MJFAS
Malaysian Journal of Fundamental and Applied Sciences

RESEARCH ARTICLE

Design a Crime Detection System based Fog Computing and IoT

Safa Riyadh Waheed[a,c], Ammar AbdRoba Sakran[b], Mohd Shafry Mohd Rahim[c], Norhaida Mohd Suaib[c], Fallah H Najjar[d], Karrar A Kadhim[a,c], Ali Aqeel Salim[f*], Myasar Mundher Adnan[g]

[a]Computer Techniques Engineering Department, Faculty of information Technology, Imam Jaafar Al-sadiq University, Iraq; [b]College of Biomedical Informatics, University of Information Technology and Communications (UOITC), Baghdad, Iraq; [c]Faculty of Engineering, School of Computing, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Johor, Malaysia; [d]Department of Computer Systems Techniques, Technical Institute of Najaf, Al-Furat Al-Awsat Technical University, Iraq; [f]Laser Center and Physics Department, Faculty of Science, Universiti Teknologi Malaysia, Johor, Malaysia; [g]Islamic University, Najaf, Iraq

Abstract The Internet of Things (IoT) is a cutting-edge innovation that facilitates the cost-effective development of smart system architectures. Although current regulations necessitate installing an analog fire alarm system, such a system lacks the intelligence to instantly notify the appropriate parties in a timely fashion. In addition, since people are not always present, an analog fire alarm will not be able to prevent immediate danger or damage in the event of a fire. Therefore, the incident must be reported as soon as possible to the appropriate party in order to lessen the impact of a fire. In this study, we suggest a smart fire-alarm system made of a fire sensor and a sound sensor that can both detect fire and noise as well as the status of the analog fire alarm system to ascertain whether the analog fire alarm system is operational. We first tested our proposed smart fire alarm system to determine its effectiveness before putting it into use. From there, we ran experiments to determine how well it worked. The outcomes show that the system is trustworthy in a range of scenarios.

Keyword: IoT, fog computing, microcontroller, smart city, smart home.

Introduction

With the Internet of Things (IoT) concept, more physical objects can be connected to the web. For instance, smart homes' control and monitoring systems include intrusion alarms, fire alarms, and thermostats. As a result, the IoT plays a significant and visible role in enhancing public life in various contexts, frameworks, fields, and settings. Furthermore, through the IoT, all these physical objects can talk to one another, sharing information and collaborating on decisions as they observe, listen, think, and carry out their respective tasks [1]. The term "Fog computing" refers to the extension of cloud computing towards the edge of networking, which enables the operation of storage, computation, and networking services between end devices and data centers. Hence, Fog computing is also known as edge computing [2-4]. Edge computing is typically referred to as a location responsible for the instantiation of services, Fog computing refers to the ease of computation, and storage resources and services are located close to devices and systems under end users' control. Although an IoT device directs some services and processes to the network's edge using Fog computing, other applications are still managed using the cloud, which provides data linkage [5]. Cloud computing provides end users access to data, information, and software programs. However, cloud computing is often complemented by the Fog paradigm, which speeds up operations and distributes communication and computation services to devices controlled by end-users; on a larger geographical scale, cloud computing is often used alone [6,7]. Fog computing's primary goal is to lessen the need for data to be sent to the cloud for tasks like processing and analysis and to keep it there for safekeeping.

***For correspondence:**
asali@utm.my

Received: 13 Oct. 2022
Accepted: 11 April 2023

10.11113/mjfas.v19n3.2906

Consequently, it is also utilized for logical, performance, and security reasons; it has an additional layer of an edge that supports and resembles those of cloud computing and IoT applications [8]. Furthermore, low corresponding state-of-the-earth resolutions are provided. Finally, cloud computing and IoT gadgets are separated by a layer of Fog, which facilitates communication and information sharing between the two. Besides, early standards examined cloud computing's inherited properties, such as integrity, confidentiality, availability, trust and reputation, and authentication.

Computer vision is a fascinating IoT application's ability to detect and recognize people's faces. IoT platforms incorporating computer vision systems can provide enhanced security for smart homes, detecting when a person is in the wrong place and, consequently, whether that person is a bad fit for their surroundings.

Related Works

Every organization has an information desk that provides customers and employees with information, advertisements, and numerous notifications. The challenge is that it calls for a team of people solely responsible for that task and always has the most recent information regarding the company and its advertising offers [9]. In addition, there are now numerous connected gadgets around us, thanks to the IoT. Many anticipate that sensing and actuation, many embedded in "things," will one-day cover cities and the world, ushering in the era of the "smart world." Work along these lines has been done by many people all over the world. In addition to its use in the criminal justice system, the Design a Crime Detection System can be put to good use in other settings, such as in schools and public transportation hubs like train stations, bus terminals, and airports. The temperature sensor is also utilized for climate regulation in the mall's central air conditioning system [10]. Its utility extends beyond commercial enterprises to include industrial institutions. Some places where the IoT is commonly used include hospitals, where an E-display system may show emergency messages [11-13]. This section will examine the most recent research in the Fog computing environment, as shown in Table 1, where security is a particularly serious issue due to the dispersed nature of data storage.

Regarding cloud computing, users are most concerned about security and privacy [14]. Although various approaches to fog computing have been studied in academia and industry, data security and privacy protection are becoming more crucial for the advancement of fog computing technology in business, industry, and government [15]. Vehicular fog computing (VFC), which makes use of moving cars as nodes in a distributed network of sensors and processors, was first proposed by Hou *et al*. [16]. They advised using this framework to enhance user interaction and computation by combining the resources of each vehicle. After conducting a quantitative analysis of VFC's capabilities, the authors presented four scenarios in which stationary and moving vehicles act as the central nodes of communication and computation. To better communicate certificate revocation information across IoT devices, for instance. [17] investigated security and privacy concerns in IoT contexts and suggested a technique to improve security that makes use of the Fog. They also offered a case study demonstrating how fog computing was utilized to safely disseminate data regarding revoked certificates in IoT settings.

Therefore, in [18], a framework was provided to comprehend, investigate, and model service delays in IoT-Fog-cloud application situations.In order to lessen service delays to IoT nodes, also suggested a policy for Fog nodes to adhere to. Their suggested strategy employs inter-Fog communication to reduce service wait times. [19] Focused on mobile IoT devices and the primary problems that would arise while studying mobility support in a Fog computing environment. Moreover, they detailed three scenarios in which mobility support is crucial in integrating the IoP and Fog computing. Furthermore, Sookhak *et al*. [20] introduced VFC to use vehicles' idle resources to increase the efficacy of Fog computing. To further elaborate on the decision-making processes and the distribution of services across vehicles as Fog nodes, they presented a cross-layer architecture for VFC.

Additionally, to determine the vulnerabilities inherent in existing Fog computing models. [21] Performed an analysis of Fog computing programs in order to spot typical security flaws. They said that many Fog platforms are insecure because developers of these apps tend to prioritize functionality over security. Therefore, they aimed to give future security-relevant directions for Fog computing by analyzing the impact of security problems and potential remedies. Furthermore, Mahmud *et al*. [22] introduced a classification scheme for Fog computing that considers the technology's many difficulties and characteristics. Finally, Table 1 illustrates an overview of the Fog computing and IoT integration literature, emphasizing each paper's unique contribution and grouped in reverse chronological order.

Table 1. An overview of Fog computing and IoT integration

Author	Year	Method
Mahmud *et al*. [17]	2018	Introduced a classification scheme for Fog computing that considers the technology's many difficulties and characteristics
Khan *et al*. [16]	2017	Performed an analysis of Fog computing programs in order to spot typical security flaws
Sookhak *et al*. [15]	2017	Introduced VFC to make use of vehicles' idle resources to increase the efficacy of Fog computing
Puliafito *et al*. [14]	2017	Focused on mobile IoT devices and the primary problems that would arise while studying mobility support in a Fog computing environment
Yousefpour *et al*. [13]	2017	Proposed a new framework to comprehend, analyze, and model service delays in IoT-Fog-cloud application scenarios
Alrawais *et al*. [12]	2017	Presented a mechanism for enhancing security that uses the Fog to disseminate certificate revocation information among IoT devices better and explored security and privacy concerns in IoT settings
Hou *et al*. [11]	2016	Introduced the concept of VFC, which uses moving automobiles as nodes in a distributed network of sensors and processors.

IoT: Its Current State and the Challenges It Faces

IoT is a concept that centers on the pervasive presence of networked, communicative smart gadgets in everyday life and surroundings. According to CISCO's predictions, web-connected devices surpassed the human inhabitants at 2010 and are expected to reach over 50 billion by 2020 [23]. Despite these tricks' relatively low point bandwidth requirements, they generate massive amounts of information that need to be saved, processed, and presented transparently and straightforwardly [24-26].

Consequently, as it is typically organized nowadays, IoT architecture is depicted at a high level in Figure 1. The four main pillars of the Internet of Things are sensing devices (things), local communication networks, internet clouds, and back-end IoT applications. Sensing technology is used to gather data about the physical world. In the end, IoT applications (like those for smart transportation, healthcare, precision agriculture, video surveillance, etc.) use these insights to better serve customers. Due to the limited storage and processing power of most IoT devices, most applications rely on cloud services to handle data collection, management, and analysis. Different sensing gadgets use various forms of communication to link up with the cloud. The more robust ones either have built-in support for 3G or 4G cellular networks or link to the Internet gateway via Wi-Fi or Ethernet. However, some devices cannot handle the high power requirements of these communication models (e.g., battery-operated devices). Other technologies, such as Bluetooth, ZigBee, and NFC, facilitate short-range communication between low-power devices (Near-Field Communication). After the raw data produced by one or more sensing sources has been properly processed in the cloud, the end user is given the pertinent insights. For example, it could be another M2M (Machine-to-Machine) workflow device serving a commercial or industrial client.

The cloud provides scalable and low-cost options for managing IoT-generated data. Furthermore, the storage, processing power, and energy constraints of IoT devices are mitigated by this system, allowing for analysis of hitherto unimaginable complexity [27]. Also, If concerned about the costs of deployment and ongoing operations, the "pay as you go" model of cloud computing offers a more practical option for the ownership and management of private data centers (D.Cs). The current Cloud services, on the other hand, were initially created for conventional Web applications, which are not significantly impacted by the distance between edge devices and data centers. On the other hand, many new Internet of Things applications (such as intelligent traffic lights and target tracking systems) demand real-time interaction and mobility support, making network latency a significant limiting factor. Moreover, IoT devices are located far from the cloud, which is not the only factor contributing to network latency.

Additionally, it is brought on by queuing delay, which is not something that can be ignored on congested networks. If the traffic volume were to be dispersed uniformly across the network, the effect of queue delays may be mitigated. Unfortunately, under the current architecture of the Internet, which is characterized by a dispersed control plane, dynamic routing is regarded as having a lower potential for risk than it has for the benefit [28].

10.11113/mjfas.v19n3.2906

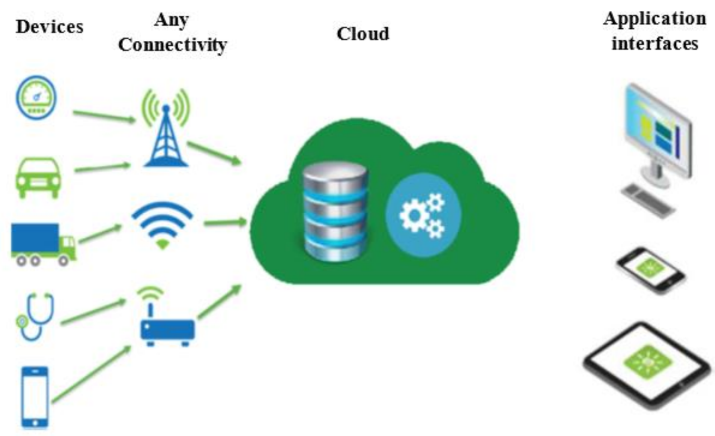

Figure 1. Traditional IoT architecture

In addition, the most common form of deployment is the straightforward shortest path routing architecture. In addition, there is a dearth of specialized mechanisms for controlling connection. This issue needs to be fixed to properly capitalize on the opportunities presented by diverse access networks in IoT scenarios.

Fog Computing (FC)

The following subsections cover the basics of Fog computing and its features, advantages, and architecture.

Fog Computing Definition

Fog computing is a limited-capabilities computing model, similar to standard cloud computing, in that it involves the distribution of processing, storage, and networking services across many end devices. As a result, it is an excellent option for real-time IoT programs that cannot afford any gap [29]. While Cisco [30] may have been the first to use the phrase "Fog computing," it has since been characterized in various ways by academics and businesses. [31] provided a general definition of Fog computing. It is stated, "Fog Computing is a geographically distributed computing architecture with a resource pool which consists of one or more ubiquitously connected heterogeneous devices (including edge devices) at the edge of the network and not exclusively seamlessly backed by Cloud services, to collaboratively provide elastic computation, storage and communication, and many other new services and tasks, in isolated environments to a large scale of clients in proximity." The authors in [31, 32] defined FC as; "a scenario where a huge number of heterogeneous, wireless and sometimes autonomous, ubiquitous and decentralized devices communicate and potentially cooperate among them and with the network to perform storage and processing tasks without the intervention of third parties. These tasks can support basic network functions or new services and applications running in a sandboxed environment. Users leasing part of their devices to host these services get incentives for doing so". FC is also defined by the Open Fog Consortium [33] as; "a system-level horizontal architecture that distributes resources and services of computing, storage, control and networking anywhere along the continuum from Cloud to Things."

Fog Computing Characteristics

An extension of the cloud that is physically closer to the IoT data processing equipment is fog computing. Fog computing, as shown in Figure 2, acts as a conduit between end devices and the cloud, bringing compute, storage, and network capabilities closer to the devices themselves. These devices are commonly referred to as fog nodes. They can be installed almost anywhere as long as there is an active internet connection. Industrial controls, switches, routers, embedded servers, and security cameras are all examples of Fog nodes [34-37] because to their ability to compute, store data, and connect to a network.

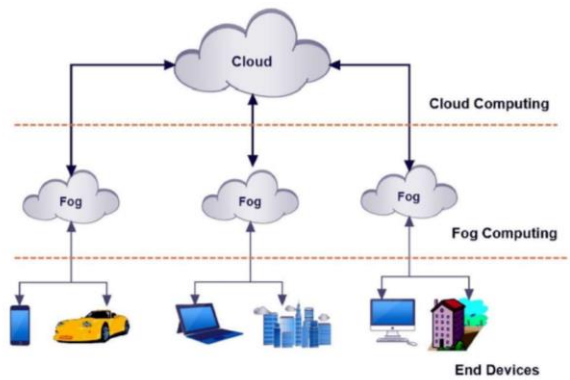

Figure 2. Fog computing is an expansion of cloud computing closer to the end devices.

One could say that Fog computing is the foundation upon which the cloud rests. The following is a summary of the features that define Fog computing, as described in [31,38] :

- Heterogeneousness: Fog nodes, also known as end devices, are manufactured by various companies and come in various shapes, sizes, and platform requirements. Therefore, the Fog is compatible with a variety of systems.
- Interoperability: Various domains and service providers are compatible with Fog components.
- Real-time interactions: In contrast to the batch processing used by the cloud, applications built for Fog computing enable real-time interactions between Fog nodes.
- Support for online analytics and interplay with the cloud: Positioned in-between cloud resources and client devices, Fog plays a crucial part in data ingestion and local processing.
- Mobility support: Fog applications rely heavily on a distributed directory system, and their capacity to connect directly to mobile devices is a key component in enabling mobility techniques like the Locator ID Separation Protocol (LISP).
- Location awareness and low latency: As Fog nodes can be placed anywhere, the network must be aware of its surroundings. Additionally, the Fog's proximity to end devices means that its data processing reduces latency.
- Scalability: The environment is constantly being monitored by vast networks of sensors. Large-scale end devices can access Fog's dispersed computing and storage resources.
- Geographical distribution: Unlike those hosted in a centralized cloud, Fog services, and applications are location independent and can be used independently of one another.

The construction of Fog Computing

FC is a method that moves some tasks from a data center for the network's periphery. The Fog is an extension of the classic cloud computing model in which data centers are supplemented by end-user devices to provide computing, storage, and networking services. Fog computing's main goal is to supply time-sensitive IoT applications with low and predictable latency [39]. As shown in Figure 3, the six layers that structure FC architecture is comprised of the physical and virtualization layer [40], the monitoring layer [41], the pre-processing layer [42], the temporary storage layer [43], the security layer [44], and the transport layer [45].

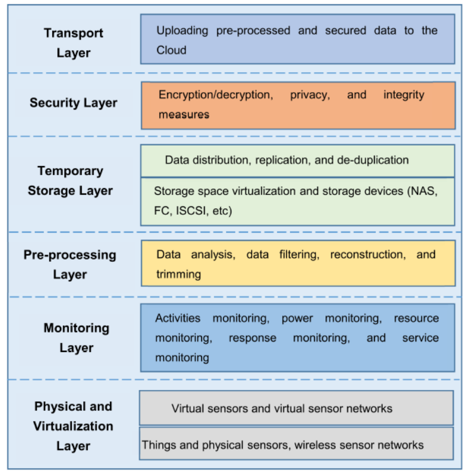

Figure 3. Layered architecture of Fog computing.

Several types of nodes, including physical, virtual, and virtual sensor networks, make up the physical and virtualization layer. Each different kind of node has different requirements for management and upkeep. The environment is sensed by a network of dispersed sensors, which then relay that information through a series of gateways to the higher levels for analysis and refinement [43, 44]. At the monitoring layer, we keep an eye on how well our resources are being used, how reliable our sensors and Fog nodes are, and how stable our networks are. This layer keeps track of all the work done by the network's nodes, keeping tabs on which ones are doing what, when, and what comes next. Additionally, the health and availability of all infrastructure-deployed applications and services are tracked [42-46].

The data management tasks are executed in the pre-processing layer. In this stage, the collected data is analyzed, and useful information is extracted through data filtering and trimming. Next, the data are placed in a temporary storage layer while being finalized for use. When data are uploaded to the cloud, they are no longer required to be kept locally so that the intermediary storage devices can be discarded [40, 46]. Finally, encryption and decryption are important functions of the security layer.

Additionally, the data can be safeguarded against manipulation via integrity measures. After pre-processing, data are uploaded to the cloud in the transport layer so that additional services can be generated and extracted [40, 46]. To conclude, in order to save space and bandwidth, just a portion of data is uploaded to the cloud. To put it another way, the data are processed at the gateway device before being uploaded to the cloud. "gateway" means "smart gateway" [47,48] here.

Sensor networks collect data and send it to the cloud via smart gateways for Mechanical and electronic gadgets connected to the web. The data collected from these numerous sources is then used to power the many user-facing services that make up cloud computing [49, 50]. Considering Fog's meager resources, a Fog computing communication protocol must be highly effective, lightweight, and flexible. Therefore, Fog's application scenario should guide the communication protocol selection [51-53].

Methodology

Protection of privacy requires a great deal of labor. The development of standards is the result of ongoing, in-depth study on IoT privacy protection technology. People's grasp of privacy protection is profound, and their awareness of it is increasingly obvious, which is the main manifestation. For instance, if user information is required, the service provider must clearly define the scope, approach, and purpose of data collection and use. While using data, the user should have the freedom to discover the truth. At this point, there are a lot more standards, and privacy protection management and technology have been vastly enhanced in terms of standardization. The logical use of private information has entered an inertial and unstoppable trend.

The IoT architecture model described in this section makes use of both the Fog computing paradigm and our design system. The suggested remedy is inspired by recent works. As stated earlier, the significant issues addressed in this study included the poor performance of the Crime Detection System. Here, the researchers have described the stages of the proposed framework used in this research. This study attempted to propose and develop to Design a Crime Detection System Based on Fog Computing and IoT.

We use the camera to capture images whenever a PIR sensor detects motion in the proposed system. The captured images will then be run through a computer vision module to locate the faces. Once that is done, we will pack it up and send it to Smartphone via mail. If we are serious about securing the area, this system is essential. Therefore, motion detection and facial recognition are the two main features of the application. The system will not proceed to facial recognition if no motion is detected.

In any case, if motion was detected, the face identification algorithm will take into account the motion in the current frame. The suggested system's entire research structure is shown in Figure 4. All the fundamentals of burglary and fire detection are included in the scheme's structure.

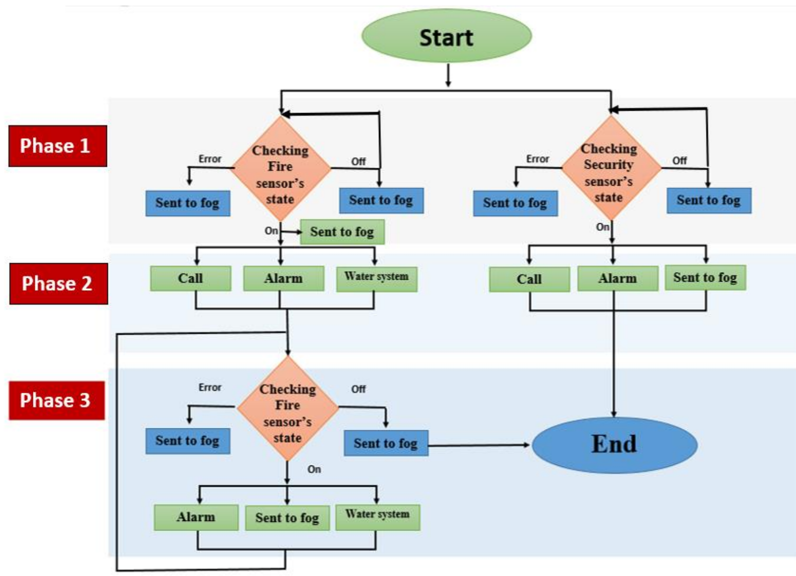

Figure 4. Framework diagram

Phase 1: In the first part of the diagram, the system will monitor the state of the sensors if they are working correctly and make sure to monitor the change of state and send the data to the Fog computing.

Phase 2: In this part of the diagram, it shows the procedures that the system performs when changing the sensor's state to a fire alarm or intrusion alarm, such as contacting the system administrator, activating the firefighting system, sending data to Fog computing, and contacting the authorities that will control the penetration or the fire.

Phase 3: In this section of the diagram, the system will monitor the changes in the sensor's state until the building is controlled

Result and Discussion

The introduced system typically consists of two main components, the first of which is concerned with home security and the latter of which is used for automatic control. The Arduino is used to program both components, which are based on Arduino microcontrollers. The infrared (IR) sensor and the fire alarm form the foundation of the home's security system. The burglar must cross in front of the IR sensor for the sensor to immediately return a logic value to the Arduino Nano kit, which switches on the alarm sound. Additionally, the fire alarm sensor will act similarly. The Arduino Nano follows the previously described protocol when there is a fire.

When it comes to responding to emergencies, the Internet of Things allows for speedier reactions because to reduced need for software development. Most fire alarms, however, are designed in such a way that the sensor reliably identifies the places at which the alarm should go off. Both the Penetration alarm and the fire detection alarm will trigger when sensing a fire, but the fire sensor can provide more precise data.. A version of codes that includes looping has been attached to the system Figure 5 and Figure 6. The face detection process is given in Figure 6. The first step is to run the raw image through the face detector. In order to weed out bogus candidates, the spatial correlation of face parts between models and detected regions will be taken into account after the "faces" have been sent out. True identities will be protected at last.

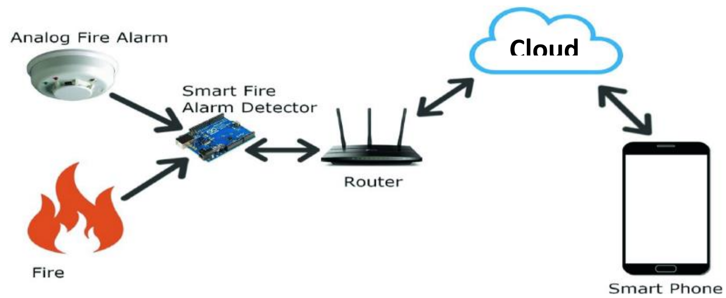

Figure 5. The shortest response time can provide faster reaction

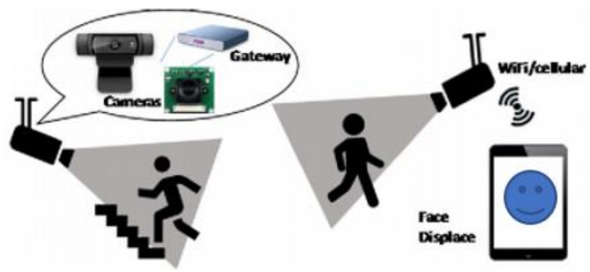

Figure 6. Faster reaction can be reached by the shortest response time

Conclusion

Due to the two exabytes of data produced daily by the Internet of Things, cloud computing now has a partner in fog computing to help it process this data. As a result, the problems caused by the explosion in data volume, variety, and velocity can be overcome by processing data nearer to where it is produced and needed. In addition, fog computing speeds up detection and reaction to events by avoiding a return trip to the cloud for analysis. Finally, diverting terabytes of data away from the main network eliminates the need for expensive bandwidth upgrades. Furthermore, it safeguards private IoT data by processing it internally. Ultimately, organizations that adopt Fog computing gain more profound and faster insights, leading to increased business agility, higher service levels, and improved safety. Home security using the Internet of Things has been experimentally proven to work satisfactorily by connecting simple appliances to it, and the appliances were successfully controlled remotely through the Internet. The designed system not only monitors the sensor data, like temperature, gas, light, and motion sensors but also actuates a process according to the requirement.

Conflicts of Interest

The author(s) declare(s) that there is no conflict of interest regarding the publication of this paper.

Acknowledgements

Researcher are thankful to the Universiti Teknologi Malaysia (UTM), Ministry of Higher Education Malaysia (MOHE), and RMC for the research financial support under the FRGS Q.J130000.2509.21H11, UTMFR, and UTM RA ICONIC GRANT Q.J130000.4354.09G60 grants. Authors are also grateful to Research Management Centre-Universiti Teknologi Malaysia (RMC-UTM) for supporting under Postdoctoral fellowship scheme.

References

[1] 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.

[2] Yi, S., Li, C., & Li, Q. (2015, June). A survey of fog computing: concepts, applications and issues. *Proceedings of the 2015 Workshop on Mobile Big Data* (pp. 37-42).

[3] Salim, A. A., Bakhtiar, H., Krishnan, G., & Ghoshal, S. K. (2021). Nanosecond pulse laser-induced fabrication of gold and silver-integrated cinnamon shell structure: Tunable fluorescence dynamics and morphology. *Optics & Laser Technology*, *138*, 106834.

[4] Salim, A. A., Bidin, N., & Islam, S. (2017). Low power CO_2 laser modified iron/nickel alloyed pure aluminum surface: Evaluation of structural and mechanical properties. *Surface and Coatings Technology*, *315*, 24-31.

[5] Waheed, S. R., Adnan, M. M., Suaib, N. M., & Rahim, M. S. M. (2020, April). Fuzzy logic controller for classroom air conditioner. In *Journal of Physics: Conference Series*, *1484*(1), 012018. IOP Publishing.

[6] Deep, S., Zheng, X., Jolfaei, A., Yu, D., Ostovari, P., & Kashif Bashir, A. (2022). A survey of security and privacy issues in the Internet of Things from the layered context. *Transactions on Emerging Telecommunications Technologies*, *33*(6), e3935.

[7] Salim, A. A., Ghoshal, S. K., Shamsudin, M. S., Rosli, M. I., Aziz, M. S., Harun, S. W., ... & Bakhtiar, H. (2021). Absorption, fluorescence and sensing quality of Rose Bengal dye-encapsulated cinnamon nanoparticles. *Sensors and Actuators A: Physical*, *332*, 113055.

[8] Najjar, F. H., Al-Jawahry, H. M., Al-Khaffaf, M. S., & Al-Hasani, A. T. (2021, April). A novel hybrid feature extraction method using LTP, TFCM, and GLCM. *Journal of Physics: Conference Series*, *1892*(1), 012018. IOP Publishing.

[9] Kadhim, K. A., Adnan, M. M., Waheed, S. R., & Alkhayyat, A. (2021). Automated high-security license plate recognition system. *Materials Today: Proceedings*.

[10] Lin, C. R. (2006). System and method of remotely controllable home network system for domestic appliances. Patent TW I, 319945.

[11] Belaid, S. L., Boudries, Z., & Aoumer, A. (2020). Direct power control improvement using fuzzy switching table of grid connected PV system. *ICREEC 2019: Proceedings of the 1st International Conference on Renewable Energy and Energy Conversion* (pp. 85-92). Springer Singapore.

[12] Salim, A. A., Bakhtiar, H., Bidin, N., & Ghoshal, S. K. (2018). Antibacterial activity of decahedral cinnamon nanoparticles prepared in honey using PLAL technique. *Materials Letters*, *232*, 183-186.

[13] Hathot, S. F., Jubier, N. J., Hassani, R. H., & Salim, A. A. (2021). Physical and elastic properties of TeO_2-Gd_2O_3 glasses: Role of zinc oxide contents variation. *Optik*, *247*, 167941.

[14] Howe, D., Kohli, R., Smith, M., Parkinson, C., McMahon, L., Solomon, R., ... & Walsh, J. (2018). *Relationship-based social work: Getting to the heart of practice*. Jessica Kingsley Publishers.

[15] Yi, S., Qin, Z., & Li, Q. (2015). Security and privacy issues of fog computing: A survey. *Wireless Algorithms, Systems, and Applications: 10th International Conference, WASA 2015, Qufu, China, August 10-12, 2015, Proceedings 10* (pp. 685-695). Springer International Publishing.

[16] Hou, X., Li, Y., Chen, M., Wu, D., Jin, D., & Chen, S. (2016). Vehicular fog computing: A viewpoint of vehicles as the infrastructures. *IEEE Transactions on Vehicular Technology*, *65*(6), 3860-3873.

[17] Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the internet of things: Security and privacy issues. *IEEE Internet Computing*, *21*(2), 34-42.

[18] Yousefpour, A., Ishigaki, G., & Jue, J. P. (2017, June). Fog computing: Towards minimizing delay in the internet of things. *2017 IEEE international conference on edge computing (EDGE)* (pp. 17-24). IEEE.

[19] Waheed, S. R., Rahim, M. S. M., Suaib, N. M., & Salim, A. A. (2023). CNN deep learning-based image to vector depiction. *Multimedia Tools and Applications*, 1-20.

[20] Sookhak, M., Yu, F. R., He, Y., Talebian, H., Safa, N. S., Zhao, N., ... & Kumar, N. (2017). Fog vehicular computing: Augmentation of fog computing using vehicular cloud computing. *IEEE Vehicular Technology Magazine*, *12*(3), 55-64.

[21] Khan, S., Parkinson, S., & Qin, Y. (2017). Fog computing security: a review of current applications and security solutions. *Journal of Cloud Computing*, *6*(1), 1-22.

[22] Mahmud, R., Kotagiri, R., & Buyya, R. (2018). Fog computing: A taxonomy, survey and future directions. *Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives*, 103-130.

[23] Hussain, G. A., & Audah, L. (2020). BCH codes for 5G wireless communication systems over multipath fading channel. *Indonesian Journal of Electrical Engineering and Computer Science*, *17*(1), 310-316.

[24] Waheed, S. R., Suaib, N. M., Rahim, M. S. M., Adnan, M. M., & Salim, A. A. (2021, April). Deep learning algorithms-based object detection and localization revisited. *Journal of Physics: Conference Series, 1892*(1), 012001. IOP Publishing.

[25] Salim, A. A., Bakhtiar, H., Ghoshal, S. K., & Huyop, F. (2020). Customised structural, optical and antibacterial characteristics of cinnamon nanoclusters produced inside organic solvent using 532 nm Q-switched Nd: YAG-pulse laser ablation. *Optics & Laser Technology*, *130*, 106331.

[26] Salim, A. A., Ghoshal, S. K., & Bakhtiar, H. (2021). Tailored morphology, absorption and bactericidal traits of cinnamon nanocrystallites made via PLAL method: Role of altering laser fluence and solvent. *Optik*, *226*, 165879.

[27] Bai, T. D. P., & Rabara, S. A. (2015, August). Design and development of integrated, secured and intelligent architecture for internet of things and cloud computing. *2015 3rd International Conference on Future Internet of Things and Cloud* (pp. 817-822). IEEE.

10.11113/mjfas.v19n3.2906

[28] Tomovic, S., Radusinovic, I., & Prasad, N. (2015, September). Performance comparison of QoS routing algorithms applicable to large-scale SDN networks. *IEEE EUROCON 2015-International Conference on Computer as a Tool (EUROCON)* (pp. 1-6). IEEE.

[29] Atlam, H. F., Alenezi, A., Alharthi, A., Walters, R. J., & Wills, G. B. (2017, June). Integration of cloud computing with internet of things: challenges and open issues. *2017 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)* (pp. 670-675). IEEE.

[30] Ai, Y., Peng, M., & Zhang, K. (2018). Edge computing technologies for Internet of Things: a primer. *Digital Communications and Networks*, *4*(2), 77-86.

[31] Verma, M., Bhardwaj, N., & Yadav, A. K. (2016). Real time efficient scheduling algorithm for load balancing in fog computing environment. *Int. J. Inf. Technol. Comput. Sci*, *8*(4), 1-10.

[32] Yi, S., Hao, Z., Qin, Z., & Li, Q. (2015, November). Fog computing: Platform and applications. *2015 Third IEEE workshop on hot topics in web systems and technologies (HotWeb)* (pp. 73-78). IEEE.

[33] Khudhair, Z. N., Mohamed, F., & Kadhim, K. A. (2021, April). A review on copy-move image forgery detection techniques. *Journal of Physics: Conference Series*, *1892*(1), 012010. IOP Publishing.

[34[Salim, A. A., Ghoshal, S. K., Bakhtiar, H., Krishnan, G., & Sapingi, H. H. J. (2020, April). Pulse laser ablated growth of Au-Ag nanocolloids: Basic insight on physiochemical attributes. *Journal of Physics: Conference Series*, *1484*(1), 012011. IOP Publishing.

[35] Hussein, M. L., Kadhim, G. A., & Salim, A. A. (2021). Tailored physical and optical traits of TiO thin film formed via spray pyrolysis strategy: influence of annealing temperature change. *NeuroQuantology*, *19*(3), 32.

[36] Salim, A. A., Bidin, N., Ghoshal, S. K., Islam, S., & Bakhtiar, H. (2018). Synthesis of truncated tetrahedral cinnamon nanoparticles in citric acid media via PLAL technique. *Materials Letters*, *217*, 267-270.

[37] Inbaraj, X. (2022). Distributed Intelligence Platform to the Edge Computing. *Research Anthology on Edge Computing Protocols, Applications, and Integration* (pp. 78-96). IGI Global.

[38] Zhang, X., Xu, M., Su, J., & Zhao, P. (2023). Structural models for fog computing based internet of things architectures with insurance and risk management applications. *European Journal of Operational Research*, *305*(3), 1273-1291.

[39] Elhadad, A., Alanazi, F., Taloba, A. I., & Abozeid, A. (2022). Fog computing service in the healthcare monitoring system for managing the real-time notification. *Journal of Healthcare Engineering*, *2022*.

[40] Muntjir, M., Rahul, M., & Alhumyani, H. A. (2017). An analysis of Internet of Things (IoT): novel architectures, modern applications, security aspects and future scope with latest case studies. *Int. J. Eng. Res. Technol*, *6*(6), 422-447.

[41] Costa, B., Bachiega Jr, J., de Carvalho, L. R., & Araujo, A. P. (2022). Orchestration in fog computing: A comprehensive survey. *ACM Computing Surveys (CSUR)*, *55*(2), 1-34.

[42] Mukherjee, M., Shu, L., & Wang, D. (2018). Survey of fog computing: Fundamental, network applications, and research challenges. *IEEE Communications Surveys & Tutorials*, *20*(3), 1826-1857.

[43] Liu, Y., Fieldsend, J. E., & Min, G. (2017). A framework of fog computing: Architecture, challenges, and optimization. *IEEE Access*, *5*, 25445-25454.

[44] Hosseinioun, P., Kheirabadi, M., Kamel Tabbakh, S. R., & Ghaemi, R. (2022). aTask scheduling approaches in fog computing: A survey. *Transactions on Emerging Telecommunications Technologies*, *33*(3), e3792.

[45] Ghobaei-Arani, M., & Shahidinejad, A. (2022). A cost-efficient IoT service placement approach using whale optimization algorithm in fog computing environment. *Expert Systems with Applications*, *200*, 117012.

[46] Aazam, M., & Huh, E. N. (2015, March). Fog computing micro datacenter based dynamic resource estimation and pricing model for IoT. *2015 IEEE 29th international conference on advanced information networking and applications* (pp. 687-694). IEEE.

[47] Souri, A., Hussien, A., Hoseyninezhad, M., & Norouzi, M. (2022). A systematic review of IoT communication strategies for an efficient smart environment. *Transactions on Emerging Telecommunications Technologies*, *33*(3), e3736.

[48] Salim, A. A., Bidin, N., Bakhtiar, H., Ghoshal, S. K., Al Azawi, M., & Krishnan, G. (2018, May). Optical and structure characterization of cinnamon nanoparticles synthesized by pulse laser ablation in liquid (PLAL). In *Journal of Physics: Conference Series*, *1027(*1), 012002. IOP Publishing.

[49] Khudhair, Z. N., Nidhal, A., & El Abbadi, N. K. (2022). Text multilevel encryption using new key exchange protocol. *Baghdad Science Journal*, *19*(3), 0619-0619.

[50] Naeem, M. A., Zikria, Y. B., Ali, R., Tariq, U., Meng, Y., & Bashir, A. K. (2022). Cache in fog computing design, concepts, contributions, and security issues in machine learning prospective. *Digital Communications and Networks*.

[51] Gupta, A., & Gupta, S. K. (2022). A survey on green unmanned aerial vehicles-based fog computing: Challenges and future perspective. *Transactions on Emerging Telecommunications Technologies*, *33*(11), e4603.

[52[Salim, A. A., Ghoshal, S. K., Suan, L. P., Bidin, N., Hamzah, K., Duralim, M., & Bakhtiar, H. (2018). Liquid media regulated growth of cinnamon nanoparticles: Absorption and emission traits. *Malaysian Journal of Fundamental and Applied Sciences*, *14*(3-1), 447-449.

[53] Marques, B., Machado, I., Sena, A., & Castro, M. C. (2017, October). A communication protocol for fog computing based on network coding applied to wireless sensors. *2017 International Symposium on Computer Architecture and High Performance Computing Workshops (SBAC-PADW)* (pp. 109-114). IEEE.

10.11113/mjfas.v19n3.2906