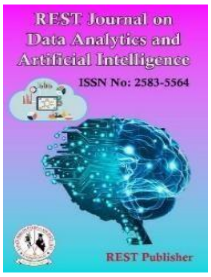
REST Journal on Data Analytics and Artificial Intelligence
Vol: 2(4), December 2023
REST Publisher; ISSN: 2583-5564
Website: http: //restpublisher.com/journals/jdaai/
DOI: https://doi.org/10.46632/jdaai/2/4/3



Security and Privacy Issues in Internet of Things (IoT) Devices Using COPRAS Method

***Sreenath Devineni, Bhargavi Gorantla**
Lead Software Engineer, USA
*Corresponding Author Email: Srinathdevineni@gmail.com

Abstract. *This paper explores various security and privacy issues inherent in IoT devices, ranging from vulnerabilities in device firmware and software to data breaches and unauthorized access. We delve into the challenges of securing IoT devices due to their resource constraints, diverse communication protocols, and often lax security practices during development. Additionally, we discuss privacy implications stemming from the collection and sharing of sensitive personal data by IoT devices, as well as the potential for surveillance and data misuse. Furthermore, we examine the implications of IoT devices in critical infrastructure and industrial systems, where security breaches can have severe consequences. Finally, we propose potential solutions and best practices to address these challenges, including robust encryption methods, regular security updates, and improved authentication mechanisms, to ensure the security and privacy of IoT devices in an increasingly connected world. The exponential growth of IoT devices across various sectors such as smart homes, healthcare, transportation, and industrial automation underscores the importance of ensuring their security and privacy. As these devices become more integrated into daily life and critical infrastructure, any vulnerability can have widespread and severe consequences. The evaluation of alternative performances through Complex Proportionality Assessment (COPRAS) requires an understanding of key criteria, exploration of options, and comparison of relevant facts. Meeting the decision-makers' desire for comparing grades involves choosing among multiple options based on predetermined competing requirements. COPRAS offer a method for such assessments in real-world scenarios, where criteria are nuanced and values cannot be quantified numerically. From the result smart thermostat got the first rank whereas wearable fitness tracker is having the lowest rank.*

***Keywords**: Internet of Things, Complex Proportionality Assessment, Radio Frequency Identification*

1. INTRODUCTION

The Internet of Things (IoT) encompasses a range o objects enhanced with electronics, software, sensors, and actuators, all interconnected via the Internet to share and collect data. These IoT devices, boasting sensors and computational capabilities, find application across various domains. Typical examples include smart homes, urban infrastructure (smart cities), energy systems (smart grids), medical devices, connected vehicles, among others. However, security and privacy concerns persist as significant challenges for IoT, introducing heightened worries regarding online privacy for users. Additionally, efforts such as Battery Life Extension and Lightweight Computing are being pursued to address these issues [1]. Fog computing emerged as a remedy for linking distant data centers to Internet of Things (IoT) gadgets. It proves to be an ideal framework for numerous IoT applications, offering advantages like heightened security, decreased bandwidth usage, and minimized latency. However, devices situated at the fringes of the Internet, known as fog devices, encounter a host of security and privacy vulnerabilities.[2] Securing IoT requires a thorough cybersecurity framework that encompasses every layer of diverse IoT systems and transcends platform boundaries. Yet, existing security measures fall short when dealing with extensive networks of varied devices and cyber-physical systems characterized by limited resources and real-time demands. Further investigation is essential to uncover and develop effective IoT security measures. These may include innovative isolation techniques capable of resisting runtime attacks, minimal trust anchors tailored for cyber-physical systems, and adaptable security protocols that can scale accordingly.[3] The Internet of Things (IoT) encompasses the vast array of physical devices worldwide that are currently connected to the internet, enabling the gathering and sharing of data. Advancements in portable communication, Wireless Sensor Networks (WSNs), and Radio Frequency Identification (RFID) have fueled the development of IoT, facilitating seamless collaboration between devices regardless of location or structure. These innovative and intelligent products hold immense potential across various applications. The primary objective of IoT is to establish intelligent environments and autonomous devices, including smart transportation, goods, cities, and living spaces. By connecting these diverse entities and equipping them with cutting-edge sensors, IoT enhances the capabilities of ordinary equipment, enabling continuous data communication without human intervention or traditional media channels. Ultimately, IoT strives to enhance our global surroundings by merging the digital and physical realms.[4] A smart grid refers to a system constructed upon advanced information and communication technology (ICT) frameworks, aimed at managing electricity in a sustainable, reliable, and efficient manner [28]. Central to the smart grid concept is the smart meter, a crucial device facilitating the monitoring of household electricity usage. It swiftly and accurately reports this data to either the utility provider, responsible for selling energy to customers, or the distribution system operator, tasked with managing and operating the grid. This process occurs at a significantly accelerated pace compared to traditional metering methods [5]. Because of the widespread presence of the Internet of Things (IoT) ecosystem, safeguarding user privacy is of utmost importance in IoT security. With interconnected devices and data transmitted over the internet, ensuring user privacy has become a major focus in numerous research inquiries. Despite significant prior investigation into privacy issues, many aspects still necessitate further exploration. Key areas such as data collection, sharing, and management, along with concerns regarding data security, persist as unresolved challenges in research [6]. The Internet of Things (IoT) brings about unforeseen security risks that were not anticipated by device manufacturers and app developers. This technology facilitates extensive data storage, analysis, monitoring, and sharing among interconnected objects and users. However, the lack of stringent control over data collection, retention, and sharing poses a significant threat to user privacy. Given the possibility of insufficient legal regulations governing IoT, there is an urgent need for legal scrutiny and potentially the introduction of new legislative measures.Producers of Internet of Things (IoT) devices often prioritize cost-cutting in production and development. Consequently, IoT gadgets typically possess constrained resources such as limited memory, energy, and bandwidth. These challenging constraints significantly impede the implementation of robust security measures, rendering traditional security techniques impractical. Moreover, certain IoT devices operate under severe energy limitations, particularly in outdoor or hostile environments. Intensive security protocols, especially those involving cryptographic algorithms, can quickly deplete the device's battery resources, hampering its intended functionality. The application layer encompasses intelligent devices that provide users with tailored services. These devices are typically simple, low-energy, and portable, making them susceptible to attacks. Malicious assaults can replace program code with flaws, causing the application to malfunction. Consequently, these applications may become compromised, shut down unexpectedly, fail to execute intended tasks, or execute authenticated services improperly. RFID technology has been implemented across various sectors such as retail, supply chain management, healthcare, transportation, and household appliances. The system comprises tags, readers, and a central server. Tags, essentially microchips with limited memory, are equipped with transponders and assigned unique identities for identification purposes. Readers, on the other hand, are devices used to communicate with RFID tags, incorporating transceivers to emit radio waves and receive responses from passive tags. The back-end server serves as a reliable repository, storing tag and reader data in its database. Numerous Internet of Things (IoT) devices are engineered for extensive deployment, exemplified by sensors. IoT implementations typically involve numerous devices with comparable attributes, which amplifies the consequences of security vulnerabilities. Likewise, various organizations have established protocols for risk assessments, indicating the unprecedented potential for interconnections among IoT devices. Moreover, many of these devices autonomously establish irregular connections with others, necessitating scrutiny of relevant security tools, strategies, and tactics [12].In cloud systems, intrusion detection methods are commonly employed to counter various types of attacks, including insider threats, flooding attacks, port scanning, and assaults on virtual machines (VMs) and hypervisors. This intrusion detection system operates by scrutinizing and overseeing access control regulations, log files, and user activity logs to identify intrusive behavior. It can be utilized within the network infrastructure to uncover malevolent activities like Denial of Service (DoS) attacks and port scanning. However, detecting rootkits becomes challenging in fog computing-based IoT devices due to their constrained computing and resource capacities. Exploiting vulnerabilities in hardware virtualization technology allows attackers to attain kernel-level privileges in specific operating systems (OS). Rootkits possess elevated privileges compared to embedded hypervisors, potentially leading to issues such as targeted system compromises or the extraction of critical data. [13]

2. MATERIALS AND METHOD

2.1. Alternative parameters: Smart Thermostat, Smart Camera, Connected Car, Wearable Fitness Tracker, Smart Lock

2.2. Evaluation parameters: Security Level, Privacy Protection, Cost, Energy Efficiency

2.3. Smart Thermostat: A smart thermostat is a device used for controlling the heating, ventilation, and air conditioning (HVAC) systems in homes and buildings. What sets it apart from traditional thermostats is its ability to connect to the internet, allowing for remote control and automation via smart phones, tablets, or computers.

2.4. Smart Camera: A smart camera, also known as an intelligent camera or IP camera, is a type of surveillance camera equipped with advanced features beyond basic video recording capabilities. These cameras are connected to the internet or a local network, enabling remote access and control.

2.5. Wearable Fitness Tracker: A wearable fitness tracker is a device designed to monitor and track various aspects of physical activity, exercise, and health metrics. These trackers are typically worn on the wrist, although some can be clipped onto clothing or worn as accessories. The primary purpose of a wearable fitness tracker is to help individuals monitor their daily activity levels and progress towards fitness goals.

2.6. Smart Lock: A smart lock is a type of locking system that utilizes wireless technology, typically Bluetooth, Wi-Fi, or Z-Wave, to enable remote control and monitoring of door locks. Unlike traditional locks that require physical keys or combinations, smart locks can be operated using smart phones, key fobs, or even voice commands through virtual assistants like Amazon Alexa or Google Assistant.

2.7. Security Level: "Security level" refers to the degree or level of security that a system, device, network, or environment possesses. It encompasses various measures and controls put in place to protect against unauthorized access, data breaches, cyber attacks, physical intrusions, and other security threats.

2.8. Privacy Protection: Privacy protection refers to the measures, practices, and regulations implemented to safeguard individuals' personal information from unauthorized access, misuse, disclosure, or exploitation.

2.9. Energy Efficiency: Energy efficiency refers to the ability of a system, device, process, or organization to achieve desired outcomes or perform tasks while minimizing the consumption of energy resources. It involves using less energy to provide the same level of service, output, or comfort, thereby reducing waste, costs, and environmental impacts associated with energy consumption.

2.10. Method: COPRAS (Complex Proportionality Assessment) stands out as a prominent approach within Multiple Criteria Decision Making (MCDM). It operates by determining the optimal solution ratio amidst a pool of feasible alternatives, juxtaposing them against a superior alternative and an inferior one. However, this method grapples with decision-making challenges, prompting researchers to explore various problem-solving techniques. Among these, the COPRAS-G technique emerges, involving the establishment of selection criteria, evaluation of linked information, and crafting methodologies to assess the fulfillment of participants' needs. Decision analysis necessitates the involvement of a Decision Maker (DM) who navigates through a set of possibilities, often with competing criteria, to arrive at a conclusive choice. Consequently, the development of the Complex Proportionality Assessment (COPRAS) method finds application, notably initiated by Lithuania in 1996, across domains like construction economics, real estate, and management. Notably, research delves into the inherent hazards associated with construction projects, employing a range of multi-objective assessment techniques. Risk assessment indices are meticulously chosen to elucidate and scrutinize the task model, accounting for national interests, aspirations, and factors impacting construction efficiency and real estate value escalation. The COPRAS method, akin to other Multiple Criteria Decision Making (MCDM) tools, prioritizes criterion weights by initially proposing a COBRAS technique, which interconnects numerous criteria for prioritizing alternatives. This approach underscores the significance of differentiating between worst and best solutions to facilitate optimal decision-making. The Cobras method is utilized to select device tools, resulting in the choice of triangular fuzzy numbers for their computational efficiency. This investigates the aims of enhancing the effectiveness of recent performance measures in TPM and COPRAS within an ambiguous context, primarily focusing on multi-criteria decision-making perspectives. Employing the "do" method, the paper's structure is as follows: Section 1 provides an overview of the problem and a review of relevant literature. Section 2 delves into the Cobras-G method and its literature review. Sections 3 and 4 delineate the core principles of the Cobras-G methodology, emphasizing its utilization through the proposed COPRAS-G approach. This intricate proportional estimation technique utilizes quantitative data framed within the Grey Systems Theory framework. The Cobras-G concept derives from applications of Grey Systems Theory in real-world decision-making contexts and time-dependent normative values. The COPRAS methodology has emerged as a prominent decision-making platform, employing ranking and selection techniques. The proposed framework's applicability has been consistently validated The evaluation of alternative performances through Complex Proportionality Assessment (COPRAS) requires an understanding of key criteria, exploration of options, and comparison of relevant facts. Meeting the decision-makers' desire for comparing grades involves choosing among multiple options based on predetermined competing requirements. COPRAS offers a method for such assessments in real-world scenarios, where criteria are nuanced and values cannot be quantified numerically.

3. RESULTS AND DISCUSSION

TABLE 1. Security and privacy issues in Internet of Things (IoT) devices

	Security Level	Privacy Protection	Cost	Energy Efficiency
Smart Thermostat	9.00	8.00	200.00	0.50
Smart Camera	8.00	7.00	180.00	0.60
Connected Car	7.00	9.00	250.00	0.40
Wearable Fitness Tracker	8.00	10.00	220.00	0.70
Smart Lock	6.00	15.00	300.00	0.50

Table 1 shows compare above values Security Level: The Smart Thermostat has the highest security level of 9.00. The Smart Camera follows with a security level of 8.00. The Connected Car has a security level of 7.00.The Wearable Fitness Tracker also has a security level of 8.00. The Smart Lock has the lowest security level of 6.00.Privacy Protection: The Wearable Fitness Tracker offers the highest level of privacy protection with a score of 10.00. The Smart Thermostat and Smart Camera both have a privacy protection score of 8.00.The Connected Car follows with a privacy protection score of 9.00.The Smart Lock has the lowest privacy protection score of 15.00.Cost: The Smart Thermostat has the lowest cost of 200.00. The Smart Camera follows with a cost of 180.00.The Wearable Fitness Tracker has a cost of 220.00. The Connected Car has a cost of 250.00.The Smart Lock is the most expensive with a cost of 300.00.Energy Efficiency: The Connected Car is the most energy-efficient with a score of 0.40. The Smart Thermostat follows with a score of 0.50. The Smart Lock and Smart Camera both have an energy efficiency score of 0.50.The Wearable Fitness Tracker is the least energy-efficient with a score of 0.70. Each device has its own strengths and weaknesses in terms of security, privacy protection, cost, and energy efficiency. For example, if privacy protection is paramount, the Wearable Fitness Tracker would be a good choice despite its higher cost and lower energy efficiency. Similarly, if cost is a major concern, the Smart Camera or Smart Thermostat might be preferable options.

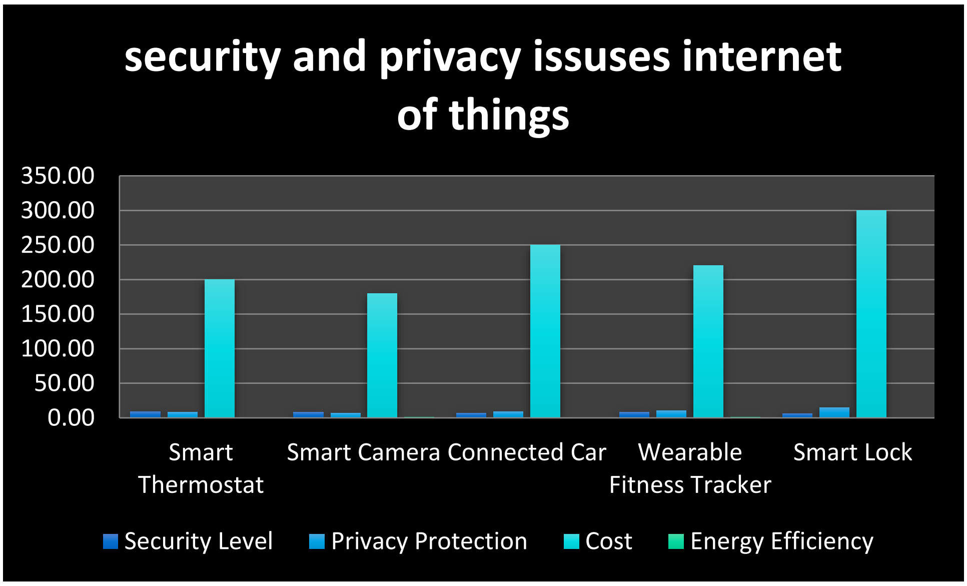


FIGURE 1. Security and privacy issues in Internet of Things (IoT) devices

Figure 1 illustrate the graphical representation of Security and privacy issues in Internet of Things (IoT) devices

TABLE 2. Normalized Data

Normalized Data			
Security Level	**Privacy Protection**	**Cost**	**Energy Efficiency**
0.2368	0.1951	0.1739	0.1852
0.2105	0.1429	0.1565	0.2222
0.1842	0.1837	0.2174	0.1481
0.2105	0.2041	0.1913	0.2593
0.1579	0.3061	0.2609	0.1852

Table 2 explains normalized data. Security Level: This column represents the security level of each IoT device, normalized to a scale between 0 and 1. A value closer to 1 indicates higher security. For example, the Smart Thermostat has a normalized security level of 0.2368, indicating that it is approximately 23.68% of the way between the lowest and highest security levels in the dataset. Privacy Protection: Similar to security level, this column represents the privacy protection level of each device, also normalized to a scale between 0 and 1. A value closer to 1 indicates higher privacy protection. For instance, the Smart Lock has a normalized privacy protection value of 0.3061, suggesting it offers the highest level of privacy protection among the devices listed. Cost: This column represents the cost of each device, normalized to a scale between 0 and 1. A value closer to 1 indicates higher cost. For instance, the Smart Camera has a normalized cost value of 0.1565, indicating it is relatively less expensive compared to other devices in the dataset. Energy Efficiency: This column represents the energy efficiency of each device, normalized to a scale between 0 and 1. A value closer to 1 indicates higher energy efficiency. For example, the Wearable Fitness Tracker has a normalized energy efficiency value of 0.2593, indicating it is relatively more energy-efficient compared to other devices.

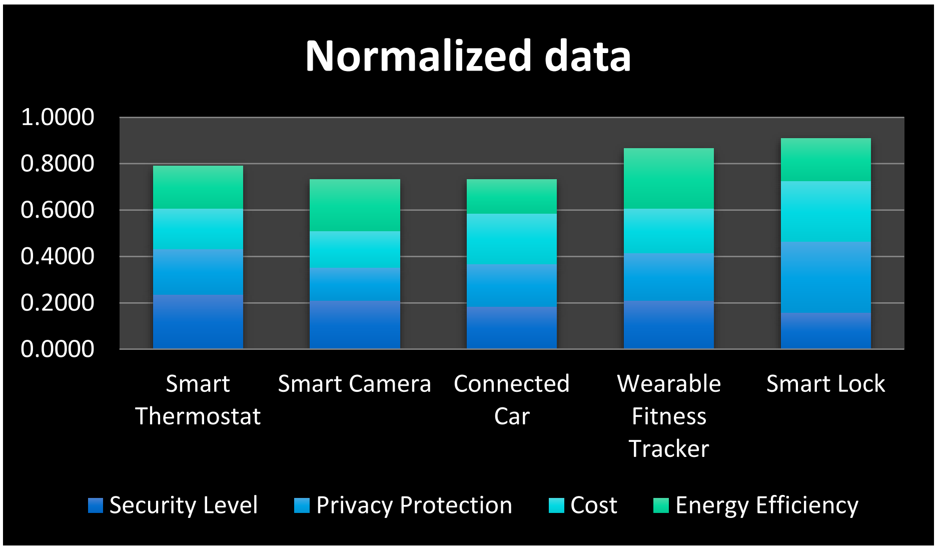


FIGURE 2. Normalized Data

Figure 2 illustrate the graphical representation of Normalized Data

TABLE 3. Weighted normalized decision matrix

Weighted normalized decision matrix			
0.06	0.05	0.04	0.05
0.05	0.04	0.04	0.06
0.05	0.05	0.05	0.04
0.05	0.05	0.05	0.06
0.04	0.08	0.07	0.05

Table 3 shows weighted normalized decision matrix. The weights and normalized scores in the matrix are used to calculate a weighted sum or weighted average for each alternative. This allows decision-makers to compare and rank the alternatives based on their overall performance, considering the relative importance of the criteria. To calculate the overall performance score for the first alternative, would multiply each criterion's score by its respective weight, and then sum the products: Overall Performance (Alternative1)=(0.02* Weight1)+(0.06* Weight2)+(0.06* Weight3)+(0.05* Weight4)

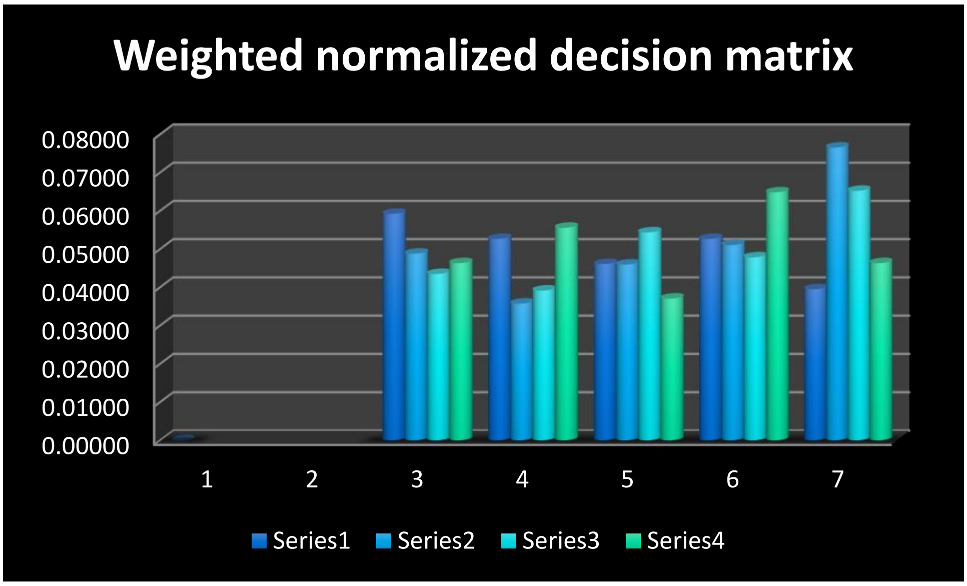


FIGURE 3. weighted normalized decision matrix

Figure 3 illustrate the graphical representation of weighted normalized decision matrix

TABLE 4. Security and privacy issues in Internet of Things (IoT) devices Bi, Ci, Min (Ci)/Ci

Bi	Ci	Min(Ci)/Ci
0.108	0.090	1.0000
0.088	0.095	0.9481
0.092	0.091	0.9824
0.104	0.113	0.7970
0.116	0.112	0.8051

Table 4 shows Bi, Ci, Min (ci\ci).This column calculates the ratio of the minimum value of Ci to Ci for each device. First, the minimum value of Ci across all devices is identified. Then, for each device, the ratio of the minimum Ci to its Ci is computed. This ratio helps to normalize the Ci values relative to the minimum Ci value across all devices. For example, for the Smart Thermostat, the minimum value of Ci is 0.090. Dividing this minimum value by the Ci value of the Smart Thermostat (0.090 / 0.090) results in 1.0000. Similarly, for the Smart Camera, the minimum value of Ci is 0.095. Dividing this minimum value by the Ci value of the Smart Camera (0.095 / 0.095) results in 0.9481. This process is repeated for each device.

TABLE 5. Final Result of Security and privacy issues in Internet of Things (IoT) devices

Qi	Ui	Rank
0.218	100.0000	1
0.193	88.3799	4
0.200	91.7712	3
0.192	87.7543	5
0.205	93.8197	2

Table 5 shows Final Result of Security and privacy issues in Internet of Things (IoT) devices qi, ui value

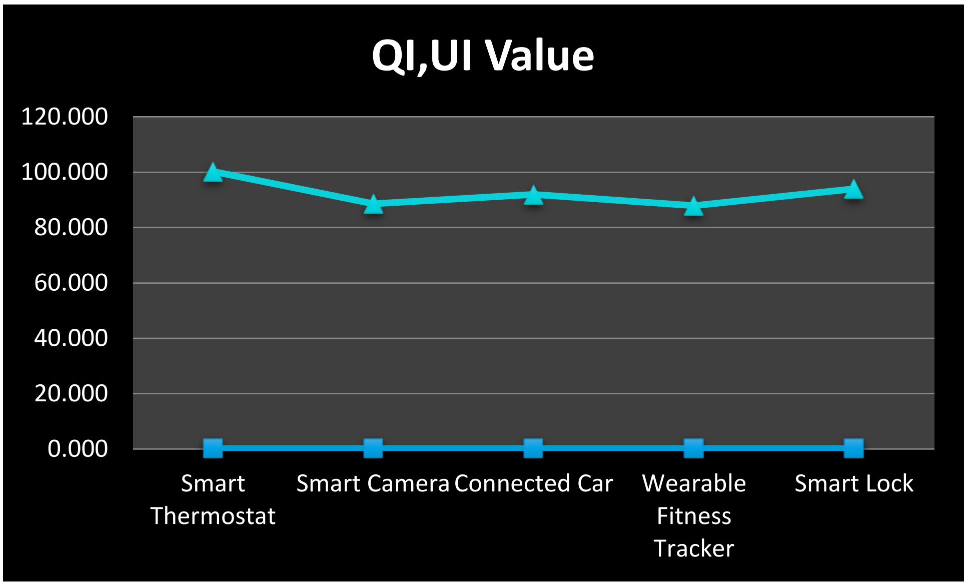


FIGURE 4. Qi, Ui value

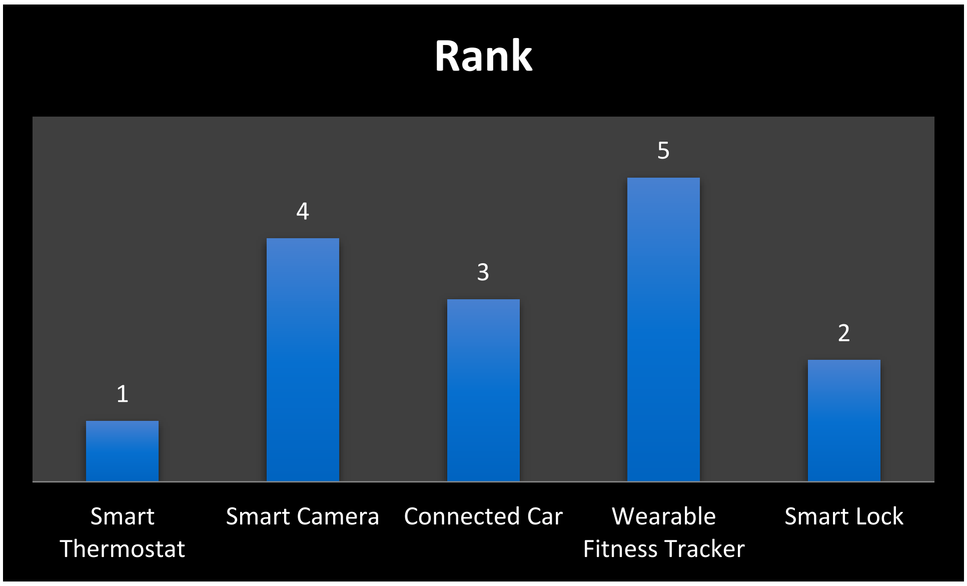


FIGURE 5. Rank

Figure 4 illustrate the graphical representation of Qi, Ui value. Figure 5 Shows ranking of Security and privacy issues in Internet of Things (IoT) devices smart thermostat is got the first rank whereas is wearable fitness tracker is having the lowest rank.

CONCLUSION

The Internet of Things (IoT) revolutionizes connectivity by embedding everyday objects with sensors and internet connectivity, enabling seamless communication and automation. However, this interconnectedness brings forth significant security and privacy challenges. IoT devices often lack robust security measures, leaving them vulnerable to cyber-attacks. Weak authentication mechanisms make unauthorized access easy, leading to data breaches and device manipulation. Moreover, inadequate encryption protocols expose sensitive information to interception and manipulation, compromising user privacy. The fragmented nature of IoT ecosystems complicates security efforts, as vulnerabilities in one device can compromise the entire network. Additionally, the lack of update mechanisms leaves devices perpetually vulnerable.

REFERENCES

[1]. Yang, Yuchen, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao. "A survey on security and privacy issues in Internet-of-Things." *IEEE Internet of things Journal* 4, no. 5 (2017): 1250-1258.

[2]. Alrawais, Arwa, Abdulrahman Alhothaily, Chunqiang Hu, and Xiuzhen Cheng. "Fog computing for the internet of things: Security and privacy issues." *IEEE Internet Computing* 21, no. 2 (2017): 34-42.

[3]. Sadeghi, Ahmad-Reza, Christian Wachsmann, and Michael Waidner. "Security and privacy challenges in industrial internet of things." In *Proceedings of the 52nd annual design automation conference*, pp. 1-6. 2015.

[4]. Bansal, Malti, Marshal Nanda, and Md Nazir Husain. "Security and privacy aspects for Internet of Things (IoT)." In *2021 6th international conference on inventive computation technologies (ICICT)*, pp. 199-204. IEEE, 2021.

[5]. Zainuddin, Naqliyah, Maslina Daud, Sabariah Ahmad, Mayasarah Maslizan, and Syafiqa Anneisa Leng Abdullah. "A study on privacy issues in internet of things (IoT)." In *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*, pp. 96-100. IEEE, 2021.

[6]. Abomhara, Mohamed, and Geir M. Køien. "Security and privacy in the Internet of Things: Current status and open issues." In *2014 international conference on privacy and security in mobile systems (PRISMS)*, pp. 1-8. IEEE, 2014.

[7]. Maras, Marie-Helen. "Internet of Things: security and privacy implications." *International Data Privacy Law* 5, no. 2 (2015): 99.

[8]. Singhai, Richa, and Rama Sushil. "An investigation of various security and privacy issues in Internet of Things." *Materials Today: Proceedings* 80 (2023): 3393-3397.

[9]. Deep, Samundra, Xi Zheng, Alireza Jolfaei, Dongjin Yu, Pouya Ostovari, and Ali Kashif Bashir. "A survey of security and privacy issues in the Internet of Things from the layered context." *Transactions on Emerging Telecommunications Technologies* 33, no. 6 (2022): e3935.

[10]. Das, Manik Lal. "Privacy and security challenges in internet of things." In *Distributed Computing and Internet Technology: 11th International Conference, ICDCIT 2015, Bhubaneswar, India, February 5-8, 2015. Proceedings 11*, pp. 33-48. Springer International Publishing, 2015.

[11]. Medaglia, Carlo Maria, and Alexandru Serbanati. "An overview of privacy and security issues in the internet of things." In *The Internet of Things: 20 th Tyrrhenian Workshop on Digital Communications*, pp. 389-395. Springer New York, 2010.

[12]. Raja, Chandrasekar, Sangeetha RajKumar, M. Ramachandran, and Manjula Selvam. "Evaluation of Landscape Design Using the Gray Relational Analysis Method."

[13]. Lee, Kanghyo, Donghyun Kim, Dongsoo Ha, Ubaidullah Rajput, and Heekuck Oh. "On security and privacy issues of fog computing supported Internet of Things environment." In *2015 6th International Conference on the Network of the Future (NOF)*, pp. 1-3. IEEE, 2015.

[14]. Yazdani, Morteza, Ali Alidoosti, and EdmundasKazimierasZavadskas. "Risk analysis of critical infrastructures using fuzzy COPRAS." Economic research-Ekonomskaistraživanja 24, no. 4 (2011): 27-40.https://doi.org/10.1080/1331677X.2011.11517478

[15]. Aghdaie, Mohammad Hasan, Sarfaraz HashemkhaniZolfani, and EdmundasKazimierasZavadskas. "Market segment evaluation and selection based on application of fuzzy AHP and COPRAS-G methods." Journal of Business Economics and Management 14, no. 1 (2013): 213-233.https://doi.org/10.3846/16111699.2012.721392

[16]. Kildienė, Simona, Arturas Kaklauskas, and EdmundasKazimierasZavadskas. "COPRAS based comparative analysis of the European country management capabilities within the construction sector in the time of crisis." Journal of Business Economics and Management 12, no. 2 (2011): 417-434.

[17]. Das, Manik Chandra, Bijan Sarkar, and Siddhartha Ray. "A framework to measure relative performance of Indian technical institutions using integrated fuzzy AHP and COPRAS methodology." Socio-Economic Planning Sciences 46, no. 3 (2012): 230-241.https://doi.org/10.1016/j.seps.2011.12.001

[18]. Dhiman, Harsh S., and Dipankar Deb. "Fuzzy TOPSIS and fuzzy COPRAS based multi-criteria decision making for hybrid wind farms." Energy 202 (2020): 117755.https://doi.org/10.1016/j.energy.2020.117755

[19]. Fouladgar, Mohammad Majid, Abdolreza Yazdani-Chamzini, Ali Lashgari, EdmundasKazimierasZavadskas, and ZenonasTurskis. "Maintenance strategy selection using AHP and COPRAS under fuzzy environment." International journal of strategic property management 16, no. 1 (2012): 85-104.https://doi.org/10.3846/1648715X.2012.666657

[20]. TuranogluBekar, Ebru, Mehmet Cakmakci, and Cengiz Kahraman. "Fuzzy COPRAS method for performance measurement in total productive maintenance: a comparative analysis." Journal of Business Economics and Management 17, no. 5 (2016): 663-684.https://doi.org/10.3846/16111699.2016.1202314

[21]. Zolfani, Sarfaraz Hashemkhani, Nahid Rezaeiniya, Mohammad Hasan Aghdaie, and EdmundasKazimierasZavadskas. "Quality control manager selection based on AHP-COPRAS-G methods: a case in Iran." Economic research-Ekonomskaistraživanja 25, no. 1 (2012): 72-86.https://doi.org/10.1080/1331677X.2012.11517495

[22]. Tavana, Madjid, Ehsan Momeni, Nahid Rezaeiniya, Seyed Mostafa Mirhedayatian, and Hamidreza Rezaeiniya. "A novel hybrid social media platform selection model using fuzzy ANP and COPRAS-G." Expert Systems with Applications 40, no. 14 (2013): 5694-5702.https://doi.org/10.1016/j.eswa.2013.05.015

[23]. Kouchaksaraei, RamtinHaghnazar, Sarfaraz HashemkhaniZolfani, and Mahmood Golabchi. "Glasshouse locating based on SWARA-COPRAS approach." International Journal of Strategic Property Management 19, no. 2 (2015): 111-122.https://doi.org/10.3846/1648715X.2015.1004565