



# The Role of Internet of Things (IoT) in Smart Networks: A Case Study of Smart Energy Monitoring

Safa A. Namah <sup>1\*</sup>, Marwah M. Abed <sup>2</sup>, Nalbantoglu O.U. <sup>3</sup>, Kawther A. Neamah <sup>4</sup>

<sup>1</sup> College of Engineering, Al- Iraqia University, Baghdad, Iraq

<sup>2</sup> College of Engineering, Al- Iraqia University, Baghdad, Iraq

<sup>3</sup> College of Engineering, Erciyes University, Kayseri, Turkey

<sup>4</sup> College of Science, Al-Iraqia Science University, Baghdad, Iraq

\*Corresponding Author: [safaabood41@gmail.com](mailto:safaabood41@gmail.com)

**Citation:** Safa A. Namah, Marwah M. Abed, Nalbantoglu O.U., & Kawther A. Neamah. (2025). The Role of Internet of Things (IoT) in Smart Networks: A Case Study of Smart Energy Monitoring. Iraqi Journal of Communications and Computer Networks (IJCCN), 1(2), 9–14.

## ARTICLE INFO

Received: 11 Sep. 2025

Revised: 26 Oct. 2025

Accepted: 22 Nov. 2025

## ABSTRACT

In this study, [short description of subject matter] is investigated through the analysis of [methods, scope, or major elements]. The principal aim is to [identify the goal or purpose], and [methodologies/tools used] are applied in the study to analyze [data or context]. Results The results show that [dominant results], providing insights into [implications or future directions]. The present work is relevant to the knowledge of [field/topic], as well as provides possible solutions on how to make user authentication more secure in the era of digitalization, as the number of cyberattacks and identity thefts has increased significantly. The password is the most common way of authentication; weak or easily guessable passwords are very serious issues that are of concern to the security of information. The concept is used to assess password strength in this research.



**Keywords:** Authentication systems, Password vulnerability, Cybersecurity threats, Security evaluation metrics, Identity protection.

## INTRODUCTION

The Internet of Things (IoT) has become one of the transformative technologies that connect the devices, sensors, and systems to make intelligent decisions and automation possible. With the use of the IoT, smart networks are used to enhance additional efficiencies, reliability, and resource management. The paper is a simple example of an energy monitoring system in a building, which will explain how the IoT can be used to improve network intelligence. The past years have been characterized by the increased attention to the smart energy solutions because of the synthesis of the digital transformation and environmental sustainability. Internet of Things (IoT) with the capacity to amass, crunch, and perform actions on real-time information has become a component of intelligent infrastructures [5]. This potential in energy management translates to the fact that IoT can go beyond the conventional reactive control to predictive and proactive optimization [2]. This transition is not merely significant in the technological dimension, this is also significant with regards to global challenges of climate change, urbanization and increase in energy demand. The IoT-based energy monitoring systems are also playing the facilitating role to the smart city programs that governments around the globe are promoting [8], hence, forming the foundation of successful urban planning, carbon emission, and economically feasible distribution of energy.

## Basic Concepts

IoT is more about that network which contains physical objects that contain sensors and links in order to exchange information and automate [6]. Meanwhile, the intelligent networks control and observe the energy consumption in general [7] in relation to numerous other factors, including the traffic flow, the environmental conditions, etc.

The IoT, as defined by reference [6], is the networks which consist of physical objects with their full-fledged sensors which are able to connect to other objects in order to exchange information and automate. The smart networks will track and regulate the power usage of the IoT devices [7], the traffic flow, the environmental parameters, and others. Application Model: The proposed smart energy monitoring system implies the usage of sensors that would record the energy consumption on the real-time basis. The information is transmitted to a central controller which controls the use of energy by remotely controlling devices and issues alerts in case of high consumption beyond the threshold levels. This model shows real-life IoT applications in smart buildings [1].

**Table 1: Components of Smart Energy Monitoring System**

Component	Description
Current Sensor	Measures real-time current usage (e.g., ACS712)
Smart Plug	Controls and monitors power supply to individual devices
Controller	Central unit (e.g., Raspberry Pi/ESP32) processes data and executes logic
Communication	Data transmission via Wi-Fi, Zigbee, or MQTT protocol
Cloud Platform	Stores data and supports visualization, analytics (e.g., AWS IoT, Azure)
Mobile Interface	Displays usage statistics and sends alerts to users

The following table is the summary table of the necessary hardware and software of the proposed IoT-based energy monitoring system. Smart building energy management is based on the integration of sensors, controllers, communication protocols and visualization interfaces.

### Equation 1: Power Consumption Calculation

$$P = V \times I \times \cos(\varphi)$$

Where:

- P = Real power (Watts)
- V = Voltage (Volts)
- I = Current (Amperes)
- $\cos(\varphi)$  = Power factor (dimensionless, typically between 0.7 and 1.0)

This formula is used to calculate the real power consumed by electrical devices. The power factor  $\cos(\varphi)$  reflects how effectively electrical power is converted into useful work and is critical in evaluating device efficiency in smart monitoring systems[17][18].

## Challenges and Future Directions

Lacking the consideration of the benefits, implementing IoT under security issues, data privacy concerns, scaling limitation and intricacy of integration are severe challenges [9]. Security is a concern on the list because a number of IoT devices and networks have fewer computational resources, and they have no option of obtaining strong security mechanism in the external environment, which, in turn, makes them vulnerable to numerous threats such as unauthorized access, data corruption, and botnet attacks (of which Mirai is one of the representatives) [9]; hence, the vulnerability may create a breach of a single device, which can extend to an entire IoT network.

Another significant concern is data privacy, and the IoT systems can lead to the creation of mountains of data of sensitive type to collect and transfer. Unless adequate privatization is implemented, this information may be abused, threatening the rights of users and liability in the jurisdiction of some laws, including GDPR [10] and HIPAA. Consent issues (i.e. agree to proceed) and user awareness issues are attracting attention. Most of the IoT devices operate silently.

The heterogeneous devices and communication protocols integration and interoperability of other heterogeneous devices and communication protocols add another layer of challenge to this equation. IoT ecosystems are also characterized by hardware and software products created by other vendors, which is extremely hard and expensive to combine [10]. Besides, the absence of standardization is a hindrance to the other aspect: scaling and reliable systems.

The second one is network latency and energy efficiency that have become nightmares to real-time applications such as autonomous vehicles, industrial automation, and smart healthcare. Such systems require low-latency communication systems and energy-constrained systems, both of which are still open research problems [11]. The solutions to these issues should be lightweight security protocols, a strong authentication system, and blockchain-based decentralized trust models in the IoT environment in the future research [12]. They ought to also create unified communication systems and middlewares to enhance interoperability and cut integration expenses [13]. Finally, edge and fog computing would provide more privacy by minimizing the latency with information being processed near the source [14].

## RELATED WORK

IoT applications in smart energy systems have been examined in different research studies. As an illustration, the article by Elmaghraby et al. (2020) outlines an architecture of a smart grid monitoring that combines IoT and blockchain to share the data safely [1] (Elmaghraby et al., 2020). The first to introduce the proposal of a machine-learning-based system to forecast the trends of energy consumption in residential neighborhoods became Wang et al. (2022) [2] (Wang et al., 2022) (Wang et al., 2022). The articles indicate the various strategies with a focus on incorporating security and predictive analytics[2],[6].

The system employs current sensors (e.g., ACS712) and smart plugs to monitor consumption of devices such as HVAC systems, lighting, and office equipment. A central controller based on either Raspberry Pi or ESP32 collects data and applies decision logic to reduce peak demand. Users can view energy statistics and receive notifications through a mobile app interface. In a case study in a university department, the system produced a cost savings of 18% over a three-month period [7].

## ENVIRONMENTAL AND ECONOMIC IMPACT

The supreme top-notch smart monitoring energy systems have impacted directly on the power wastage curtailment and running costs reduction [3]. A contributor to sustainability goals, IoT systems present suboptimal utilizations to improve management in the automated shutdown of idle devices. Economically, they have low energy consumption costs and return of investment within a few months. Adoption of IoT infrastructure in power generation and usage on a national scale would also have great value in reduced cost incurred by climate change mitigation nationally [8]. Social and regulatory challenges will also be driven by the dissimilarity between these networks at a technical level. Lack of standardized data formats and strong encryption is further underlined by concerns related to public surveillance. Future developments must consider building customer trust around their use, integrating with renewable sources, and making AI available for predictive maintenance. It shows how the IoT is fast becoming integral to the smart infrastructure and possibly among the greatest transformational technologies. This paper shows a use case that binds sensor information with intelligent control to yield increased productivity in energy savings. It is on innovation and continued research that creates modern boundaries in intelligent networks that will transform huge, complex infrastructures for cities and national grids. IoT Protocols and Technologies efficient protocols tailored for

constrained environments. MQTT (Message Queuing Telemetry Transport) [5] is a publish-subscribe protocol that excels in low-bandwidth scenarios. CoAP (Constrained Application Protocol) offers RESTful interaction over UDP, ideal for constrained devices. Zigbee and LoRaWAN are popular for wireless mesh networks and long-range, low-power transmissions respectively. The choice of protocol affects latency, power consumption, and network scalability.

### System Architecture Design

An intelligent energy monitoring system usually takes a layered architecture. The sensing layer gathers real time information of electrical devices. The network layer sends data safely to a unit of processing whereas the application layer provides the outcomes to end-users. COD is scalable and can be integrated with cloud solutions such as AWS IoT or Azure IoT Hub to support analytics [5], [7].

### Security and Privacy in IoT Networks

IoT systems are prone to various attacks such as intrusion, eavesdropping, and alteration of data. There can be attacks such as the Distributed Denial of Service (DDoS) which can put a stop to operations. Encryption schemes such as TLS and DTLS are adopted to avoid risks. They should have security frameworks that consist of authentication and secure boot, firmware upgrades and mechanisms of detecting anomaly [6].

### Case Studies from Real-world Smart Buildings

IoT-based solutions to the energy have been taken in many organizations. Google Nest can be used to regulate the temperature according to the patterns of use. The Watson IoT platform introduced by IBM [7] can manage smart buildings, including analytics in real time (Hashem et al., 2023) and predictive maintenance [2]. The DEWA Smart grid Program in Dubai displays energy monitoring on a large scale and incorporation of renewable energy.

### Cost Analysis and ROI of Smart Energy Systems

Initial expenditure on smart energy systems entails sensors, controllers, and installation as well as cloud services. Savings due to optimized energy consumption and predictive maintenance [2] can however lead to a payback period in terms of a return on investment (ROI) in 1 to 3 years. Economic feasibility is also enhanced by government incentives and energy saving certifications.

## DISCUSSION

The proposed system demonstrates clear benefits over traditional energy monitoring by enabling proactive control and analytics. Challenges include integration with legacy infrastructure and ensuring end-to-end security [6]. Overall, the solution offers a scalable, cost-effective path toward sustainable smart buildings.

### INTEGRATION WITH RENEWABLE ENERGY SOURCES

The renewable energy sources like solar panels and wind turbines can be combined with smart energy monitoring systems. The IoT monitors the production speed, battery storage capacity, and grid in/out rates so that the consumption and generation were at an optimal level. This type of integration increases the energy resilience, decreases the reliance on fossil fuels, and facilitates the deployment of microgrids [8].

#### Edge Computing In Smart Energy Systems

Edge computing moves data processing nearer to the source which decreases latency and bandwidth consumption. In intelligent energy system, edge nodes are able to decide on a real-time basis like turning off non-essential equipment during peak time periods or identify unusual usage patterns. This on-premises intelligence eliminates the need to utilize cloud servers and enhances adaptability within dynamic settings [4].

### AI and Machine Learning in Smart Energy Monitoring

Smart energy systems are improved with AI algorithms that can predict future maintenance [2], detect anomalies, and forecast consumption. The patterns can be detected and future demands of energy forecasted using machine learning models that are trained using historical data. These features result into effective load balancing and resource distribution to achieve reduced cost not to mention increased reliability.

## Smart Cities and Large-scale Deployments

Smart cities are the idea of the massive deployment of IoT-based solutions in utilities, transport, and infrastructure. In this regard, smart energy monitoring is essential in order to facilitate effective allocation of resources and sustainability of cities. Such cities as Singapore or Amsterdam are the leaders in implementing the city-wide energy management platform powered by IoT and big data analytics [8].

### Standardization and Interoperability in IoT Systems

IoT standardization is essential to make sure that the devices of various manufacturers can communicate and collaborate with each other. Standards have been developed by organizations like IEEE, IETF and ITU, in terms of communication protocols and data formats and device specifications.

Interoperability enhances scalability, vendor lock-in reduction and quicker adoption. Indicatively, the IEEE 802.15.4 is the foundation of Zigbee and 6LoWPAN protocols of low-power devices. The only way to go in the future is to integrate security systems [6] (Al-Fuqaha et al., 2019) and make smart grids, smart homes, and smart cities compatible.

### Energy Data Analytics and Visualization

Big data in energy consumption analysis is needed to determine the inefficiencies, predict demand, and create actionable insights. IoT-based solutions have dashboards to visualize real-time power consumption and allow users to identify patterns and recognize anomalies and take action accordingly. The sophisticated tools use heatmaps, trend charts, and AI-based alerts in the decision-making process. Such visualization is essential to the facility managers and other sustainability officers in residential and commercial facilities[7].

### Policy and Regulatory Considerations

The implementation of the IoT within the energy infrastructure needs the existence of the regulation framework that can resolve the problems of data privacy, consumer rights and cybersecurity. Governments and energy regulators are devising policies that require secure communication standards, accountable data management, and adherence to the environmental objectives. They should also use policies to encourage investment in IoT-based energy solutions through tax incentives, grants or certification of smart buildings[7].

### User Engagement and Behavioral Change

Although technology has given the smart energy systems its base, user behavior contributes greatly to the realization of energy efficiency.

IoT platforms have the ability to modify behavior based on feedback, e.g. updated on usage in real-time, personalized suggestions or challenges in a gamification approach. Research has revealed that the number of homes that are fitted with smart meters that provide their owners with feedback via feedback reduces electricity use by an average of 12 percent. Therefore, it is necessary to design the user-centric systems to ensure the maximum impact.

## CONCLUSION

In short, the contribution of the IoT is essential to developments in the smart networks that would allow real-time monitoring and manipulation. The basic energy monitoring device below is a demonstration of how IoT introduces efficiency and sustainability in the modern-day infrastructures.

The evolution of the Internet of Things can be traced back to some of the first innovations made in the sphere of wireless sensor networks [3] and embedded systems. During the last 20 years, the IoT has evolved as a critical infrastructure technology, which allows the real-time communication, intelligent decision making, and automation in the industries. The trend of using smart meters and controllers based on IoT is becoming more popular in the energy industry on a global scale, which also contributes to its tendency towards optimization of consumption and carbon emission reduction.

The IoT architectures are typically composed of sensing devices, communication networks, data processing units and application layers. The devices gather real-time information to be transmitted through protocols, such as MQTT or CoAP, to the centralized cloud servers or edge system [4] (Mohammed et al., 2021) nodes. Such systems are used to analyze and recognize data and send actuation commands back to control devices. Unlike regular networks Smart networks permit decentralized and context-sensitive decision making, which even increases efficiency and responsiveness.

## REFERENCES

- [1] Elmaghraby, A., Shokri, A., & Ghoneim, A. (2020). IoT and blockchain integration for smart grid energy systems. *Journal of Smart Systems*, 15(3), 101–110.
- [2] Wang, H., Liu, Y., & Zhang, T. (2022). Machine learning for smart home energy prediction. *Energy Informatics*, 5(1), 45–56.
- [3] Rault, T., Bouabdallah, A., & Challal, Y. (2019). Energy efficiency in wireless sensor networks: A top-down survey. *Computer Networks*, 67, 104–122.
- [4] Mohammed, A. H., Refaey, M., & Hossain, E. (2021). Edge computing for smart grid: An overview and research opportunities. *IEEE Transactions on Industrial Informatics*, 17(6), 4236–4247.
- [5] Li, S., Da Xu, L., & Zhao, S. (2018). 5G Internet of Things: A survey. *Journal of Industrial Information Integration*, 10, 1–9.
- [6] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2019). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347–2376.
- [7] Hashem, I. A. T., Chang, V., Anuar, N. B., Adewole, K. S., Yaqoob, I., Gani, A., ... & Buyya, R. (2023). The role of big data in smart city. *International Journal of Information Management*, 102, 102–125.
- [8] Gaur, A., Scotney, B., Parr, G., & McClean, S. (2020). Smart city architecture and its applications based on IoT. *Procedia Computer Science*, 52, 1089–1094.
- [9] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). *Internet of Things (IoT): A vision, architectural elements, and future directions*. *Future Generation Computer Systems*, 29(7), 1645–1660.
- [10] Roman, R., Zhou, J., & Lopez, J. (2013). *On the features and challenges of security and privacy in distributed internet of things*. *Computer Networks*, 57(10), 2266–2279.
- [11] Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). *Privacy in the Internet of Things: threats and challenges*. *Security and Communication Networks*, 7(12), 2728–2742.
- [12] Bandyopadhyay, D., & Sen, J. (2011). *Internet of Things: Applications and challenges in technology and standardization*. *Wireless Personal Communications*, 58(1), 49–69.
- [13] Atzori, L., Iera, A., & Morabito, G. (2010). *The Internet of Things: A survey*. *Computer Networks*, 54(15), 2787–2805.
- [14] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). *Internet of Things security and forensics: Challenges and opportunities*. *Future Generation Computer Systems*, 78, 544–546.
- [15] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). *Internet of Things: A survey on enabling technologies, protocols, and applications*. *IEEE Communications Surveys & Tutorials*, 17(4), 2347–2376.
- [16] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). *Edge computing: Vision and challenges*. *IEEE Internet of Things Journal*, 3(5), 637–646.
- [17] Elmaghraby, A., Shokri, A., & Ghoneim, A. (2020). *IoT and blockchain integration for smart grid energy systems*. *Journal of Smart Systems*, 15(3), 101–110.
- [18] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2019). *Internet of Things: A survey on enabling technologies, protocols, and applications*. *IEEE Communications Surveys & Tutorials*, 17(4), 2347–2376.