Evaluating Food Order Industry Performance Using the COPRAS Method: A Multi-Criteria Decision-Making Approach

*Chandrasekar Raja, Chinnasami Sivaji, M. Ramachandran, Ramya Sharma
REST Labs, Kaveripattinam, Krishnagiri, Tamil Nadu, India.
*Corresponding Author Email: chandrasekarrajarsri@gmail.com

Abstract. *Technology advancement and reliance on the Internet have opened up new opportunities for mobile application marketing in India. There are 15 to 50 billion active websites on the Internet, according to Worldwidewebsize.com. Many conventional methods of product promotion and sales have been rendered obsolete by these websites and apps. The creation of mobile applications, which use the Internet as a medium to advertise goods and services, is the result of collaboration between marketing intelligence and technology. Customers and corporate organizations view the goods and services on the market today with modern eyes. Online marketing is the foundation of marketing tactics that are tailored to today's consumers. This essay examines how people perceive ordering food through online food delivery services while taking advantage of online services. Different businesses have been altered by digital technology to differing degrees, and frequent technology use has made people constantly connected to the internet. Customers can quickly place orders using an online food ordering system based on their preferences. The major goal of this study is to identify the elements that affect consumers' opinions on online food delivery services offered by Pizza Hut, KFC, Dominos, Swiggy, and Zomato. In order to gather a sample from the 167 respondents, the researcher employed descriptive research and a convenience sampling technique. The variables and items were tested with the WSM approach. The purpose of the study was to identify the factors that affect consumers' perceptions of online food services. The findings indicate that the majority of the customers are young people, and that frequent social media events and negative past experiences are among the factors that have an impact on their perception.*

1. INTRODUCTION

The Internet of Things (IoT) encompasses a 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 COBRA'S 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.
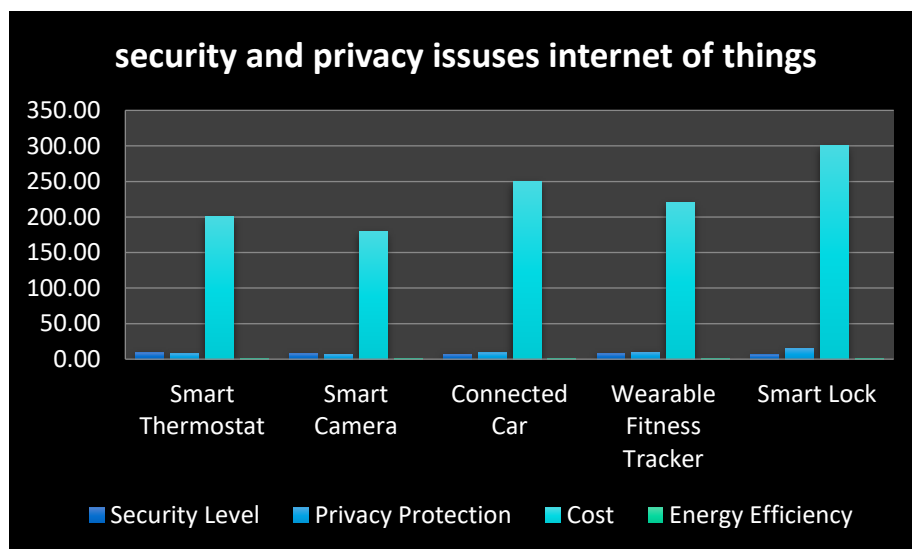

FIGURE 1. Security and privacy issues in Internet of Things (IoT) devices

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.
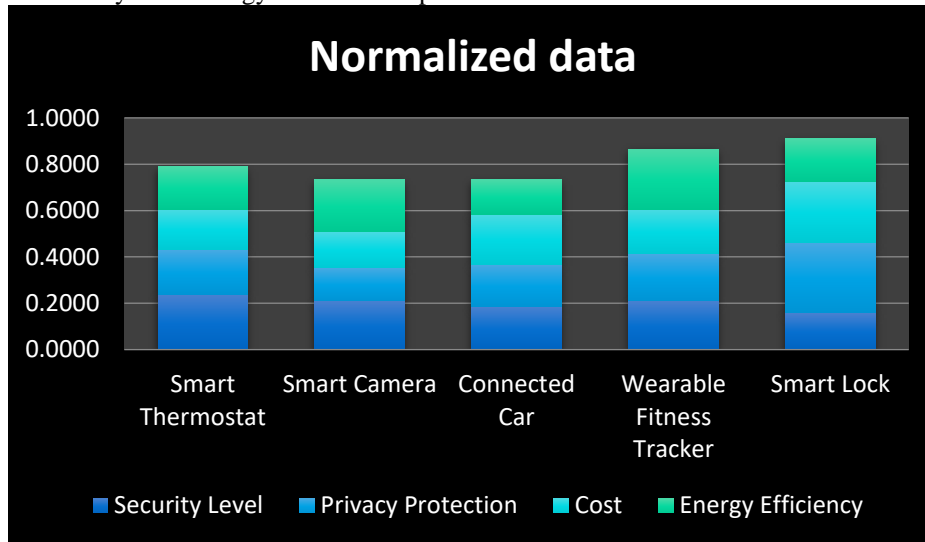

FIGURE 2. Normalized Data

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)
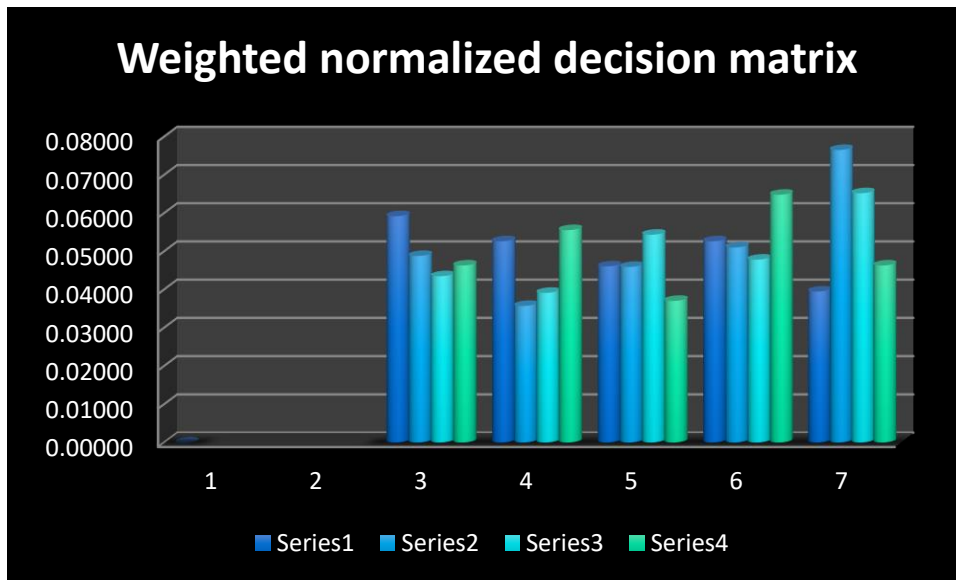
FIGURE 3. weighted normalized decision matrix

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
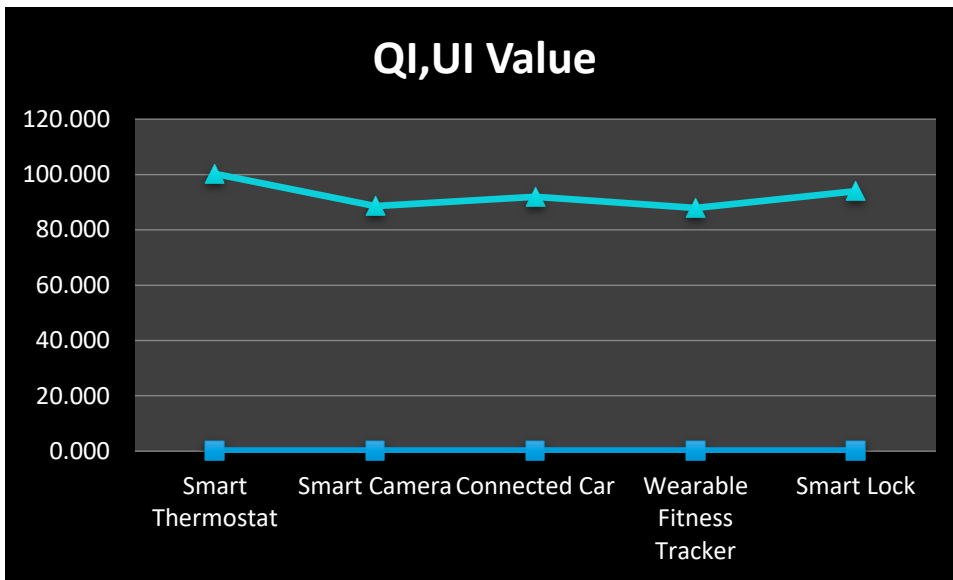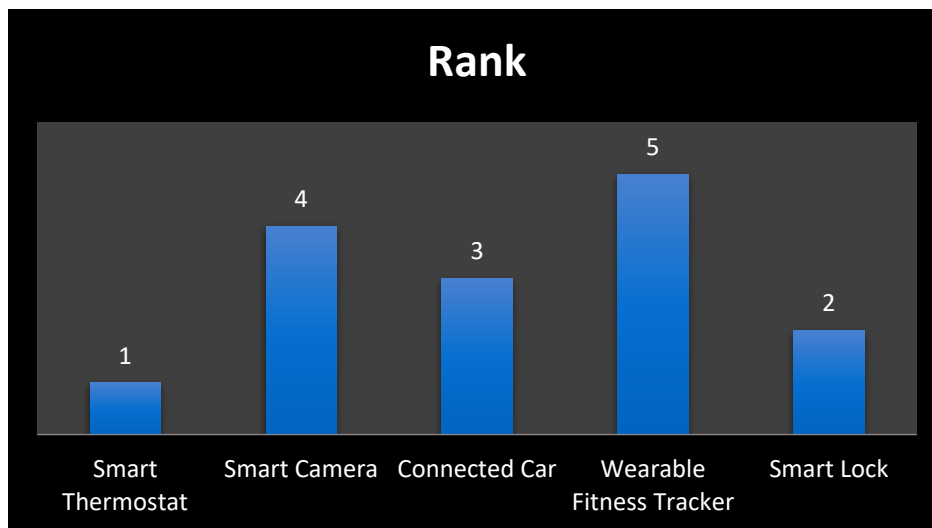
FIGURE 4. Qi, Ui value

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.

4. 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]. Somasundaram, T., V. G. Jisha, R. Rupashree, and A. J. Excelce. "Changes in customer perceptions towards online food ordering services through food apps (Swiggy&Zomato): An empirical study." In *AIP Conference Proceedings*, vol. 2393, no. 1, p. 020032. AIP Publishing LLC, 2022.

[2]. Sengupta, Mousumi, Nilanjan Sengupta, and Suma Raghupathi. "A Case Study on Pizza Hut: Competitors' Envy, Consumers' Choice." (2012).

[3]. Mondurailingam, M., V. Jeyaseelan, and A. K. Subramani. "Comparative study on customer satisfaction towards KFC and McDonalds, Chennai." *ZENITH International Journal of Multidisciplinary Research* 5, no. 6 (2015): 50-62.

[4]. Shanmugasundar, G., R. Sivaramakrishnan, R. Sridhar, and M. Rajmohan. "Computer aided modelling and static analysis of an inspection robot." *Applied Mechanics and Materials* 766 (2015): 1055-1060.

[5]. Mike, Barry, and J. W. Slocum. "Changing Culture at Pizza Hut and Yum! Brands, Inc." *Organizational Dynamics* 32 (2003): 319-330.

[6]. Kimes, Sheryl E., and Philipp Laque. "Online, mobile, and text food ordering in the US restaurant industry." (2011).

[7]. Tobing, Roy Deddy Hasiholan. "A food ordering system with delivery routing optimization using global positioning system (GPS) technology and google maps." *Internetworking Indonesia Journal* 8, no. 1 (2016): 17-21.

[8]. Shanmugasundar, G., R. Sivaramakrishnan, R. Sridhar, and M. Rajmohan. "Computer aided modelling and static analysis of an inspection robot." *Applied Mechanics and Materials* 766 (2015): 1055-1060.

[9]. Hongzhen, X. U., Tang Bin, and Song Wenlin. "Wireless food ordering system based on web services." In *2009 Second International Conference on Intelligent Computation Technology and Automation*, vol. 4, pp. 475-478. IEEE, 2009.

[10]. Das, Jyotishman. "Consumer perception towards "online food ordering and delivery services": an empirical study." *Journal of Management (JOM)* 5, no. 5 (2018): 155-163.

[11]. Zulkarnain, Kedah, Haque Ahasanul, and Ahmed Selim. "Key success factors of online food ordering services: An empirical study." *Malaysian institute of Management* 50, no. 2 (2015): 19-36.

[12]. Alagoz, Serhat Murat, and Haluk Hekimoglu. "A study on TAM: Analysis of customer attitudes in online food ordering system." *Procedia-Social and Behavioral Sciences* 62 (2012): 1138-1143.

[13]. Shanmugasundar, G., Tapan K. Mahanta, Robert Čep, and Kanak Kalita. "Novel fuzzy measurement alternatives and ranking according to the compromise solution-based green machining optimization." *Processes* 10, no. 12 (2022): 2645.

[14]. Hatim, Shahirah Mohamed, Nur Azmina Mohamad Zamani, Lily Marlia Abdul Latif, Mahani Ahmadkardri Normah Ahmad, and Norhaslinda Kamaruddin Azham Hussain. "E-FoodCart: An Online Food Ordering Service." *Shahirah Mohamed Hatim* 8, no. 4 (2019).

[15]. Sunitha, R. "Work life balance of women employees of teaching faculties in karnataka state." *Journal of Management and Science* 10, no. 4 (2020): 40-42.

[16]. Shanmugasundar, G., R. Sivaramakrishnan, and M. Rajmohan. "Computer aided simulation for workspace plot of a newly designed inspection robot." In *2014 IEEE International Conference on Computational Intelligence and Computing Research*, pp. 1-6. IEEE, 2014.

[17]. Raina, Ashish, Varinder Singh Rana, and Arun Singh Thakur. "Popularity of online food ordering and delivery services-a comparative study between Zomato, Swiggy and Uber eats in Ludhiana." *International Journal of Management, Technology and Engineering* 9, no. 3 (2019): 6080-6088.

[18]. Hsiao, Kuo-Lun, and Chia-Chen Chen. "What drives continuance intention to use a food-ordering chatbot? An examination of trust and satisfaction." *Library Hi Tech* (2021).

[19]. Rao, Ch Maheswara, and K. Venkatasubbaiah. "Application of WSM, WPM and TOPSIS Methods for the Optimization of Multiple Responses." *International journal of hybrid information technology* 9, no. 10 (2016): 59-72.

[20]. Shanmugasundar, G., Gaurav Sapkota, Robert Čep, and Kanak Kalita. "Application of MEREC in multi-criteria selection of optimal spray-painting robot." *Processes* 10, no. 6 (2022): 1172.

[21]. Sahabuddin, Md, and Imran Khan. "Multi-criteria decision analysis methods for energy sector's sustainability assessment: Robustness analysis through criteria weight change." *Sustainable Energy Technologies and Assessments* 47 (2021): 101380.

[22]. Vimala Saravanan, M. Ramachandran, Manjula Selvam, Chandrasekar Raja, "Application of the EDAS Technique for Selecting the Electric Motor Vehicles", Journal on Electronic and Automation Engineering, 2(4), December 2023, 27-36.

[23]. Gao, Jianqiang, Binbin Wang, Ziyi Wang, Yufeng Wang, and Fanzhi Kong. "A wavelet transform-based image segmentation method." *Optik* 208 (2020): 164123.

[24]. Findawati, Yulian, Nadifatul Qomariyah, Arif Senja Fitroni, and Dahlan Abdullah. "Decision support system for Islamic couple selection using fuzzy-AHP and WSM method-based web." In *MATEC web of conferences*, vol. 197, p. 15009. EDP Sciences, 2018.

[25]. Ponnada, Venkata Tulasiramu, and SV Naga Srinivasu. "Efficient CNN for lung cancer detection." *Int J Recent Technol Eng* 8, no. 2 (2019): 3499-505.

[26]. Kumar, Krishna, Ravindra Pratap Singh, Prashant Ranjan, and Narendra Kumar. "Daily plant load analysis of a hydropower plant using machine learning." In *Applications of Artificial Intelligence in Engineering: Proceedings of First Global Conference on Artificial Intelligence and Applications (GCAIA 2020)*, pp. 819-826. Springer Singapore, 2021.

[27]. Krishnan, G. Sai, G. Shanmugasundar, M. Vanitha, S. Srinivasan, and G. Suresh. "Investigation on the Mechanical and Morphological Properties of Red banana/Ramie Fiber vinyl ester composites." In *IOP Conference Series: Materials Science and Engineering*, vol. 961, no. 1, p. 012015. IOP Publishing, 2020.

[28]. Naufal, Ammar, Amelia Kurniawati, and Muhammad Azani Hasibuan. "Decision support system of SMB telkom university roadshow location prioritization with weighted sum model method." In *2016 2nd International Conference of Industrial, Mechanical, Electrical, and Chemical Engineering (ICIMECE)*, pp. 107-111. IEEE, 2016.

[29]. Chourabi, Zouhour, Faouzi Khedher, Amel Babay, and Morched Cheikhrouhou. "Multi-criteria decision making in workforce choice using AHP, WSM and WPM." *The Journal of The Textile Institute* 110, no. 7 (2019): 1092-1101.

[30]. Jaganathan Rajamanickam, M. Ramachandran, Ramya sharma, Chinnasami Sivaji, "Distributed Generation (DG) system using COPRAS method", REST Journal on Advances in Mechanical Engineering, 2(3) September 2023, 11-22.

[31]. Mandala, V., and S. N. R. D. Surabhi. "Integration of AI-Driven Predictive Analytics into Connected Car Platforms. IARJSET, 7 (12)." (2020).

[32]. Sunitha, R. "A study on competency mapping scale to map the competencies of university teachers (with special reference to karnataka state)." *South Asian Journal of Engineering and Technology* 11, no. 1 (2021): 1-3.

[33]. Feng, L., T. D. Bui, and Yuan Yan Tang. "Classification of similar 2-D objects by wavelet-sparse-matrix (WSM) method." *International journal of pattern recognition and artificial intelligence* 15, no. 02 (2001): 329-345.

[34]. Suneja, Bhavesh, Ashish Negi, Narendra Kumar, and Rishav Bhardwaj. "Cloud-based tomato plant growth and health monitoring system using IOT." In *2022 3rd International Conference on Intelligent Engineering and Management (ICIEM)*, pp. 237-243. IEEE, 2022.

[35]. Ponnada, Venkata Tulasiramu, and SV Naga Srinivasu. "Integrated clinician decision supporting system for pneumonia and lung cancer detection." *International Journal of Innovative Technology and Exploring Engineering (IJITEE)* (2019).

[36]. Shanmugasundar, G., and R. Sivaramakrishnan. "Software Development for an Inverse Kinematics of Seven-Degrees of Freedom Newly Designed Articulated Inspection Robot." *International Journal of Computer Applications* 975 (2012): 8887.

[37]. Mandala, Vishwanadham. "Predictive Failure Analytics in Critical Automotive Applications: Enhancing Reliability and Safety through Advanced AI Techniques." *Journal of Artificial Intelligence and Big Data* (2024): 48-60.

[38]. Mandala, Vishwanadham. "Towards a Resilient Automotive Industry: AI-Driven Strategies for Predictive Maintenance and Supply Chain Optimization."

[39]. Jadhav, Anil, and Rajendra Sonar. "Analytic hierarchy process (AHP), weighted scoring method (WSM), and hybrid knowledge-based system (HKBS) for software selection: a comparative study." In *2009 Second International Conference on Emerging Trends in Engineering & Technology*, pp. 991-997. IEEE, 2009.

[40]. Surabhi, Srinivas Naveen D., Chirag Shah, Vishwanadh Mandala, and Priyank Shah. "Range Prediction based on Battery Degradation and Vehicle Mileage for Battery Electric Vehicles." *International Journal of Science and Research* 13 (2024): 952-958.

[41]. Kurinjimalar Ramu, M. Ramachandran, Ramya sharma, Prabakaran Nanjundan, "Urban Agriculture Overview of Sustainability Using GRA Methodology", Building Materials and Engineering Structures, 2(3), September 2023, 7-14.

[42]. Shukla, Hari Shanker, Narendra Kumar, and Rakesh Prakash Tripathi. "Image restoration using modified binary particle Swarm Optimization Richardson-Lucy (MBSO-RL) algorithm." *Int. J. Appl. Eng. Res* 10, no. 22 (2015): 43077-43081.

[43]. Ponnada, Venkata Tulasiramu, and SV Naga Srinivasu. "End to End System for Pneumonia and Lung Cancer Detection using Deep Learning." *Int. J. Eng. Adv. Technol* 8 (2019).

[44]. Raibagi, Tejas, Ashwin Vishwakarma, Jahnavi Naik, Rujata Chaudhari, and Geetanjali Kalme. "Orderista-AI-based Food Ordering Application." In *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, pp. 34-37. IEEE, 2021.

[45]. Kimes, Sheryl E. "The current state of online food ordering in the US restaurant industry." (2011).

[46]. Kumar, Nishant. "Service quality and behavioral intention: the mediating effect of satisfaction in online food ordering services." In *e-journal-First Pan IIT International Management Conference–2018*. 2020.

[47]. Sunitha, R., and J. K. Raju. "RISK MANAGEMENT IN BANKING SECTOR--AN DESCRIPTIVE STUDY." (2013).

[48]. Sharma, Abhishek, and Naredra Kumar. "Encryption of text using fingerprints as input to various algorithms." *Int. J. Sci. Res* 3, no. 4 (2014): 418-421.

[49]. Mandala, Vishwanadham, Srinivas Naveen Reddy Dolu Surabhi, Phani Durga Nanda Kishore Kommisetty, Bala Maruthi Subba Rao Kuppala, and Roopak Ingole. "Towards Carbon-Free Automotive Futures: Leveraging AI And ML For Sustainable Transformation." *Educational Administration: Theory and Practice* 30, no. 5 (2024): 3485-3497.

[50]. Fuladipanah, Mehdi, H. Md Azamathulla, Ozgur Kisi, Mehdi Kouhdaragh, and Vishwandham Mandala. "Quantitative forecasting of bed sediment load in river engineering: an investigation into machine learning methodologies for complex phenomena." *Water Supply* 24, no. 2 (2024): 585-600.

[51]. SHIPMAN, Zehra Dilistan. "Understanding online food ordering: How the process results in satisfaction of the customers." *Beykoz Akademi Dergisi* 7, no. 2 (2019): 81-90.

[52]. Chandrasekar Raja, M. Ramachandran, Prabakaran Nanjundan, Manjula Selvam, "Analyzing Power Systems and Power Electronics Interdependencies: A DEMATEL Method Approach", Building Materials and Engineering Structures 1(4), December 2023, 10-21.

[53]. Ponnada, Venkata Tulasiramu, and SV Naga Srinivasu. "Edge AI system for pneumonia and lung cancer detection." *Int J Innov Technol Exploring Eng* 8, no. 9 (2019).

[54]. Kumar, Krishna, Rachna Shah, Narendra Kumar, and Ravindra Pratap Singh. "Application of Robotic Process Automation." In *Applications of Artificial Intelligence in Engineering: Proceedings of First Global Conference on Artificial Intelligence and Applications (GCAIA 2020)*, pp. 929-937. Springer Singapore, 2021.

[55]. Surabhi, Srinivas Naveen D., Chirag Vinalbhai Shah, Vishwanadh Mandala, and Priyank Shah. "Advancing Faux Image Detection: A Hybrid Approach Combining Deep Learning and Data Mining Techniques." *International Journal of Science and Research (IJSR)* 13 (2024): 959-963.