these attempts have been successful in depicting threats to IoT protocols on a global scale [7, 12]. In an attempt to enhance the recoverability of IoT systems, researchers have also proposed self-recoverable IoT architectures, which employ time synchronisation combined with a novel algorithm to achieve formerly unobtainable results [13].

Within the field of IoT, there has also been research into the specific security threats and concerns related to CIoT and IIoT, with individual analyses having been performed for both CIoT [14, 15] and IIoT [16] systems. In order to achieve significantly higher levels of security and privacy, researchers have explored the viability of applying blockchain to CIoT and IIoT security [17]. Additionally, Wurm et al. [9] analysed and contrasted the security features and concerns in CIoT and IIoT devices. Techniques for enhancing the reliability and scalability of CIoT and IIoT systems have also similarly been investigated.

Research has also be conducted into the standardisation of IoT systems. Reference [4] is a comprehensive document analysing and outlining regulations and standards related to the security framework of IIoT systems from both business and implementational viewpoints. Additionally, [4] defines crucial terms related to the trustworthiness of IIoT systems. Taking a major step in the right direction, the European Telecommunication Standards Institute released the first global standard for CIoT devices, which outlines baseline requirements for internet-connected consumer products, in early 2019. The most recent iteration of this standard was released in June 2020 [18].

3.1 Research Gap and Contributions

It is clear that substantial research has been conducted in the field of IoT. Whilst a majority of this research has focussed on individual factors such as security, privacy and safety that impact the functioning of IoT devices, these variables or characteristics have not been comprehensively analysed in terms of their cooperative

functioning. Additionally, these factors have usually been examined for IoT frameworks in general and have not been compared and contrasted across the CIoT and IIoT spaces.

This paper investigates the factors affecting the trust and resilience (see Sect. 3.2) of IoT systems. This paper initially identifies and provides definitions for key factors that influence the trust and resilience of IoT systems according to the current research in the field. Next, it assesses the importance of each of these factors in determining the trust and resilience of CIoT and IIoT systems (both separately and combined) based on the results of a survey conducted amongst IoT consumers and experts. The paper ranks the factors against each other based on a pairwise analysis of the collected data. Using the survey results, this paper makes recommendations to enhance the trust and resilience in both the CIoT and IIoT spaces, thereby providing logical steps to follow as the IoT market enlarges.

The remainder of this paper is organised as follows: Sect. 3.2 introduces the concept of trust and resilience and presents key definitions of certain factors that describe the trust and resilience of IoT systems. Section 4 describes the methodology of the study utilised to analyse the impact of each of these factors on the trust and resilience of both CIoT and IIoT systems. The results of the study are presented and analysed in Sect. 5. Conclusions are drawn in Sect. 6, and the future scope of the work is discussed in Sect. 7.

3.2 Trust and Resilience of IoT Systems

IoT systems, like all other information systems, have key features and elements that define their trust and resilience (T&R). T&R of IoT systems is particularly important due to our continuously increasing dependence on them. A system is said to be resilient to a fault if its core capabilities are unhindered in the presence of that fault. T&R of an IoT system can be defined by its capacity to "withstand a major disruption within acceptable degradation parameters and to recover within an acceptable time" [19]. This encompasses resistance to both external attacks and internal failures, and adaptation to continual change in global policies and standards.

Whilst no system can be fully trustworthy and resilient, laws and standards assist in maintaining their T&R to a certain degree by creating a balance between functionality and compliance. Although creativity and innovation can lead to the development of novel products and services, improper maintenance and failure to adhere to standards can result in issues such as data and identity theft. It is imperative to establish thorough guidelines and standardisation techniques in order to streamline processes related to the collection and transmission of data, and enhance the interoperability of IoT devices.

However, developing effective regulations necessitates an understanding of the different facets of the subject you are dealing with. In this subsection, six key characteristics that comprise T&R of IoT systems—security, privacy, safety,

recoverability, reliability and scalability—have been defined based on the current research in IoT [4]. All further mentions of these characteristics will adhere to the definitions in this subsection.

Security. Collins Dictionary defines security as "all the measures that are taken to protect a place, or to ensure that only people with permission enter it or leave it" [20]. A similar definition can be extended to IoT systems: Security in an IoT system refers to the countermeasures that can be put in place to prevent any individual or group from exploiting the system. Systems have vulnerabilities or security risks that may be exploited and thus, need to be kept secure and protected from unauthorised access. The security of a system is defined by the CIA triad: confidentiality, which deals with unauthorised disclosure of information, integrity, which deals with unauthorised modification or deletion of data, and availability, which deals with reliable access to systems and data by authorised personnel [4].

Privacy. For the purposes of this paper, Adam Moore's [21] definition of privacy, wherein privacy is defined as an "access control right over oneself and to information about oneself", has been adopted. Privacy is the right of an individual or a group to decide how information concerning them should be utilised. This includes control over who has access to this personal information and the methods involved in collecting, processing and storing the information [4]. In terms of IoT, privacy refers to preventing the unauthorised access of personal information of an individual or a group in an IoT system. Privacy is ensured if this data is handled by an entity and in a manner that said individual or group has lawfully agreed to. With the growing popularity of IoT and the spike in the amount of personal information being handled and analysed by IoT systems and devices, manufacturers and service providers are required to become increasingly sensitive to consumer privacy and data protection. As such, major steps are being taken towards redefining the current techniques for ensuring privacy and aligning them with global standards [22].

Safety. An IoT system is said to be safe when it can operate without putting people at risk beyond specified acceptable limits. An IoT system must operate without endangering the lives of or causing physical harm to its users [4]. Device malfunctions and transmission of incorrect data may affect health, cause bodily harm or even be life threatening. Safety of IoT systems encompasses the measures taken to prevent such occurrences.

Recoverability. The recoverability of an IoT system is its ability to be restored to a stable state once the failures acting on it cease [23]. Recoverability is closely related to fault tolerance which aims to ensure the attainment of system goals even in the presence of unfavourable conditions and errors [24]. They are focussed on providing certain service level guarantees despite the occurrence of faults. A system is said to be recoverable to a fault if "there exists a control law such that the post-fault system satisfies the design specifications" [24].

Reliability. Reliability is the ability of an IoT system to consistently perform as it is expected to. Reliability determines whether an IoT system is capable of performing its assigned tasks for an extended period of time [4]. Reliability is applicable not only to IoT devices and their data collection techniques but also to the

utilised communication frameworks. It is an essential factor in building trust in both commercial and industrial applications.

Scalability. As defined by Gupta et al. [25], scalability is "the ability of a device [or system] to adapt to changes in the environment and meet changing needs in the future". In terms of IoT, scalability refers to the capability of IoT systems to "support an increasing number of connected devices, users, application features and analytics capabilities, without any degradation in the quality of service" [26]. In this increasingly virtual and hyper-connected world, ecosystems must possess the ability to scale and plan for unusual spikes in requests. It is important for IoT systems to adapt to changing volumes of work due to factors such as seasonal demands.

4 Methodology

In order to analyse the influence of each of the T&R factors on the T&R of CIoT and IIoT systems, an online survey was conducted amongst more than 90 consumers and industry and corporate experts from across the world (however, a majority of the survey respondents were from India) using the SurveySparrow platform. The survey explicitly defined each of the T&R factors in order to reduce any ambiguity resulting from the wording of the questions.

The survey was divided into two sections—one for CIoT systems (see Fig. 1) and one for IIoT systems. Both of the sections contained the same questions, but were specific to the respective system. For each pair of factors, survey respondents were asked which factor they believed is more important in determining the T&R of the relevant type of IoT system. These choices were to be made under the assumption that the remaining 4 factors were stable or perfectly implemented. Respondents were additionally asked to take into account the impact of the remaining 4 factors on the factors under consideration, whilst making their choices. Figure 2 details the instructions for answering the questions in the CIoT section of the survey (Fig. 3).

Fig. 1 Survey section on T&R factors in CIoT systems. *Source* SurveySparrow

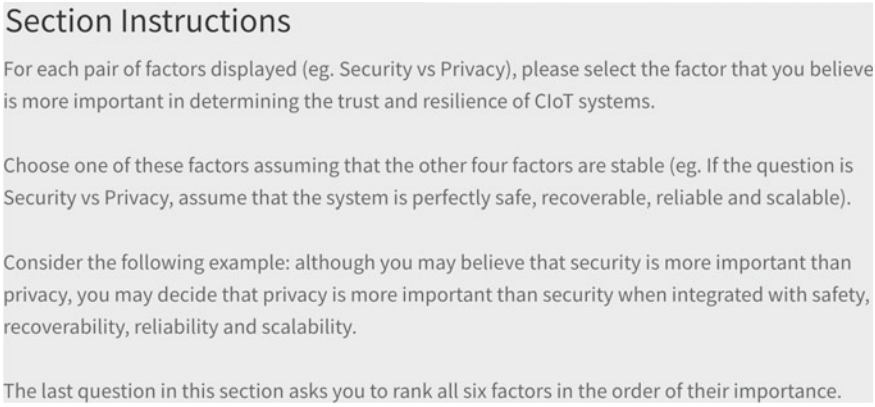

Fig. 2 Section instructions for survey section on T&R factors in CIoT systems. *Source* SurveySparrow

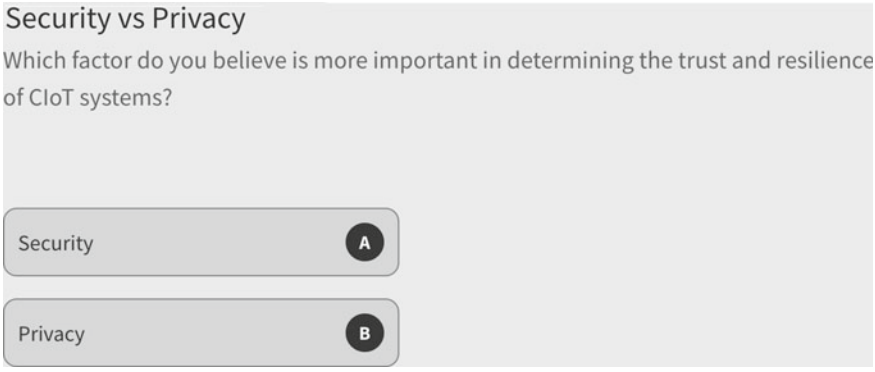

Fig. 3 A sample question from the CIoT section of the survey. *Source* SurveySparrow

The collected data was examined using the SpiceLogic AHP Software v2.2 [27]. The technique used to analyse the data was the analytic hierarchy process (AHP) for multi-criteria decision making (MCDM). Initially, as shown in Fig. 4, the objectives for the AHP were added, with the aim to maximise each T&R factor in the IoT system. Then, a pairwise analysis was conducted on the data, taking into each account each possible pair of factors. The percentages of survey respondents who chose each factor in the survey were inputted as weights in order to calculate the priority trade-off for each pair.

This procedure was followed for the responses for both CIoT systems and IIoT systems. Additionally, a pairwise analysis was performed on the combined data for both types of systems.

Objective	Attribute Type	Range	Relative Priority
1. Maximize Security	Subjective	0 to 100	24.77%
2. Maximize Privacy	Subjective	0 to 100	19.51%
3. Maximize Safety	Subjective	0 to 100	24.46%
4. Maximize Recoverability	Subjective	0 to 100	9.26%
5. Maximize Reliability	Subjective	0 to 100	17.84%
6. Maximize Scalability	Subjective	0 to 100	4.15%

Fig. 4 Maximisation objectives and their relative priorities. *Source* SpiceLogic Analytic Hierarchy Process Software v2.2

5 Results

The pairwise analysis conducted on the survey responses yielded a chart of the relative priority numbers of percentages of each of the T&R factors. These percentages indicate the importance of each of the T&R factors to the respective IoT system when stacked against each other. Based on the results from the AHP software, bar charts were created using Excel for the relative priorities of the T&R factors for CIoT systems, IIoT systems and the two when considered as a whole (Fig. 5).

As depicted in Fig. 6, security assumed the highest priority for CIoT systems with a relative priority number of nearly 25%, followed closely by safety. The subsequent levels of importance were occupied by privacy and reliability, respectively, whilst recoverability and scalability were considered to be the least important T&R factors by a margin of almost 9%.

As shown in Fig. 7, security was similarly assigned the highest relative priority number for IIoT systems. The generated relative priority number for safety was

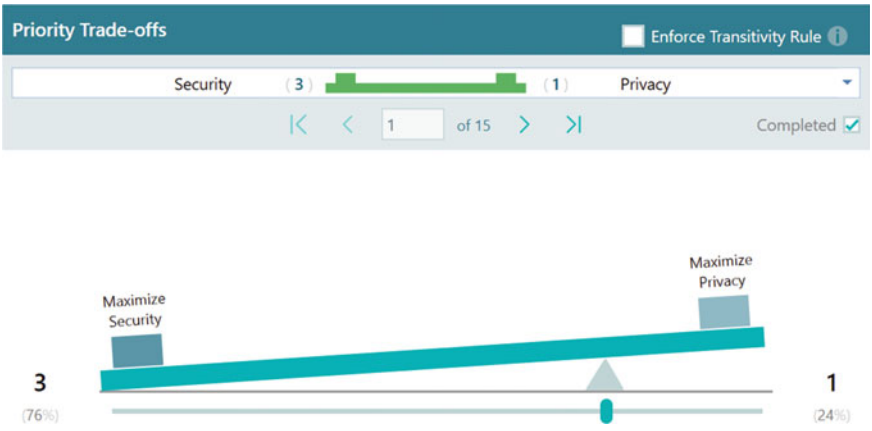

Fig. 5 Priority trade-off for maximisation of security and maximisation of privacy. *Source* SpiceLogic Analytic Hierarchy Process Software v2.2

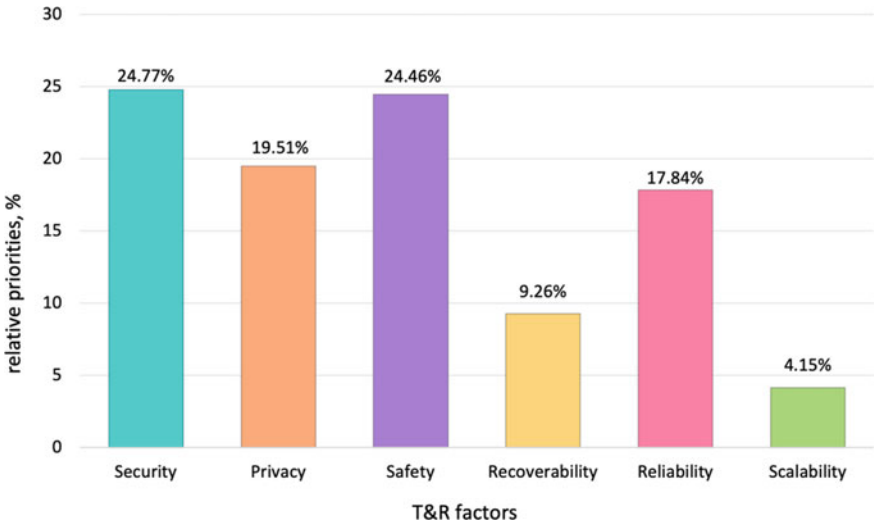

Fig. 6 Relative priorities of T&R factors for CIoT systems

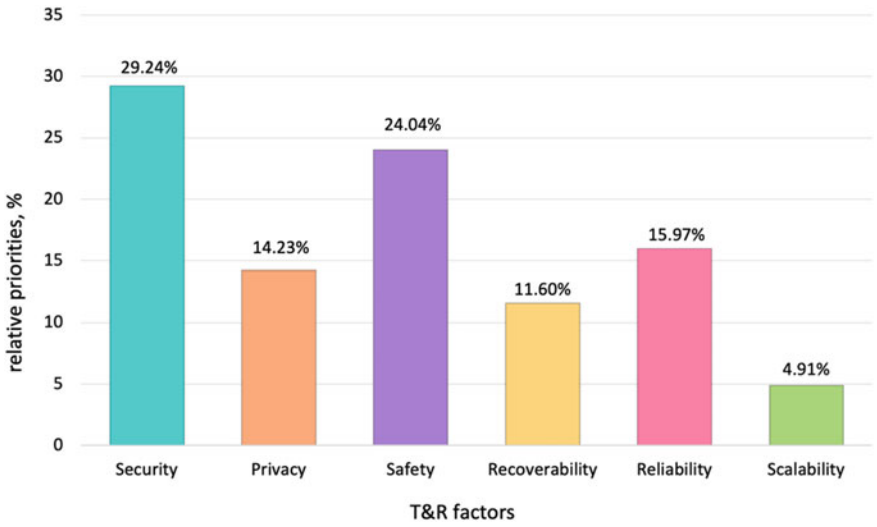

Fig. 7 Relative priorities of T&R factors for IIoT systems

similar to that in CIoT systems. Recoverability and scalability were again deemed to be the least influential in terms of the T&R of IIoT systems.

Comparing the two charts in Figs. 6 and 7, it is apparent that although security and safety occupied the highest two ranks for both types of systems, survey respondents considered security more important in determining the T&R of IIoT

systems as opposed to CIoT systems. This is reasonable given the fact that IIoT involves access to greater amounts of confidential data and the coordination of many more physically adjacent systems. These systems must additionally be accessible to authorised staff at all times, failing which severe consequences such as the shutting down of entire factories could be observed.

Privacy and reliability were found to be less important to IIoT systems than to CIoT systems. One reason for this could be concern surrounding personal data in view of relatively recent data leaks such as the Facebook-Cambridge Analytica data scandal. Further, although privacy was considered more important than reliability for CIoT systems, reliability was considered more important in relation to IIoT systems.

Recoverability was more important to IIoT systems, indicating the need for the development of more fault-tolerant IIoT systems, whilst scalability remained the least important T&R factor with no major changes in its relative priority number across IoT systems.

On performing a combined pairwise analysis (see Fig. 8) of T&R factors for both CIoT systems and IIoT systems, a similar trend was observed. An important detail to note is that security was indisputably assessed to be the most important T&R factor across IoT systems. Further, despite the aforementioned reflection regarding reliability and privacy, overall, reliability fared marginally better than privacy.

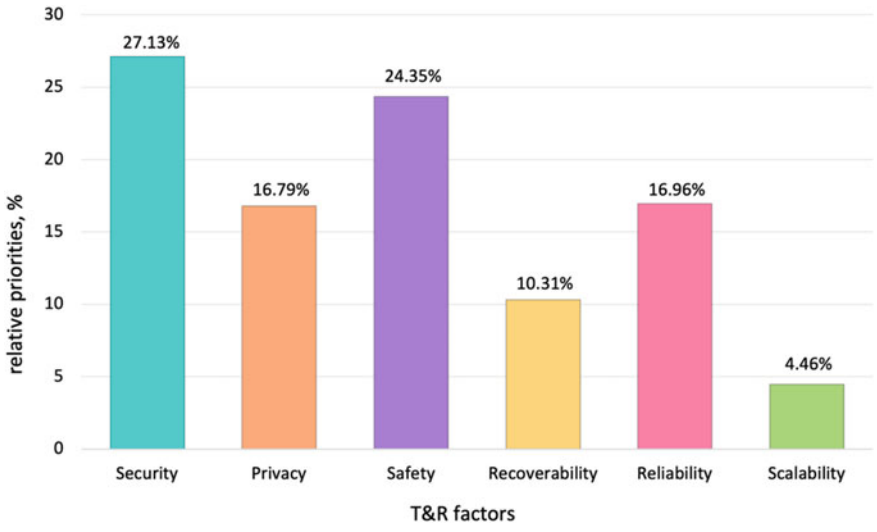

Fig. 8 Relative priorities of T&R factors for combined analysis (both CIoT and IIoT systems)

6 Conclusion

With the recent surge in IoT, many concerns have been raised as to its long-term feasibility. It is becoming increasingly necessary to address the issues surrounding the security and privacy of IoT, amongst other factors. This paper collectively laid down concise definitions for six key terms (security, privacy, safety, recoverability, reliability and scalability) influencing the T&R of IoT systems with the aim of analysing these factors with respect to the CIoT and IIoT spaces. Specifically, it utilised pairwise comparisons as part of the Analytic Hierarchy process to rank the factors according to their importance in determining the T&R of IoT devices. It compared and analysed results, obtained from a survey conducted amongst IoT experts, between CIoT and IIoT systems. It established that security is the most important factor influencing the T&R of Io systems and, in the future, special emphasis must be placed on enhancing the security features of IoT systems in order to defend against the onset of ever-increasing cyber attacks.

7 Future Scope

Although this study was limited to a small sample and the results may not be representative of the general consensus regarding the T&R of CIoT and IIoT systems, going forward the study could be extended to a larger sample to validate its findings.

The results of this study could be used to perform case studies comparing the T&R of different IoT products. The AHP software generated a multi-criteria utility function based on the relative weights of the T&R factors using a weighted sum model. For example, the combined utility function (U) for CIoT and IIoT was given by:

$$\begin{aligned} U = {} & 0.27 * [\text{Security}] + 0.17 * [\text{Privacy}] + 0.24 * [\text{Safety}] \\ & + 0.10 * [\text{Recoverability}] + 0.17 * [\text{Reliability}] \\ & + 0.04 * [\text{Scalability}] \end{aligned} \tag{1}$$

This function could be used to compare multiple IoT product alternatives and generate rankings for them.

Additionally, whilst the AHP operated under the assumption that each of the T&R factors were independent, a method such as the analytic network process (ANP) could be later used to consider the interdependence between the factors, whilst developing IoT systems.

Acknowledgements I would like to thank Dr. Dinesh Likhi, adjunct professor at the Indian Institute of Technology, Roorkee, for guiding me throughout this research, Dr. Akanksha Upadhyaya, Associate Professor, Rukmini Devi Institute of Advanced Studies, New Delhi for her review and comments on the paper, and Dr. Kavita Khanna, Associate Professor and the Head of the Department of Computer Science and Engineering, The NorthCap University, Gurgaon for guiding me and giving me the opportunity to present my paper at the ICCSDF 2021 conference at The NorthCap University. I would also like to thank my parents for their constant guidance and support.

References

1. International Telecommunication Union.: ITU-T Y.4000/Y.2060 "ITU-T recommendations". http://handle.itu.int/11.1002/1000/11559. Last accessed 20 Jan 2021
2. IBM.: What is the Internet of Things (IoT)? https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/. Last accessed 26 Jan 2021
3. Norton.: What is the Internet of Things? How the IoT Works, and More. https://us.norton.com/internetsecurity-iot-what-is-the-internet-of-things.html. Last accessed 26 Jan 2021
4. Industrial Internet Consortium.: IIC:PUB:G4:V1.0:PB:20160919 "Industrial Internet of Things Volume G4: Security Framework". https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf. Last accessed 24 Jan 2021
5. Gartner.: Gartner Identifies Top 10 Strategic IoT Technologies and Trends. https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends. Last accessed 20 Jan 2021
6. Ngo, Q.-D., Nguyen, H.-T., Le, V.-H., Nguyen, D.-H.: A survey of IoT malware and detection methods based on static features. ICT Express (2020). https://doi.org/10.1016/j.icte.2020.04.005
7. Ronen, E., Shamir, A., Weingarten, A.-O., OFlynn, C.: IoT goes nuclear: creating a ZigBee chain reaction. In: IEEE Symposium on Security and Privacy (SP), pp. 195–212. IEEE (2017). https://doi.org/10.1109/sp.2017.14
8. Panchal, A.C., Khadse, V.M., Mahalle, P.N.: Security issues in IIoT: a comprehensive survey of attacks on IIoT and its countermeasures. In: IEEE Global Conference on Wireless Computing and Networking (GCWCN), pp. 124–130. IEEE (2018). https://doi.org/10.1109/gcwcn.2018.8668630
9. Wurm, J., Hoang, K., Arias, O., Sadeghi, A.-R., Jin, Y.: Security analysis on consumer and industrial IoT devices. In: 21st Asia and South Pacific Design Automation Conference (ASP-DAC), pp. 519–524. IEEE (2016). https://doi.org/10.1109/aspdac.2016.7428064
10. Atlam, H.F., Wills, G.B.: IoT security, privacy, safety and ethics. In: Digital Twin Technologies and Smart Cities, pp. 123–149. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-18732-3_8
11. Papp, D., Tamás, K., Buttyán, L.: IoT hacking—a primer. Infocommun. J. **11**(2), 2–13 (2019). https://doi.org/10.36244/ICJ.2019.2.1
12. Vaccari, I., Cambiaso, E., Aiello, M.: Remotely exploiting AT command attacks on ZigBee networks. Secur. Commun. Netw. 1–9 (2017). https://doi.org/10.1155/2017/1723658
13. Qiu, T., Liu, X., Han, M., Li, M., Zhang, Y.: SRTS: a self-recoverable time synchronization for sensor networks of healthcare IoT. Comput. Netw. **129**, 481–492 (2017). https://doi.org/10.1016/j.comnet.2017.05.011
14. Alladi, T., Chamola, V., Sikdar, B., Choo, K.-K.R.: Consumer IoT: security vulnerability case studies and solutions. IEEE Consum. Electron. Mag. **9**(2), 17–25 (2020). https://doi.org/10.1109/mce.2019.2953740

15. Loi, F., Sivanathan, A., Gharakheili, H.H., Radford, A., Sivaraman, V.: Systematically evaluating security and privacy for consumer IoT devices. In: Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, pp. 1–6 (2017)
16. Bakhshi, Z., Balador, A., Mustafa, J.: Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models. In: 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), pp. 173–178. IEEE (2018). https://doi.org/10.1109/wcncw.2018.8368997
17. Wang, Q., Zhu, X., Ni, Y., Gu, L., Zhu, H.: Blockchain for the IoT and industrial IoT: a review. Internet Things **10**, 100081 (2020). https://doi.org/10.1016/j.iot.2019.100081
18. European Telecommunication Standards Institute: ETSI EN 303 645 "ETSI Releases World-Leading Consumer IoT Security Standard". https://www.etsi.org/newsroom/press-releases/1789-2020-06-etsi-releases-world-leading-consumer-iot-security-standard. Last accessed 27 Jan 2021
19. IGI Global: "What is System Resilience?" https://www.igi-global.com/dictionary/cyber-threats-to-critical-infrastructure-protection/51260. Last accessed 26 Jan 2021
20. Collins Dictionary.: Definition of 'Security'. https://www.collinsdictionary.com/dictionary/english/security. Last accessed 26 Jan 2021
21. Moore, A.D.: Defining privacy. J. Soc. Philos. **39**(3), 411–428 (2008)
22. Tawalbeh, L., Muheidat, F., Tawalbeh, M., Quwaider, M.: IoT privacy and security: challenges and solutions. Appl. Sci. **10**(12), 4102 (2020). https://doi.org/10.3390/app10124102
23. Nykyri, M., Kuisma, M., Karkkainen, T.J., Hallikas, J., Jappinen, J., Korpinen, K., Silventoinen, P.: IoT demonstration platform for education and research. In: IEEE 17th International Conference on Industrial Informatics (INDIN), vol. 1, pp. 1155–1162. IEEE (2019). https://doi.org/10.1109/indin41052.2019.8972280
24. Yang, H., Jiang, B., Staroswiecki, M., Zhang, Y.: Fault recoverability and fault tolerant control for a class of interconnected nonlinear systems. Automatica **54**, 49–55 (2015). https://doi.org/10.1016/j.automatica.2015.01.037
25. Gupta, A., Christie, R., Manjula, R.: Scalability in Internet of Things: features, techniques and research challenges. Int. J. Comput. Intell. Res. **13**(7), 1617–1627 (2017)
26. Tata Consultancy Services: "Build a Scalable Platform for High-Performance IoT Applications". https://www.tcs.com/content/dam/tcs/pdf/discover-tcs/Research-and-Innovation/Build_a_Scalable_Platform_pdf.pdf. Last accessed 26 Jan 2021
27. SpiceLogic Inc.: Analytic Hierarchy Process Software v2.2. https://www.spicelogic.com/Products/ahp-software-30/