iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** XII **Month of publication:** December 2024

DOI: https://doi.org/10.22214/ijraset.2024.66177

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue XII Dec 2024- Available at www.ijraset.com

IOT-Based Smart Home Automation Systems: Enhancing Energy Efficiency and Security

Venkatesh A[1], Naveen Kumar V[2], Hemanth Kumar M L[3]
[1]*Senior Scale Lecturer, Electronics & Communication Engineering, Government Polytechnic Nagamangala, Mandya, Karnataka, India*
[2]*Senior Scale Lecturer, Electronics & Communication Engineering, Government Polytechnic Arakere, Mandya, Karnataka, India*
[3] *Senior Scale Lecturer, Electrical & Electronics Engineering, Government Polytechnic Chinthamani, Chikkaballapura, Karnataka, India*

Abstract: ***The increase in the use of advanced technologies has made the Internet of Things an integral element of smart home automation, for creating energy efficient and secure environment. In this report, we investigate the smart home architecture, challenges, and applications as well as the trends and future directions in IoT-enabled smart homes. Their study starts with analyzing the core components consisting of sensors, connection protocols like ZigBee and Wi-Fi, and actuators that let you connect and automate seamlessly. Real-world case studies show how IoT-based Energy Management Systems, such as smart thermostats and lighting, can reduce energy consumption by up to 30%. Another application of interest is security, in the form of real-time surveillance, smart locks, and intrusion detection systems that are shown to significantly enhance home safety with reductions in emergency response times and burglary rates. However, this report highlights the future challenges faced with the advancements in device interoperability, high initial costs, and cybersecurity vulnerabilities. The emergence of 5G, edge computing, AI, and blockchain will provide promising solutions to these issues, enabling the development of scalable and secure IoT Ecosystems. Finally, suggestions are made on a pathway for industry stakeholders and policymakers to encourage innovation and adoption. By solving these challenges, IoT can make smart homes smart, energy efficient, secure, and sustainable living spaces, as well as drive great success in energy and security management.***

Keywords: Internet of Things (IoT), Smart Home Automation, IoT Sensors and Actuators, ZigBee and Z-Wave, Home Security Systems

I. INTRODUCTION

A. Background

With the Internet of Things (IoT), physical devices are becoming connected to the Internet and are able to communicate, collect, and exchange data all by themselves. As an umbrella term that describes the architecture of connecting devices (smart thermostats, lighting systems, surveillance cameras, and home appliances) into a single network, IoT has redefined the means through which a person works with his living space in the realm of smart homes. Statista (2023) says that the global smart home market is expected to be 195 billion by 2025 due to the fast-growing interest in IoT [1]. As the number of IoT devices (IoT) exceeds 14 billion by 2024, there is an increasing reliance on smart systems to simplify processes, increase safety, and improve resource efficiency in households. While smart homes powered by IoT, are not only about automation but can make an intelligent ecosystem that learns user behaviors and consumes energy efficiently without compromising privacy and security.

B. Purpose

The two key contributing elements to the evolution of IoT-based smart home systems are energy efficiency and security. Approximately 40 percent of the world's energy is consumed by buildings, which is why it is so important to cut energy wastage in order to combat climate change and bring down utility costs. By providing real-time monitoring and intelligent control over energy-consuming devices, IoT systems could enable up to 30 % reduction in energy consumption according to the International Energy Agency (IEA). At the same time, the prevalence of cyberattacks is growing (and in fact, IoT-specific breaches rose by 300 % between 2020 and 2023), meaning that smart homes need strong security [2]. Unauthorized access, data breaches, and the exposures of interlinked devices are all to be covered by security concerns, for which advanced intrusion detection frameworks and data encryption are needed. Our work here explores whether IoT-based smart home systems do in fact address this dual priority where they enable quality-of-life improvements for residents and energy efficiency and security goals.

Scope

This report comprehensively examines the integration of IoT in smart home automation systems, focusing on enhancing energy efficiency and ensuring security. It covers the following areas:

1) Technology Overview: Device, sensor, actuator, and communication protocols such as ZigBee, Z-Wave, and Wi-Fi are included in the underlying IoT architecture.
2) Energy Efficiency: Real case studies showing the energy reduction impact driven by smart lighting, heating, ventilation, and air conditioning (HVAC) enabled IoT systems.
3) Security Measures: An analysis of security threats with associated mitigation strategies (encryption, anomaly detection, blockchain, etc.).
4) Challenges and Future Trends: Interoperability, standardization issues, and current (emerging) solutions such as AI and edge computing.
5) With these considerations, the report is able to present a thorough understanding of the technological, operational, and societal implications of IoT in smart home systems.

C. Research Questions/Goals

This report aims to address the following key questions:

1) How does IoT enhance energy efficiency in smart homes?

By using real-time data, predictive analytics, and device automation, IoT reduces energy usage with measurable reductions in energy bills and carbon footprints.

2) How can IoT improve security in home automation systems?

With the integration of advanced security protocols, machine learning in the detection of threats; and especially the integration of privacy setting technologies, IoT systems can ensure users' safety against evolving cyber threats.

Finally, it is concluded that already IoT based smart home automation systems have great potential to reduce energy consumption and increase security while serving for an intelligent and sustainable living. This report investigates these aspects further, taking a more nuanced view of where they are now and could be in the future.

II. LITERATURE REVIEW

A. IoT Technology for Smart Homes

Smart homes have taken on the intelligence of IoT technology through sensors, devices, and communication protocols cued together into a single homogenous experience. This ecosystem is built around sensors, vital to this ecosystem, able to sense real-time data on temperature, humidity, motion, light, and energy use. They can be paired to work with actuators that enable automation like closing or opening the lighting-connected loads and controlling HVAC systems [3]. Smart home automation is founded on devices such as smart thermostats, security cameras, and energy meters to enhance the user experience, efficiency, and most importantly minimize human error. There are communication protocols that guarantee the smoothness of the connection among the devices. ZigBee and Z Wave are quite famous for low power consumption and strong security. A 100m range with data rates up to 250 kbps using the IEEE 802.15.4 standard, ZigBee is appropriate for temperature sensors. Smart locks and alarms can operate on sub-GHz frequencies, making it less predictable for interference, and thus more reliable. Even if more power intensive, Wi-Fi is helpful in dealing with high bandwidth tasks like video streaming [4]. Bluetooth Low Energy (BLE), a low-power short-range protocol can be applied to wearables and smart speakers.

This brings these technologies together to form an interconnected space where there is fluid data flow. Many devices connected to smart hubs will get aggregated data and are now controlled collectively through mobile apps or voice commands. The reason for that interconnectivity is to allow functionalities like predictive maintenance, real-time monitoring, and personalized settings.

B. Energy Efficiency

Real-time analytics and automation are therefore a boost to energy efficiency enabled by IoT. The International Energy Agency says the installed base of IoT-enabled energy management systems (EMS) can optimize energy consumption across appliances, reducing household energy use by up to 30%. Machine learning thermostats, such as the Nest Learning Thermostat, use their machine intelligence to figure out how like to heat and cool the home and then change how to heat and cool it as well, reducing heating costs by 10 to 12 percent and cooling costs by a whopping 15 percent [5]. As in a 2022 California case study, 1,000 smart thermostat homes in a year saved 1.2 GWh of energy. Like Philips Hue, smart lighting systems are able to be controlled remotely for brightness, color, and guaranteed lights turned off when not in use in unoccupied rooms.

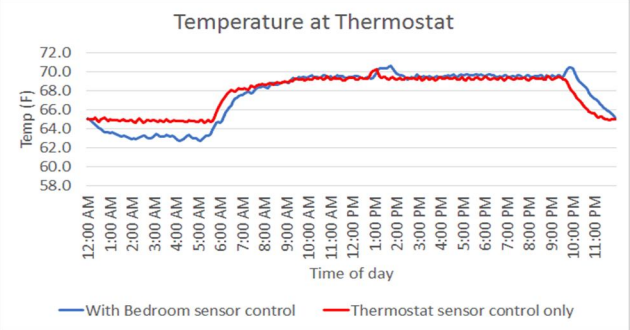


Figure 1: Temperature at Thermostat

Temperature regulation improvements are illustrated using control using IoT enabled bedroom sensors compared to thermostat only control. With IoT its even more hyper accurate and precise when it comes to temperature changes to the point of reducing energy waste whilst maintaining comfort. This reflects research on how smart thermostats make energy efficiency practical in a real time world and save users between 10 and 12 % on their heating bill and 15 % on their cooling costs. [6]Control of IoT appliances further improves efficiency. Smart plugs present insights into the consumption pattern as well as the ability to schedule the appliance at an off-peak hour to cut electricity costs. Renewable energy systems such as solar panels and battery storage run in tandem with energy distribution to increase integration. Real-time monitoring enables excess energy generation during peak production to be stored or redirected, hence cutting grid dependency.

However, problems still persist. Low or no interoperability with other devices is a big hurdle, where proprietary protocols most commonly prevent it. There are also high initial costs that stop the widespread adoption from happening. While IoT systems promise to deliver long-term savings, the costs ranging between $1,500 and $2,000 per household are prohibitive.

C. Security in IoT

Smart homes are overrun with IoT devices, which present a host of security issues. The attack surface for cybercriminals also increases its size as there will be more connected devices. In 2016 the Mirai botnet attack exploited IoT vulnerabilities to attack (hamburgers) IoT devices and launch distributed denial of service (DDoS) attacks. The security of IoT devices is typically lacking strong features. According to a Symantec study, 75% of IoT devices lack proper encryption, and thus data is placed at the mercy of breaches. Unauthorized access, data interception, and device hijacking are threats [7]. Smart lock: a compromised smart lock may allow other people to gain entry unauthorized; Hacked cameras: leaked sensitive footage. To solve the issues mentioned above, IoT security frameworks were created to do end-to-end encryption, which makes data confidential during transmission. Cheers to Secure Sockets Layer (SSL) and Transport Layer Security (TLS). Additional protection requires authentication mechanisms such as two-factor authentication (2 FA) and biometric verification. Blockchain technology also increases IoT security. Blockchain goes further than ensuring the tamper-proofness of all transactions and data exchanges, it creates decentralized ledgers [8]. Blockchain verifies devices, and secures communication, while IBM's Watson IoT platform uses it for its authentication and security. Blockchain can cut IoT cyber risks by up to 50%, according to studies.

However, gaps persist. Security is fragmented due to the weakness of standardized protocols, and lack of regulatory oversight. Most of these devices were designed with functionality over security, thus introducing them into technological networks can leave them open to advanced attacks. Secondly, the harnessed computational power of IoT devices is insufficient to support the execution of sophisticated security measures.

D. Gaps in Existing Research

The IoT technologies for smart homes have come a long way but there are some serious gaps that need attention. It still remains a major challenge to achieve device interoperability. However the current ecosystem is too fragmented, and many devices do not work on different protocols. Not only is this restrictive, but it also poses security vulnerabilities in a way that poorly integrated systems are more easily broken into. The second concern is scalability. With an increasing number of connected devices, network congestion, and latency are substantial problems. While ZigBee and Z-Wave prove effective for small-scale problems, much larger IoT deployments present a challenge for these protocols. By 2025, there will be more than 75 percent of global network traffic coming from IoT devices, which explains the need for more robust communication infrastructures.

As for energy efficiency frameworks, there must be innovation as well [9]. Current systems, as compared, however, are optimized to work for appliances but with IoT and smart grids and renewable energy systems underexploited. IoT-powered microgrids have the potential to improve energy distribution and reduce dependence on centralized grids but studies in this field are scarce.

Security challenges persist. Improvements to lightweight encryption algorithms and intrusion detection systems for resource-constrained IoT devices are clearly needed. However, proactive threat detection using artificial intelligence (AI) and machine learning (ML) is not fully explored. Privacy concerns matter as much as any other issue. Federated learning, a technique that trains collaborative models between devices without sharing raw data across them, still requires development to gain user trust.

III. SYSTEM DESIGN AND ARCHITECTURE

A. Components of IoT-Based Smart Home Systems

The architecture of IoT-based smart home systems revolves around three key components: actuators, sensors and communication networks. It creates an interrelated environment that software automates processes, improves energy usage, and enhances security.

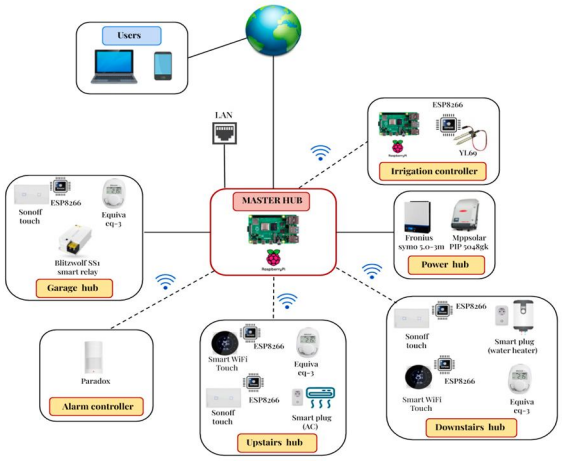


Figure 2: IoT-Based Smart Home System Architecture

IoT Sensors: Collecting real-time data in smart homes is dependent on sensors. Parameters such as motion, temperature, humidity, light, and gas concentrations are measured by these devices. Take motion sensing devices like passive infrared (PIR) sensors as an example, which can trigger or start the automation of lights or security systems. Digital thermocouples provide advanced temperature sensors for which precise HVAC system adjustments are made to keep optimal indoor conditions [10]. In addition, gas sensors, like MQ2 or MQ135, monitor harmful gases (carbon monoxide (CO), or volatile organic compounds (VOCs)) for an extra level of safety. The market for IoT sensors is projected to grow by a compound annual growth rate (CAGR) of 25.1 percent, all due to the uptake of smart homes, according to Allied Market Research (2023).

Figure 3: Top 10 Sensors for IIoT (Industrial Internet of Things) Solutions

Actuators and Controllers: The system issues commands to actuators and they perform physical action. Motorized valves for water systems, servo motors for automated blinds, and relays to switch appliances on or off are examples. A Raspberry Pi or Arduino controller coordinates sensor data, and sends actuator commands. The current modern controllers are often programmed with microprocessors capable of running the AI algorithm locally, so that edge computing is achievable for reducing latency and enhancing system responsiveness.

Figure 4: IoT System Architecture for Smart Homes

Communication Networks: For smart homes to work smoothly, we require reliable communication between sensors, controllers, and cloud platforms [11]. For low data, low-power applications like ZigBee and Z-Wave are preferred, while Wi-Fi is used for the high bandwidth tasks of video streaming. A more scalable and more secure form of communication offers newer protocols such as Thread which supports IPv6. Wi-Fi and Bluetooth technologies are expected to account for about 50 percent of all of the traffic to and from the Internet of Things (IoT) by 2025 according to Cisco due to their wide compatibility and ease of integration.

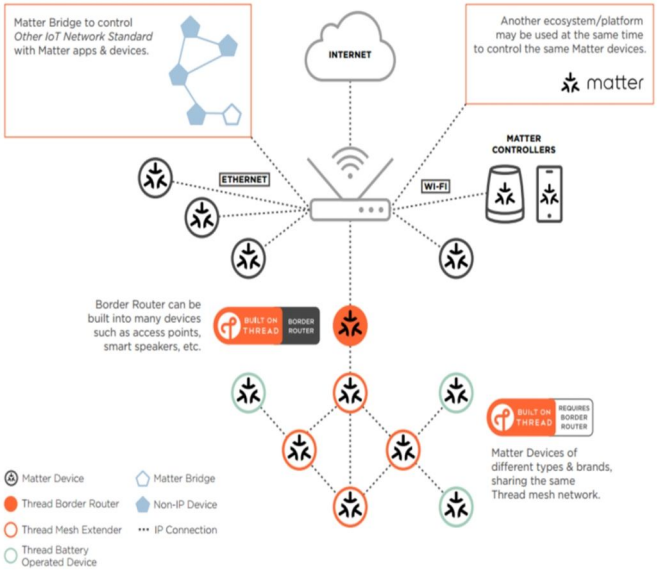


Figure 5: Matter IoT Ecosystem Architecture

B. Energy Management Architecture

The designing of energy management in IoT-enabled smart homes is centered around the best use of consuming available power and bringing renewable energy sources into it. Based on the advanced algorithms and IoT devices, the architecture monitors, analyzes, and controls energy consumption in near real-time.

1) *Role of AI/ML in Optimizing Energy Usage:* Energy optimization highly relies on AI and machine learning algorithms. These algorithms look through the history and the current wall of time predict energy consumption patterns, and suggest or perform actions to reduce wasted energy. For example taking AI-powered thermostats as an example, AI can learn the user's behavior and change how the HVAC systems operate dynamically [12]. McKinsey & Company's (2023) research indicates that such systems can cut energy consumption by 20-25%. Demand response mechanisms through ML models allow appliances that aren't used during rush hour and times when electricity is most expensive to operate.

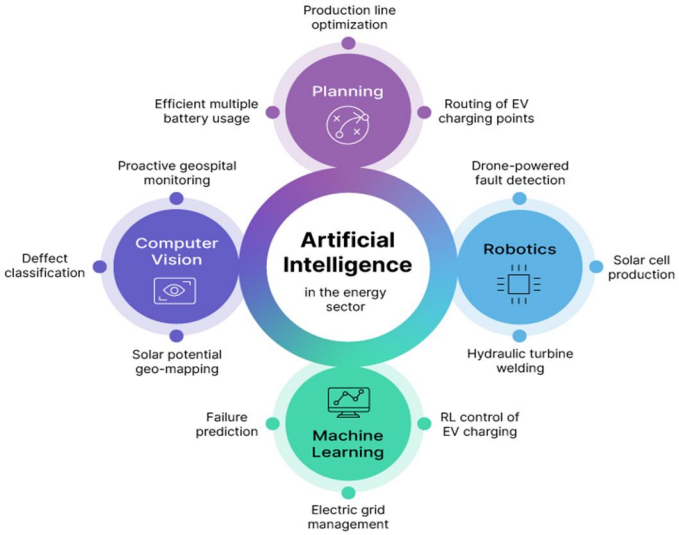


Figure 6: Artificial Intelligence in the Energy Sector

Visual insights into consumption offered through energy dashboards help residents make better decisions. Using AI, users are able to get actionable recommendations, like when to cut down the usage time during peak periods or to adjust to power-efficient mode. In addition, AI will help with predictive maintenance in appliances like water heaters or air conditioners that will allowing them to function continuously with optimum efficiency before a breakdown can occur.

2) *Integration with Renewable Energy Sources:* With the addition of renewable energy sources such as solar panels and wind turbines to IoT-based energy management systems, they are being increasingly integrated. Real-time energy generation, storage, and distribution are being managed by smart inverters and controllers [13]. As one example, the International Renewable Energy Agency (IRENA) study points out that homes fitted with IoT-integrated solar devices can raise energy utilization efficacy by 30 to 40 %. Grid interaction is also enabled by IoT platforms so that surplus energy generated from renewable sources is allowed to be fed back to the grid or stored in battery systems.

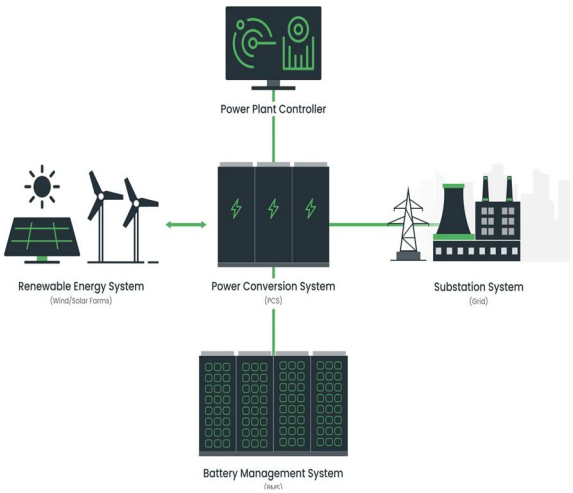


Figure 7: Renewable Energy System Architecture

By having IoT in place, Virtual Power Plants (VPP) can aggregate renewable energy from various homes to form a decentralized energy network. These networks increase grid stability, reducing to an extent dependence on fossil fuels. With IoT data analytics, VPPs use energy flow to optimally bring homes away from unsustainable energy use patterns while advancing cost savings.

C. Security Framework

One of the reasons for IoT devices to be complex and require this much amount of security is because of the interconnection nature of IoT devices in smart homes. Encryption, blockchain technology, and real-time intrusion detection systems are part of a secure architecture.

1) *End-to-End Encryption:* Data Confidentiality and Integrity is crucial in smart homes with the aid of IoT. However, encrypted data transmitted from devices and to the cloud platforms can be intercepted or tampered with unless protected by the end-to-end (E2EE) [14]. For data security, it is usually used advanced encryption standards (AES-256). E2EE is useful for instance, in the case of smart locks and cameras that use it to stop unwanted access to sensitive pieces of information. Symantec's (2022) Report revealed that 70% fewer IoT devices are compromised when properly encrypted.

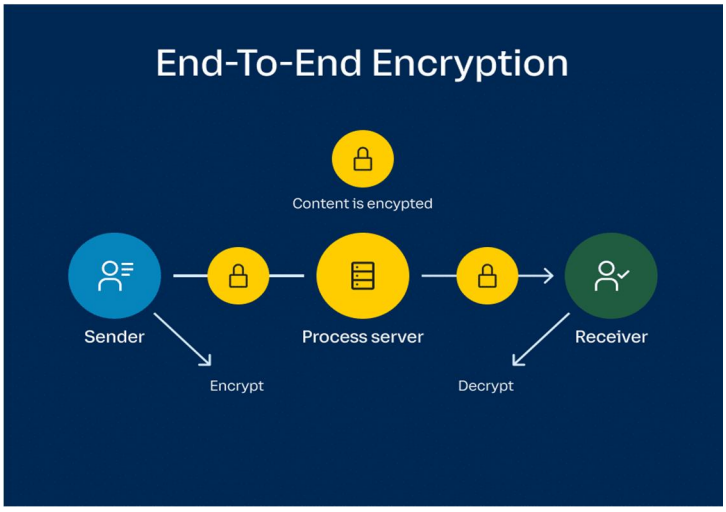


Figure 8: End-to-End Encryption

2) *Role of Blockchain in Enhancing Security:* So, the problem of security for IoT devices and their networks has become Blockchain technology. This means that the blockchain creates an immutably decentralized ledger of all transactions and device activity. Blockchain frameworks have smart contracts that automate security protocols like automatically revoking a device's access if an anomaly is detected [15]. For instance, IBM's Watson IoT platform authenticates devices using blockchain to also secure data communication between them. IoT security can be enhanced by blockchain — as much as 50 % — says the research, with the main benefit being the reduction of risk of tampering and data forgery.

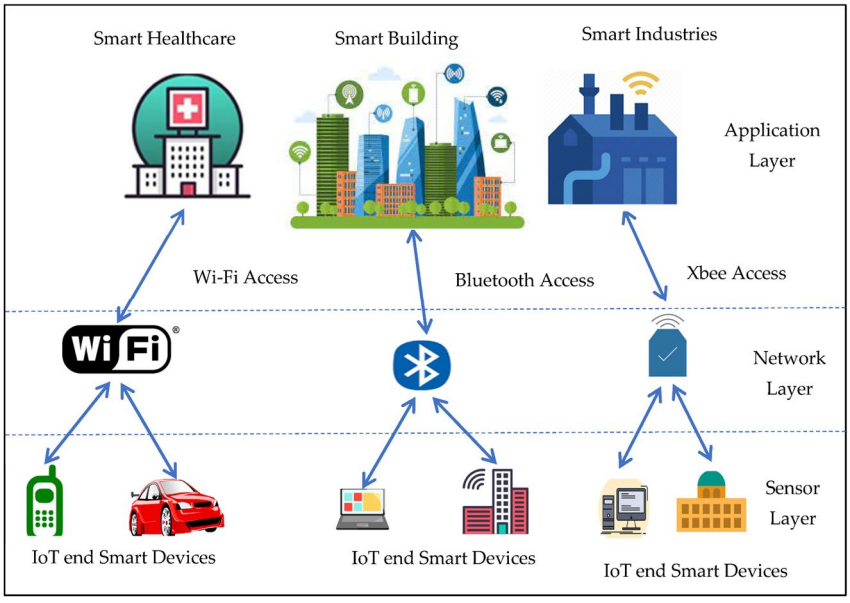


Figure 9: IoT Architecture Across Smart Applications

3) *Real-Time Intrusion Detection Systems:* IoT security is something that's made up of a cornerstone, intrusion detection. Intrusion Detection Systems (IDS) based on machine learning are used to examine network traffic behaviors and respond to possible threat events in real-time. These systems involve anomaly detection models that mark unusual behavior, like unauthorized attempts to log in, or too much data usage by a device. As reported by Palo Alto Networks (2023), IDS implementation into IoT networks decreases the average time response rate to cyber attacks from hours to milliseconds [16]. As more smart home security systems leverage IoT-specific IDS frameworks such as Kismet and Snort to provide proactive protection, the adoption of such systems is growing.

Smart homes using IoT-integrated systems are also able to automatically neutralize threats beyond detecting intrusions. For example, immediately alerted mobiles could be used to notify the affected area or compromised devices isolated from the network. With these automated responses, the risk of long security gaps is basically eliminated.

IV. BENEFITS AND USE CASES

A. *Energy Efficiency Use Cases*

Smart home systems are essential to use IoT to optimize the use of energy, decrease environmental impact, and decrease costs. Motion sensors and bright versions of smart lighting adjust automatically based on occupancy and ambient light. For example, Philips Hue can reduce energy consumption by up to 80% to save electricity compared to incandescent bulbs and allows the users to control their lighting using a remote control to set up the schedule and light that don't need. And, HVAC systems are high in energy efficiency. Smart thermostats like Nest or Ecobee are powered by IoT and start learning the user's preferences about heating and cooling and dynamically adjust the heating or cooling accordingly [17]. Facts indicate that smart thermostats can cut heating bills by 10% to 12% and cooling bills by 15%. In a 2022 California case study, 1,000 smart thermostats helped 1.2 GWh of energy to save one year of households.

Smart plugs and meters provide user insights as to how and whether it is wasting energy in real-time. In UK pilot households, Sense Energy Monitor devices identify energy-intensive appliances and suggest changes, with an average 20% electricity reduction achieved over 6 months.

B. *Security Applications*

With advanced, interconnected solutions, IoT improves home security. There are also real-time surveillance cameras like Arlo and Ring which will send live feeds, motion alerts, and cloud storage. Geofencing features help cameras to power down while users are around and increase reliability and energy conservation. Systems like August Smart Lock and Schlage Encode access control both lock and unlock doors with smartphones. Often, however, these systems include biometric verification or temporary digital keys to ensure secure access. The smart lock market is also expected to witness a CAGR of 18.8%, suggests MarketsandMarkets, as people demand Internet of Things (IoT) enabled solutions [18]. IoT's skill lies in the field of threat detection by connected smoke detectors, water leak sensors, and intrusion alarms. Smoke detectors mounted to the HVAC system can independently shut off airflow to prevent smoke and assist in emergency exiting. According to a 2021 Japanese study, IoT-based detection systems reduced emergency response times by 35%. Their impact is shown in real-world adoption. In 2019, Smart Nation, Singapore's IoT-enabled security systems were deployed to more than 50,000 households, and residential burglaries have been reduced by 15 percent since. The findings point to a dual role for IoT in protecting the home and supporting societal safety.

C. *Integration with Smart Cities*

However, IoT-based smart homes are a key part of the overall energy and security strategy of the smart cities. On a larger scale, these interconnected ecosystems are optimizing energy use, and guaranteeing safety. Smart homes are energy-smart in that they interact with smart grids to dynamically balance demand and supply. In time of peak hours, IoT-enabled appliances take a break from all nonessential operations to prevent blackouts due to grid load. Participating households who installed an IoT home within a grid as part of Amsterdam's Smart City pilot managed to reduce the peak hour energy use by 15%. The data contributed by smart homes are used in citywide surveillance systems. But, for example, facial recognition mounted on doorbell cameras can let law enforcement know there's an unauthorized person there [18]. The Array of Things project was IoT in residence, enabling better data for crime hot spots for law enforcement response by 10%.

The integration of IoT also includes cloud pricing towards sustainability. Solar panels and energy storage in homes contribute excess energy that helps to support renewable energy goals. By 2030, smart city initiatives with IoT homes could reduce urban carbon emissions by as much as 40 percent, says IRENA.

D. Conclusion

Yet IoT-based smart home systems, due to their inherent security and energy efficiency benefits, along with smart city integration, provide significant benefits. IoT utilizes smart lighting, HVAC, and energy monitoring to reduce both energy costs and environmental footprint. Robustness is what security applications have to offer with its capability to refrain from illegal crime, it also helps to have better crime prevention and emergency response. Its emergence as a technological phenomenon set for the 21st century promises to revolutionize future houses and communities, and when embedded in smart cities, IoT-enabled homes create an enabling ecology for urban sustainability and safety.

V. CHALLENGES AND LIMITATIONS

A. Energy Efficiency Challenges

However, IoT-enabled energy efficiency presents many challenges. The lack of standardized communication protocols constitutes a big problem for interoperability of devices. There are proprietary technologies used by different manufacturers, which prevent seamless integration and give rise to isolated systems. Energy management systems suffer from this fragmentation of data which limits its effectiveness [19]. For example, it is found that 60% of smart devices experience compatibility issues when connected to multi-vendor networks.

Adoption is hindered by high initial costs as well. Even installing IoT devices like smart thermostats, sensors, and energy monitoring systems requires a high one-time cost. The cost of equipping a home with IoT energy solutions is $1,500 to $2,000 on average, according to the International Energy Agency. While the resulting energy savings are long-term the initial financial burden continues to be a barrier to uptake for many households, especially in low and middle-income regions.

B. Security Challenges

In the context of IoT-enabled smart homes security is a limitation that is only growing to privacy concerns and data vulnerability. IoT collects vast amounts of data from things like energy usage patterns to video surveillance feeds. According to a 2022 Kaspersky study, 41 % of IoT devices are vulnerable to cyberattacks for lacking encryption and default credentials. Such data isn't protected, and unauthorized access not only intrudes on privacy, it also makes peoples' homes vulnerable to intrusion and financial fraud.

Security issues are compounded by inadequacies in standards. Since there are no universal compliance frameworks, the industry often places functionality over security. Such inconsistency ends up in fragmented security measures that make it easier for the attackers to utilize vulnerabilities [19].

For instance, the Mirai botnet attack of 2016 exploited poor security on IoT devices to create large-scale distributed denial of service (DDoS) attacks, to demonstrate the scale at which insufficient compliance can be risky.

C. Technological and Operational Limitations

Unlike traditional systems, IoT systems are also constrained in terms of scalability and network performance. With a smart home consisting of more and more connected devices, network congestion is an increasing concern. For instance, existing protocols such as ZigBee and Z-Wave are efficient for limited-scale applications, yet may fall short in coping with the data traffic caused by the presence of larger IoT ecosystems [20]. By 2025, Cisco predicts that more than 75 % of all network traffic will come from IoT devices—forcing the need for more robust communication infrastructures.

Challenges of scalability reach cloud-based processing and storage. When relying on central cloud systems latency is higher and responsiveness is lower. Despite their promise, edge computing solutions are not capitalized upon for being complex and too expensive to implement. The Lack of these limitations impedes the effectiveness of smart homes empowered with IoT to adapt to upcoming emergent needs.

D. Conclusion

Challenges faced by IoT-enabled smart homes such as device interoperability (and lack thereof cost), security vulnerability, and scalability constraint show the impingence of standards, innovation, and cost-effective solutions. These are issues that have to be addressed for the full potential of IoT in creating smart home ecosystems on the lines of efficiency and scalability to be realized with IoT.

VI. FUTURE TRENDS AND OPPORTUNITIES

A. Emerging Technologies

The emergence of 5G and the coming of 6G offer huge expectations in the way 5G will run IoT in smart homes. 5G with ultra-low latency and 100 times faster than 4G speeds gives IoT devices the ability to communicate more efficiently for seamless integration of real-time applications such as augmented reality (AR) for home management. Data rate greater than 1 Tbps is expected from 6G by 2030 and those capabilities will further enhance and will support the IoT ecosystem in an advanced manner [20]. Another transformational technology is edge computing, which reduces reliance on centralized cloud systems by processing data in locations closer to their source – and off the network – reducing latency and network congestion. AI combined with edge computing makes it possible to quickly, contextually decide things, like anticipating appliance failures in real-time.

B. Energy Efficiency Innovations

The IoT applications is driven by innovations in energy management. AI powered predictive maintenance using data to predict equipment failure and reduce energy wastage. For example, smart HVAC systems that use predictive algorithms can extend operation service lifespans by 20%. Decentralized energy systems represented by IoT-powered microgrids include renewable energy sources such as solar panels and battery storage. These microgrids provide real-time demand-based energy distribution, thus minimizing reliance on traditional grids and cutting carbon emissions. The International Energy Agency reports that IoT-driven microgrids could slice urban energy costs by 25% over the next decade as reported in a 2023 study.

C. Advanced Security Measures

There are advanced measures that are critical as security threats evolve. With the explosion of new unlimited possibilities that the IoT universe brings, quantum cryptography based on quantum mechanics principles promises virtually unbreakable encryption, and data integrity in IoT networks [15]. This is then further complemented by AI-based anomaly detection that analyses behavioral patterns in order to detect irregularities and protect from cyber attacks. Recurrent implementations in smart home environments have shown these systems can reduce detection times from hours to seconds.

D. Market and Adoption Trends

Rising consumer demand and technological advancements led to a forecast of the smart home market to reach $317 billion by 2030. There is a growing amount of IoT adoption and it is estimated that by 2030 IoT will be connected to 24 billion devices. This growth highlights the growing need for IoT solutions for energy efficiency, security, and smart city integration, which involve a degree of transformation to spur the next chapter.

VII. RECOMMENDATIONS

A. Improving Energy Efficiency and Security

IoT-based smart homes need AI-driven optimization tools to enhance energy efficiency. Studies show that predictive analytics and real-time monitoring systems can reduce energy wastage by up to 30 % in IoT-enabled households. Decentralized energy solutions that decentralize the grid exist as integration of IoT devices with renewable energy sources, such as microgrids and solar panels [17]. To secure sensitive data, it also pays to use end-to-end encryption and AI-based intrusion systems to detect cyber threats proactively. According to Gartner (2023), combining AI with blockchain can cut IoT security breaches in half.

B. Regulatory Frameworks and Standardization

The interoperability and security challenges must be addressed with the development and enforcement of regulatory frameworks. Device integration from manufacturer to manufacturer can easily be accomplished via standardized protocols, like Thread and Matter. Compliance with these standards should be forced upon governments and international organizations by having them enforce device compatibility and data protection. For instance, the European Union's Cybersecurity Act sets an ideal baseline for certifying IoT products and improving the distrust and safety of customers. Moreover, the regulatory policies should promulgate tax benefits or subsidies for the prompt entry of energy-efficient IoT systems into the market.

C. Role of Industry Stakeholders and Policymakers

Collaboration should take priority among industry stakeholders in order to create interoperable and secure ecosystems. For advances in lightweight encryption methods and scalable IoT systems, investment in research and development is necessary. Public-private partnerships have to be created and funding for pilot projects be established for policymakers to make innovation happen [20].

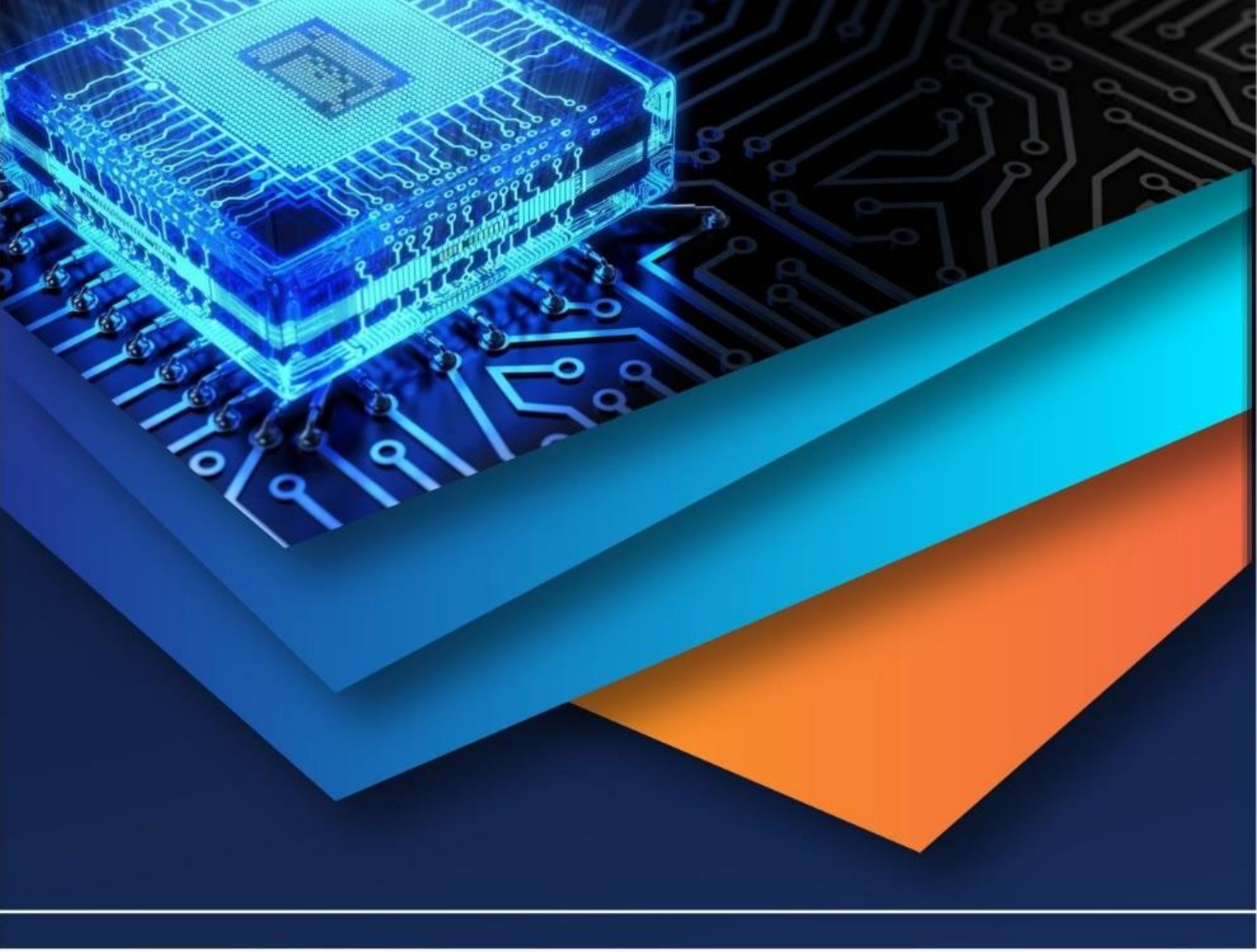
It is also important to educate consumers on IoT technology benefits, as well as the right way to apply it. Through designing for a future where technology drives ahead aligned with consumer needs and regulations, the stakeholders can access the full potential of IoT to turn smart homes into efficient, secure, and sustainable living. Strategic action is the most important factor for pushing large-scale adoption and innovation in the IoT sector.

VIII. CONCLUSION

The report shows how an IoT-based smart home system can provide exciting possibilities for energy-efficient and secure home systems. The energy management gains seen from these IoT-enabled smart lighting, HVAC systems, and energy monitoring devices have been shown to be measurable, and studies report a reduction in household energy consumption as high as 30%. Renewable energy sources integration and on such technologies as predictive maintenance only reinforce IoT's importance in reducing carbon emissions and reducing operational costs. At the same time, IoT has developed in security aspects such as real-time surveillance, smart locks, and AI-based intrusion detection for better home safety and assisted broader societal protection through smart city integration. It is rightly stated that IoT plays a role of both in energy efficiency and security. IoT optimizes resource usage while reducing environmental impact and households' financial savings. In term of security, the platform is designed to be as robust as blockchain, quantum cryptography, and anomaly detection systems to protect the safety and privacy of residents. But problems like device interoperability, scalability, and standardized protocols are still huge problems that need tackling before IoT can truly be fostered. As for IoT-based smart homes, the future will be dependent on the continuous development in technologies such as 5G/6G, edge computing, and AI. Such advancements would provide heightened efficiency, and effectiveness and be seamlessly merged into smart cities, forming interjoined ecosystems, which will enhance the lives of druggies as well as the communities as a whole. A liaison is required among policymakers and industry stakeholders to remove regulatory an

REFERENCES

[1] Adibi, S., Rajabifard, A., Shojaei, D. & Wickramasinghe, N. 2024, "Enhancing Healthcare through Sensor-Enabled Digital Twins in Smart Environments: A Comprehensive Analysis", Sensors, vol. 24, no. 9, pp. 2793.
[2] Bakare, M.S., Abdulkarim, A., Zeeshan, M. & Shuaibu, A.N. 2023, "A comprehensive overview on demand side energy management towards smart grids: challenges, solutions, and future direction", Energy Informatics, vol. 6, no. 1, pp. 4.
[3] Chaudhari, P., Yang, X., Mark Ming-Cheng Cheng & Li, T. 2024, "Fundamentals, Algorithms, and Technologies of Occupancy Detection for Smart Buildings Using IoT Sensors", Sensors, vol. 24, no. 7, pp. 2123.
[4] Dobrovolskis, A., Kazanavičius, E. & Kižauskienė, L. 2023, "Building XAI-Based Agents for IoT Systems", Applied Sciences, vol. 13, no. 6, pp. 4040.
[5] Esfandi, S., Tayebi, S., Byrne, J., Taminiau, J., Giyahchi, G. & Seyed, A.A. 2024, "Smart Cities and Urban Energy Planning: An Advanced Review of Promises and Challenges", Smart Cities, vol. 7, no. 1, pp. 414.
[6] Fartitchou, M., Lamaakal, I., Maleh, Y., Makkaoui, K.E., Allali, Z.E., Pławiak, P., Alblehai, F. & Abd El-Latif, A.,A. 2024, "IOTASDN: IOTA 2.0 Smart Contracts for Securing Software-Defined Networking Ecosystem", Sensors, vol. 24, no. 17, pp. 5716.
[7] Gentile, A.F., Macrì, D., Carnì, D.L., Greco, E. & Lamonaca, F. 2024, "A Performance Analysis of Security Protocols for Distributed Measurement Systems Based on Internet of Things with Constrained Hardware and Open Source Infrastructures", Sensors, vol. 24, no. 9, pp. 2781.
[8] He, P., Zhou, Y. & Xiao, Q. 2024, "A Survey on Energy-Aware Security Mechanisms for the Internet of Things", Future Internet, vol. 16, no. 4, pp. 128.
[9] Hu, L., Han, C., Wang, X., Zhu, H. & Ouyang, J. 2024, "Security Enhancement for Deep Reinforcement Learning-Based Strategy in Energy-Efficient Wireless Sensor Networks", Sensors, vol. 24, no. 6, pp. 1993.
[10] Iordache, V., Minea, M., Gheorghiu, R., Bădău, F., Angel Ciprian Cormoș, Valentin, A.S., Ion Nicolae Stăncel & Stoica, V. 2024, "Integrating Connected Vehicles into IoT Ecosystems: A Comparative Study of Low-Power, Long-Range Communication Technologies", Sensors, vol. 24, no. 23, pp. 7607.
[11] Isong, B., Kgote, O. & Abu-Mahfouz, A. 2024, "Insights into Modern Intrusion Detection Strategies for Internet of Things Ecosystems", Electronics, vol. 13, no. 12, pp. 2370.
[12] Machele, I.L., Onumanyi, A.J., Abu-Mahfouz, A. & Kurien, A.M. 2024, "Interconnected Smart Transactive Microgrids—A Survey on Trading, Energy Management Systems, and Optimisation Approaches", Journal of Sensor and Actuator Networks, vol. 13, no. 2, pp. 20.
[13] Mustafa, R., Sarkar, N.I., Mohaghegh, M. & Pervez, S. 2024, "A Cross-Layer Secure and Energy-Efficient Framework for the Internet of Things: A Comprehensive Survey", Sensors, vol. 24, no. 22, pp. 7209.
[14] Netinant, P., Utsanok, T., Rukhiran, M. & Klongdee, S. 2024, "Development and Assessment of Internet of Things-Driven Smart Home Security and Automation with Voice Commands", IoT, vol. 5, no. 1, pp. 79.
[15] PDF 2024, "Enhancing IoT Network Security: ML and Blockchain for Intrusion Detection", International Journal of Advanced Computer Science and Applications, vol. 15, no. 4.
[16] Rajarajeswari, S., Shola, U.R., Kataria, A. & Dutta, S. 2021, Home Automation through Smart Lighting, Smart Security and other Appliances, EDP Sciences, Les Ulis.
[17] Takacs, A. & Haidegger, T. 2024, "A Method for Mapping V2X Communication Requirements to Highly Automated and Autonomous Vehicle Functions", Future Internet, vol. 16, no. 4, pp. 108.
[18] Vardakis, G., Hatzivasilis, G., Koutsaki, E. & Papadakis, N. 2024, "Review of Smart-Home Security Using the Internet of Things", Electronics, vol. 13, no. 16, pp. 3343.
[19] Xu, H., Liu, W., Li, L. & Zhou, Q. 2024, "An IoT-based low-cost architecture for smart libraries using SDN", Scientific Reports (Nature Publisher Group), vol. 14, no. 1, pp. 7022.
[20] Yilmaz, S. & Dener, M. 2024, "Security with Wireless Sensor Networks in Smart Grids: A Review", Symmetry, vol. 16, no. 10, pp. 1295.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY