National Journal of Antennas and Propagation, ISSN: 2582-2659 Vol. 7, No. 1, 2025 (pp. 8-14)
RESEARCH ARTICLE
WWW.ANTENNAJOURNAL.COM

Design and Implementation of An Rfid-Based Smart Home Automation System Using Iot and Cloud Computing

Dev Ras Pandey[1], Kapesh Subhash Raghatate[2], Seema Pant[3*]
[1]Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India.
[2]Research Scholar, Department of CS & IT, Kalinga University, Raipur, India.
[3]Assistant Professor, New Delhi Institute of Management, New Delhi, India.

KEYWORDS:
RFID,
Home Automation,
Cloud computing,
Security,
IOT.

ARTICLE HISTORY:
Received 11.01.2025
Revised 03-02-2025
Accepted 14-03-2025

DOI:
https://doi.org/10.31838/NJAP/07.01.02

Abstract

In recent years, home automation has become more popular. Since IoT technology is constantly developing, everything is now controlled by it. Smarter and more sophisticated home automation solutions have been developed. The appliances must be completely automated with no user input at all in order to improve the quality of life. This makes it possible for the end user to engage with the appliances without any hassles. Without actually touching a button, the appliances understand and respond to the user's needs. In addition to being more challenging to manage, wired sensor systems necessitate extensive wiring of the sensors at various places. As a result, wireless sensor nodes have become increasingly important and are essential to the effective deployment of home automation. One of the major benefits of automating household appliances is energy conservation. Therefore, the consumer needs to be informed about how much energy the automated appliances use. In a developing nation like India, where people lead hectic lives, it is crucial to provide comfortable, cost-effective energy-saving solutions with increased efficiency. Due to recent security breaches in many homes, home security must contain certain items. A secure living can occur in the home if various security features are accessible. Public attention and worry have been sparked by recent publications on IoT and smart homes, which have significant security issues. Security in smart homes is just as important as it is in any other computing systems to ensure that data is not lost, altered, or accessed without authorisation. It goes without saying that with traditional residences, an intruder can only threaten or steal a home if they are physically present in the neighbourhood. However, when a home is connected to the Internet, an attacker or intruder can use the Internet to access and control the property from anywhere in the globe at any time, monitoring the occupants of the home via connected cameras.

Author's e-mail: ku.devraspandey@kalingauniversity.ac.in, India.kapesh.kumar.nayak@kalingauniversity.ac.in, seema.pant@ndimdelhi.org

Corresponding Author's Orcid id: 0009-0004-4161-2369, 0009-0007-9036-1983, 0009-0000-9638-5619

How to cite th is article: Pandey DR, Raghatate KS, Pant S, Design and Implementation of An Rfid-Based Smart Home Automation System Using Iot and Cloud Computing, National Journal of Antennas and Propagation, Vol. 7, No.1, 2025 (pp. 8-14).

Introduction

One area of computing that deals with the distribution or delivery of computer services through the Internet is called cloud computing. The vast majority of individuals on the planet nowadays often employ cloud computing-based services to fulfil their own demands. Software developments have pushed businesses to choose a quick, safe, and expandable IT infrastructure in order to meet today's demands.[1] The personal property development industry typically has difficulties that must be carefully managed to meet the increasing demands. Large sums of money are typically spent on staffing, administrative know-how, and the expanding

requirements of IT infrastructure. These disadvantages often cause organisations to shift their attention away from their primary areas of business and instead focus more on these responsibilities. Managing a cloud's resources can be difficult because cloud computing generally focusses more on representing complex, large-scale, heterogeneous distributed systems. Because of this intricacy, they are compelled to rely on an automated and integrated intelligent approach for effectively allocating their resources; these dependencies allow them to provide services that seem safe, dependable, and economical. As a result, cloud computing is seen as a method that provides enterprises with a number of different advantages. Reliefs that are either immediate or long-term in nature help to reduce costs without taking location independence into account. Without taking into account the associated costs, it is impossible to enjoy the aforementioned benefits; therefore, a number of issues, including security, privacy, availability, performance, and integrity, compromise the disadvantages.[2] Regarding cloud-based solutions, it is required that they incorporate appropriate testing methods to guarantee the confidentiality and integrity of the relevant data; this ensures that the integrated solutions meet the needs of the business they are meant to support (figure 1). Finding the advantages of a cloud computing solution and confirming the issues of an appropriate testing strategy that can assist in assessing the overall potential of an application or investment under consideration are the goals of an automated technique. Thus, cloud computing is currently seen as the biggest trend in the field of computing infrastructure. It is thought to be a far more inclusive word that includes little to no centralised infrastructure. When loosely coupled data centres collaborate, they can achieve higher utilisation levels. Through virtualisation or thin clients via the "Cloud," these integrations carry out a similar function of displaying GUI interfaces to users (Figure 1).[3]

Background of the Study

Automatic identification systems, such as optical barcode readers, serve as the foundation for the architecture of radio frequency identifier technology. In an optical barcode system, a barcode reader—also known as a barcode scanner—allows users to retrieve product information. The system at the cash counter has a reader attached to it in the optical barcode architecture.[4] Product type and manufacturer information can be found on the barcode label. It has no information regarding the product's cost. This reader transfers the information to the system's backend after reading the data from the label, which is made up of vertical lines

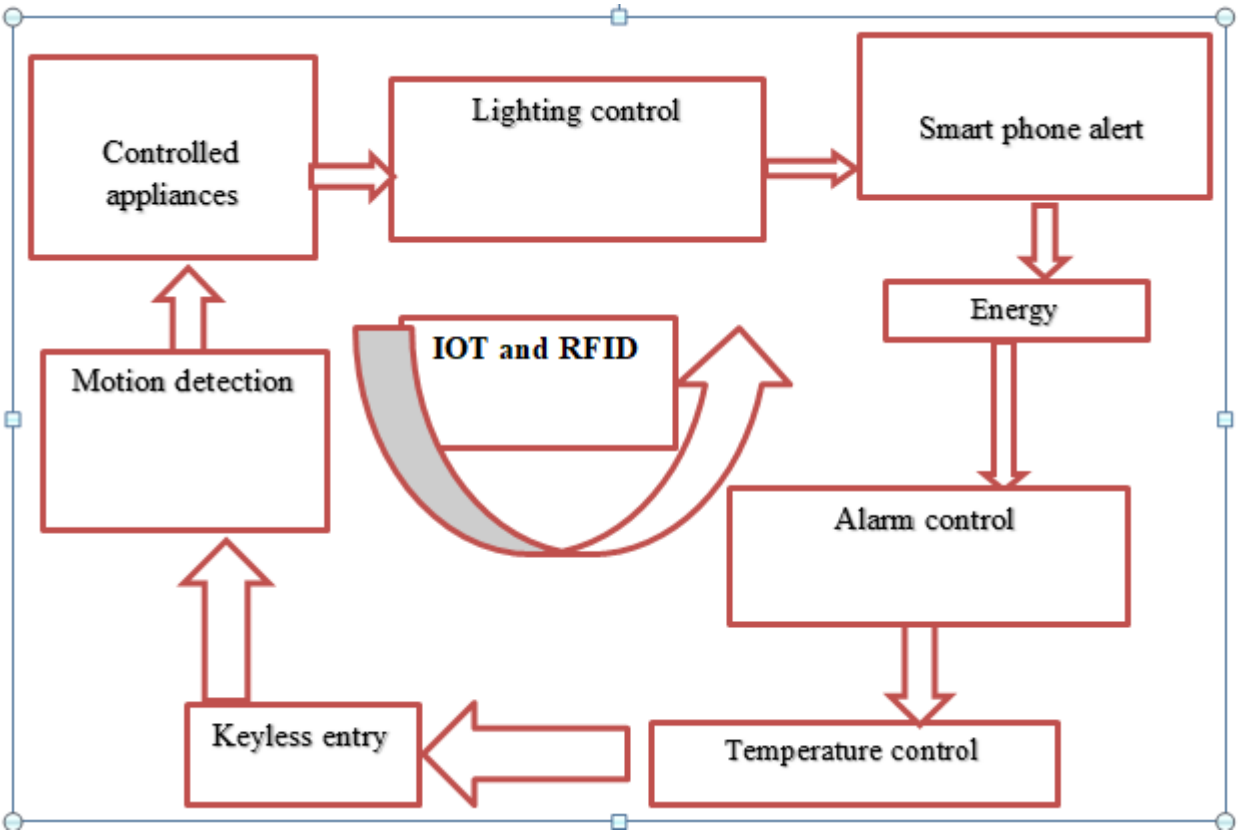

Fig. 1: IOT in smart home

with varying widths. Information about the product is kept in a database. The system that is located at the cash counter then receives the price information. Radio waves are the basis of radio frequency identification technology. The rate of vibration between 3 Hz and 300 GHz is known as the radio frequency. It corresponds to the frequencies of radio waves and other currents that transport radio signals. Electric oscillations are known as radio frequencies. The rate of oscillation is referred to as radio frequency. Radio is a synonym for radio frequency. Since more people are using computers and mobile devices in all relevant fields, data storage is one of the most important factors to take into account in today's communication world. According to their research, a vast variety of large and small business industries are expanding quickly today, and they are spending a significant amount of money to stay the same. This demand has forced them to rely on the necessity of a robust storage hub and extremely strong IT support. However, not many companies can afford this significant investment in backup support services and IT infrastructure.[5]

Cloud computing appears to be the most economical option for individuals who are unable to pay for such costs. This technique is a better choice for a few very large corporate industries because of features like reduced maintenance costs, computing efficiency, and effectiveness in the areas of data storage. Utilising cloud computing solutions significantly reduces the amount of hardware and software combinational models that users need. A well-known fact is that we have all used cloud computing-based services at some point. Some of the common cloud services include the well-known mail services like Gmail, Hot Mail, or Yahoo, among others. The users here must be able to operate the cloud computing systems interface software, which seems as easy as using a Web browser. The cloud network handles the entire process. When using the email service, a user is supposed to make sure that their data is stored on the cloud server rather than on a computer. It is impossible to see the underlying methodology and architecture that make up the cloud's backbone [6]. It doesn't matter if the cloud services are built on PHP, XML, Ruby, HTTP, or other similar technologies as long as they are functional and easy to use. By utilising scarce resources, cloud computing techniques may effectively run micro-level firms and enable even small businesses to access technology that were previously unattainable. Small firms can simply turn maintenance costs into earnings with the use of cloud computing solutions. For instance, in an in-house IT server, users may be required to concentrate more on its functioning and ensure the absence of errors in the system so that it operates smoothly. Hence the need for an effective and efficient operation of the system without any flaws, this shows that an increased volume of time and money is to be invested for a high success rate. As far as the technical faults and complications are concerned, the service provider would be completely held responsible in cloud computing.

Overview of Home Automation Systems and Applications Framework

The world is currently transitioning to an automated environment, with the majority of systems in homes, businesses, and automobiles being automated. One such improvement and innovation in mechanisation processes is the home automation system, which combines human labour with machinery to operate different kinds of loads in home systems. Numerous technologies and controllers via PCs, laptops, smartphones, and tablets would automatically operate the household appliances.[7]

Home Automation System

By making them easily accessible, a home automation system simplifies the use of a large number of household appliances. These technologies typically result in significant operational energy savings. These days, energy-saving techniques in building or home automation systems make living incredibly easy and comfortable. This system includes characteristics that allow all electrical and electronic gadgets in houses to be controlled automatically. Wireless communications can also be used to remotely control these items. This system can be used to centrally control all of the equipment used in the home, including kitchen appliances, air conditioning and heating systems, audio/video systems, security systems, and lighting equipment. For its applications, this system primarily uses actuators, sensors, and control devices. The primary controlling device would receive the sensed data from the sensors, which can detect light, motion, temperature, and other sensing aspects. These sensors can be classified as photodetectors, level sensors, pressure sensors, current transformers, infrared sensors, thermocouples or thermistors, and more [11]. Generally speaking, these sensors need specific extra signal conditioning devices in order to communicate with the primary controller. Devices like programmable logic controllers, which have been shown to receive data from sensor devices and use the built-in programs to control the actuators, would be connected to controllers like smartphones, touchpads, and personal computers/ laptops. Program changes may be experienced depending on the load activities. The programmable controller

can be used to connect several kinds of sensors and actuators via their input and output modules. Various different controlling mechanisms would be included in the duty of managing the home equipment in addition to actuators, which have been observed as the final controlling devices. These actuators include switches, relays, and motors. When it comes to these systems' remote access capabilities, communication is crucial to effectively managing the operations. This smart home system's ability to continuously monitor the concerned environment or equipment through video surveillance using cameras, scheduling, and energy-saving features is another noteworthy feature. This feature makes it possible for the elderly and disabled to confidently and easily operate various systems or pieces of equipment.

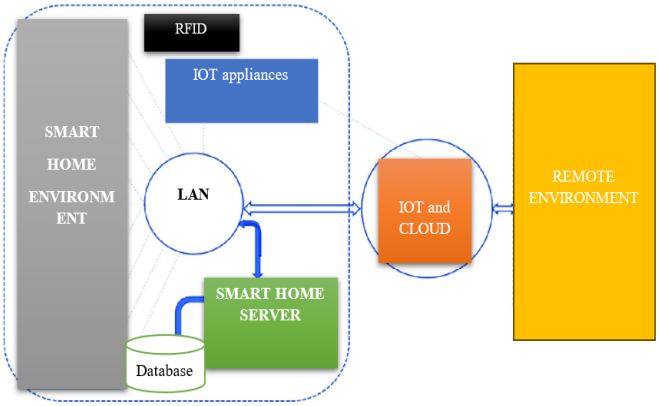

Fig. 2: Proposed System 1 Architecture for Secured Data Output

Nowadays, it's normal practice for people to access data via the internet utilising simple devices from anywhere at any time. To change the controlling parameters of sources from adjacent locations with the least amount of power consumption, online services and the Internet of Things have been used. Many residences may eventually be made up of different amenities that have been linked to resource observers. With the help of the cloud computing (CC) community, a mix of these services supports the emerging field of intelligent homes. The improvised resources might be used to calculate the same functions as on the home field. To control the power application that increases the utilisation of various home equipment, for instance, consumers gather the benefits from services.[9] The primary goal of smart metering is to improve environmental efficiency by dividing household data among designated facilities that track power usage. According to Lakshmanaprabu et al. (2019), the primary focus is on striking a balance between the development of the house manage dashboard approach for isolating people with algorithms to share the home energy details with alternate communities encased in eco-efficiency. The primary use of smart homes is in computer techniques for different areas of the home environment. The creation of smart home environments incorporates the most up-to-date information from the best-reviewed IoT studies (Sukhpal et al., 2019). The deployment of network tools capable of applying the house appliances is one of the usual characteristics of a smart home. According to Perumal et al. (2008), this method divides the search process into device-specific categories such as energy control, digital entertainment, assistive computing, home security, and device administration. The home field's supported living or health care has been successfully determined through the application of obtained results. The major focus of the found outcome is stable remote health observation at the lowest possible cost. Therefore, a variety of models support earlier applications of pre-date web services by an organised vendor that should be specialised in health care applications. Common models are supported with living applications, particularly with the integration of these approaches (Wang et al., 2006). The implementation of extensive Smart Home standards across several domains is connected to an impressive dependent networking technique via the internet. The optimal sample for the Radio Frequency Identification (RFID) technology may be examined in the context of wireless networks.

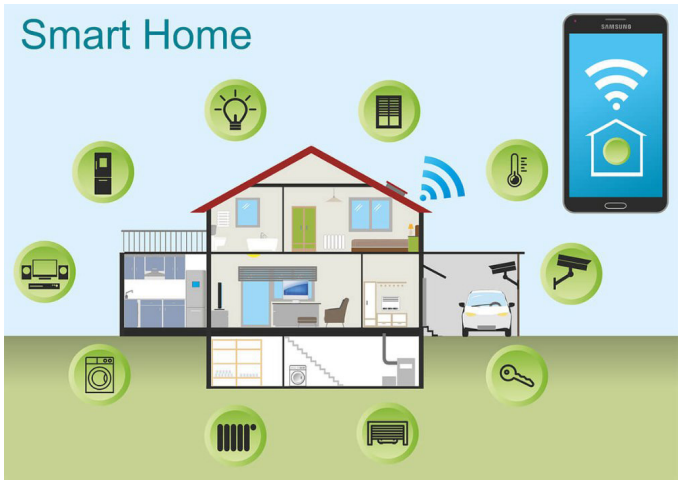

Fig. 3: Smart Home Automation (Web)

Social media information is gathered via the web combination of Smart Home devices, which is the intelligent remote application in Smart Grids (Kamilaris et al., 2010); (Koen et al., 2009). Home appliances are therefore vast Smart Home clouds. The viability of creating new computing domains and related services is what defines these remote integrations. Thus, concerns

over data privacy have arisen as a result of the efforts to develop the necessary home-based devices. Smart Metering is the most effective way to address these issues.[10]

Experimental results

The elements that go into automating smart homes using the iFogSim toolkit in a simulation platform. Numerous sensing devices are used to regulate a range of activities, including light, voltage, motor speed, room temperature, and smart home security.

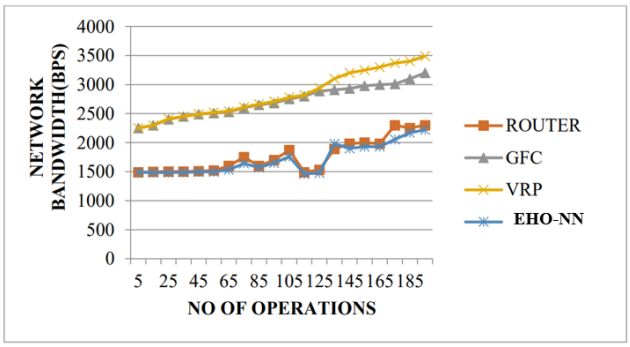

Fig. 4: Network Bandwidth analysis

Figure 4 made it abundantly evident that the VRP model had a maximum network bandwidth need and provided inefficient resource allocation. The GFC model then demonstrated marginally better resource allocation and a marginally lower demand for network bandwidth. In addition, compared to the other ways, the ROUTER model (3) provides superior resource allocation and a lower network bandwidth demand. However, compared to previous methodologies, the EHO-NN model provided better network bandwidth requirements and efficient resource utilisation.[17] For example, the VRP technique requires a maximum network bandwidth of 3400B/s when operating at 95. Next, a somewhat reduced network bandwidth of about 3200B/s was provided by the GFC model. The proposed EHO-NN model then displays a minimum bandwidth requirement of 2250B/s, while the ROUTER model provided nearly ideal results with a minimum network bandwidth of 2350B/s. This value guaranteed that the EHO-NN model will perform better in terms of network bandwidth utilisation.

The delay analysis of several methods under varying operation counts is displayed in Figure 5. The VRP model provided inefficient resource allocation and displayed maximum network latency, as the figure made evident. Subsequently, the GFC model demonstrated marginally improved resource allocation and reduced network latency.[16]. In addition, the ROUTER architecture has

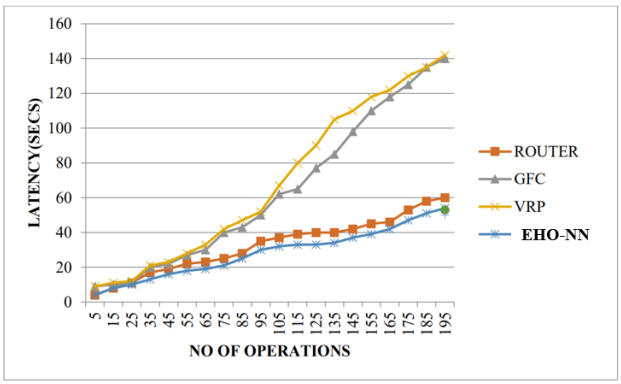

Fig. 5: Latency analysis

lower network latency and better resource allocation than the other approaches. However, compared to previous methodologies, the EHO-NN model provided better network latency and efficient resource utilisation.[13] For example, the VRP technique requires a maximum delay of 142s when operating at a maximum of 95. The GFC model then provided a somewhat reduced latency of about 140s. Then, with a minimum latency of 60 s, the ROUTER model provided results that were almost ideal, whereas the EHO-NN model that was given had a minimum latency of 38 s. This setting guaranteed that the EHO-NN model will improve in terms of network latency.[15]

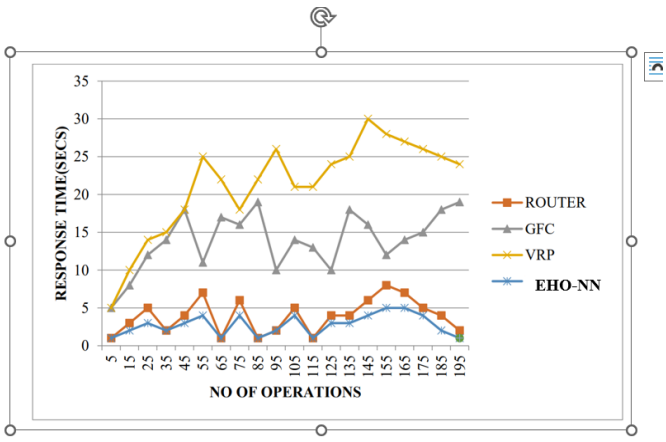

Fig. 6: Response time analysis

The response time study of several approaches under varying numbers of processes is shown in Figure 6. The VRP model provided inefficient resource allocation and displayed maximum response time, as the figure made evident. Subsequently, the GFC model demonstrated marginally improved resource allocation and a marginally reduced response time. Furthermore, compared to the other ways, the ROUTER model provides superior resource allocation and a shorter reaction time.[14] However, compared to previous methodologies, the EHO-

NN model provided better response time and efficient resource utilisation. For example, the VRP technique requires a response time of 24s while operating at the maximum of 95. The GFC model thereafter provided a somewhat slower response time of about 19 seconds. Then, with a minimum response time of 2 seconds, the ROUTER model provided results that were almost ideal, while the EHO-NN model that was given had a minimum response time of 1 second. This value guaranteed that the EHO-NN model will improve in terms of network response time.[15]

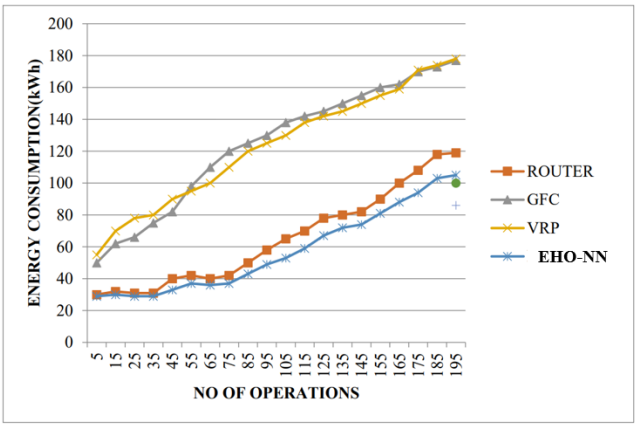

Fig. 7: Energy Consumption analysis

The energy consumption analysis of different approaches under different numbers of processes is shown in Figure 7. The VRP model provided inefficient resource allocation and demonstrated maximum energy use, as the figure made evident. Subsequently, the GFC model demonstrated marginally improved resource allocation and marginally reduced energy use. In addition, the ROUTER model uses less energy and allocates resources more effectively than the other approaches. However, compared to previous strategies, the ID-IPSO model provided superior energy consumption and efficient resource utilisation in a significant way. For example, the VRP technique demands a maximum energy consumption of 175kWh when operating at 95. The GFC model then provided a marginally reduced energy consumption of about 174 kWh.[11] Then, with a minimal energy consumption of 120kWh, the ROUTER model provided results that were almost ideal, whereas the EHO-NN model that was given showed a minimum energy consumption of 115kWh. This value guaranteed that the EHO-NN model will improve in terms of energy usage.

Conclusion

Thermostats, washing machines, cleaning robots, entertainment systems, security systems, smoke detectors, and door locks are just a few of the devices that smart home systems enable users to monitor and control. There are trade-offs between convenience, control, security, and privacy when integrating IoT technology into our homes. If an attacker is successful in breaching a smart home or smart device, they can watch the occupants of the house, take sensitive information, and violate the privacy of the user. It is important to note that a Smart Home (SH) is a desirable target for an attacker due to the fact that it contains personal information, is always online, lacks a dedicated system administrator, and has a variety of devices from various manufacturers with varying vulnerabilities. Additionally, an attacker can always search the Internet for a specific vulnerability in a particular device from a particular manufacturer to exploit. Evaluating information security threats in IoT-based smart homes is the focus of the proposed study. In order to alert users about potential security concerns, enhance security, and provide advice, this research project investigates the information security threats associated with connecting smart devices to the Internet and to one another while constructing a smart home.

References

1. Kumar, Vikas, Rahul Kumar, Srinivas Jangirala, Saru Kumari, Sachin Kumar, and Chien-Ming Chen. “An Enhanced RFID-Based Authentication Protocol using PUF for Vehicular Cloud Computing.” *Security and Communication Networks* 2022, no. 1 (2022): 8998339.
2. Gope, Prosanta, Ruhul Amin, SK Hafizul Islam, Neeraj Kumar, and Vinod Kumar Bhalla. “Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment.” *Future Generation Computer Systems* 83 (2018): 629-637.
3. Chigozirim, Ajaegbu, Deshi Shiligak Josiah, Onadeko David Oluwaseun, and Adediran Oluwaseyi. “An Innovative Smart Home System with Cloud Integration.” *IUP Journal of Information Technology* 20, no. 3 (2024): 35-51.
4. Baykara, Muhammet, and Sherzad Abdullah. “Designing a securable smart home access control system using RFID cards.” *Journal of Network Communications and Emerging Technologies (JNCET)* 10, no. 12 (2020): 1-12.
5. Latif, Rana M. Amir, Muhammad Farhan, Laiqa Binte Imran, Kashif Manzoor, Tayyaba Tariq, and Hassan Raza. “Real-Time Simulation of IoT Based Smart Home System and Services Using RFID.” *KIET Journal of Computing and Information Sciences* 2, no. 2 (2019): 12-12.
6. Fatima, Haram, Habib Ullah Khan, and Shahzad Akbar. “Home Automation and RFID-Based Internet of Things Security: Challenges and Issues.” *Security and Communication Networks* 2021, no. 1 (2021): 1723535.

7. Froiz-Míguez, Iván, Tiago M. Fernández-Caramés, Paula Fraga-Lamas, and Luis Castedo. "Design, implementation and practical evaluation of an IoT home automation system for fog computing applications based on MQTT and ZigBee-WiFi sensor nodes." *Sensors* 18, no. 8 (2018): 2660.
8. Mostafizur Rahman, M. (2019). Effectiveness of RFID Technology in Library Management System in Bangladesh. *Indian Journal of Information Sources and Services*, *9*(3), 21–29. https://doi.org/10.51983/ijiss.2019.9.3.637
9. Jabbar, Waheb A., Tee Kok Kian, Roshahliza M. Ramli, Siti Nabila Zubir, Nurthaqifah SM Zamrizaman, Mohammed Balfaqih, Vladimir Shepelev, and Soltan Alharbi. "Design and fabrication of smart home with internet of things enabled automation system." *IEEE access* 7 (2019): 144059-144074.
10. Ahmed, Mohammed Imtyaz, and G. Kannan. "Cloud-based remote RFID authentication for security of smart internet of things applications." *Journal of Information & Knowledge Management* 20, no. supp01 (2021): 2140004.
11. Islam, Md Mohaiminul, Md Nahiyan Farook, S. M. G. Mostafa, and Yasir Arafat. "Design and implementation of an IoT based home automation." In *2019 1st international conference on advances in science, engineering and robotics technology (ICASERT)*, pp. 1-5. IEEE, 2019
12. Kumar, TM Sathish. "Security Challenges and Solutions in RF-Based IoT Networks: A Comprehensive Review." *SCCTS Journal of Embedded Systems Design and Applications* 1.1 (2024): 16-19.
13. Yonis, E. G. (2024). The Effect of Thickness on the Thermal Conductivity Coefficient and Some Mechanical Properties of Acrylic Material Used in the Manufacture of Dentures. International Academic Journal of Science and Engineering, 11(2), 8–14. https://doi.org/10.9756/IAJSE/V11I2/IAJSE1143
14. Le, V. H. (2024). An Optimal Model for Allocation Readers with Grid Cell Size and Arbitrary Workspace Shapes in RFID Network Planning. *Journal of Internet Services and Information Security, 14*(1), 180-194. https://doi.org/10.58346/JISIS.2024.I1.012
15. Uvarajan, K. P. "Integration of Artificial Intelligence in Electronics: Enhancing Smart Devices and Systems." *Progress in Electronics and Communication Engineering* 1.1 (2024): 7-12.
16. Rahim, Robbi. "Scalable Architectures for Real-Time Data Processing in IoT-Enabled Wireless Sensor Networks." *Journal of Wireless Sensor Networks and IoT* 1.1 (2024): 28-31.
17. Abdullah, Dahlan. "Leveraging FPGA-Based Design for High-Performance Embedded Computing." *SCCTS Journal of Embedded Systems Design and Applications* 1.1 (2024): 29-32.
18. Hoa, N. T., & Voznak, M. (2025). Critical review on understanding cyber security threats. Innovative Reviews in Engineering and Science, 2(2), 17-24. https://doi.org/10.31838/INES/02.02.03
19. Tang, L., Chen, Y., & Zhou, J. (2025). Reconfigurable computing architectures for edge computing applications. SCCTS Transactions on Reconfigurable Computing, 2(1), 1–9. https://doi.org/10.31838/RCC/02.01.01
20. Laa, T., & Lim, D. T. (2025). 3D ICs for high-performance computing towards design and integration. Journal of Integrated VLSI, Embedded and Computing Technologies, 2(1), 1–7. https://doi.org/10.31838/JIVCT/02.01.01
21. Prasath, C. A. (2023). The role of mobility models in MANET routing protocols efficiency. National Journal of RF Engineering and Wireless Communication, 1(1), 39-48. https://doi.org/10.31838/RFMW/01.01.05
22. Srimuang, C., Srimuang, C., & Dougmala, P. (2023). Autonomous flying drones: Agricultural supporting equipment. International Journal of Communication and Computer Technologies, 11(2), 7-12. https://doi.org/10.31838/IJCCTS/11.02.02