JCTA Journal of Computing Theories and Applications ISSN:3024-9104

Research Article

IMANoBAS: An Improved Multi-Mode Alert Notification IoT-based Anti-Burglar Defense System

Edith Ugochi Omede[1,*], Abel Edje[1], Maureen Ifeanyi Akazue[1], Henry Utomwen[1], and Arnold Adimabua Ojugo[2]

[1] Department of Computer Science, Delta State University Abraka, Nigeria; email: edithomede@delsu.edu.ng, toboredje@gmail.com, akazue@delsu.edu.ng, henry4real003@yahoo.co.uk.
[2] Department of Computer Science, Federal University of Petroleum Resources Effurun, Delta State, Nigeria; email: ojugo.arnold@fupre.edu.ng
* Corresponding Author: Edith Ugochi Omede

Abstract: Burglary involves forced or unauthorized entry, which leads to damage or loss of property having monetary or emotional value and, more severely, puts lives at risk. The dire need for the safety of lives and properties has attracted so much research on burglary alert system using Internet of Things (IoT) technology. Most of the research focused on alerting the users of burglary attempts using any or a combination of two notification methods: SMS, call, and email. This study emphasizes three-mode notification that combines SMS, call, and email using the application of IoT technology in a burglary alert system, which uses a Passive Infrared (PIR) sensor for burglar detection to ensure that Homeowners or authorized personnel get alerts in events of imminent attempt to break-ins. The study also details the sensor integration with its supporting components, such as the central hub or microcontroller, buzzer, LED, and network interface in the development of the system. The software was developed to facilitate seamless integration with the hardware, ensuring timely and accurate event detection and subsequent alert generation using Arduino IDE programming language, a framework based on the C++ language. The system effected the 3-mode notification to ensure that users get notification in case of an imminent break-in since the failure of the three modes simultaneously is extremely rare. The system's performance based on its responsiveness on the 3-mode notifications was evaluated, and an average of 83.56% responsiveness was obtained, indicating an acceptable response time.

Keywords: Burglar systems; IMANoBAS; IoT; Notification Alerts; Security.

1. Introduction

Conventional burglar alarm systems have served as a basic deterrent to intruders and served the security needs of many [1]; however, they have been found to lack real-time monitoring capabilities and diverse notification methods [2]–[4]. The birth of the Internet of Things (IoT) has proffered fledging new possibilities as wireless sensor networks to provide the capabilities for intelligent and interconnected burglary alert systems. The sensors are strategically placed at critical points of the protected premises (to include and not limited to) doors, windows, and other spotted vulnerable areas. They are equipped to detect motion, environmental changes, and unauthorized access attempts. It achieves this by continuously monitoring these parameters so that a minor anomaly or change in the system is promptly identified as a potential intrusion cum security breach [5]. IoT gateways act as central hubs within the system to facilitate seamless communication and data transfer. They collect data from various sensors and transmit securely to a cloud-based processing platform [5], [6].

Internet of Things (IoT) technology has been increasingly used in developing home security systems, particularly in creating burglary alert systems. The integration of IoT in these systems enables homeowners to monitor and control their homes remotely using mobile devices and receive real-time notifications in the event of an intrusion. IoT-based burglary alert systems use a combination of sensors and alarms to detect and deter potential burglars and can be customized to suit the specific needs of each homeowner [7]. In recent years, there

Received: December, 4th 2023
Revised: February, 1st 2024
Accepted: February, 3rd 2024
Published: February, 9th 2024

has been an increase in the adoption of IoT-based home security systems due to their ease of installation, cost-effectiveness, and reliability. The ability to remotely monitor and control homes has made IoT burglary alert systems a popular choice among homeowners. Also, IoT-based burglary alert systems offer an added layer of security as they can be integrated with other home automation systems, such as smart locks, lighting, and thermostats, to create a more comprehensive and connected home security solution. This integration enables homeowners to automate their homes and create personalized security scenarios that respond to their unique needs. The integration of IoT technology in burglary alert systems offers homeowners a more comprehensive and connected home security solution that is both cost-effective and reliable. As IoT technology continues to advance, more homeowners are expected to adopt IoT-based security systems to protect their homes from potential intruders. This expectation has attracted much research, though none in the literature we studied integrated the three-mode notification. Instead, they employed either one or a combination of any two, as is seen in [3],[5],[8].

Our study seeks to implement an IoT-based burglary alert system with three (3) notification modes, providing enhanced security measures and prompt response to potential threats by integrating the blynk server service to the Gmail server for email. SMS and call notifications are enabled using TinyGsm and Python Libray for an Arduino SIM900 GPRS. The Gmail server is chosen due to its availability, cost-effectiveness, and maintainability. The cornerstone of the proposed system lies in integrating multiple notification modes in deploying smart sensors to ensure prompt alertness that facilitates security.

2. Review of Related Literature(s)

2.1. IoTs in Burglar Alert System: A Review

In [8] a smart IoT security for smart homes was deployed. It explored a Raspberry Pi with a No-Infrared (NoIR) Pi Camera for image capturing with a passive infrared (PIR) motion detection sensor. It uses motion sensor data and NoIR camera images to predict security threats via a face-recognition classification technique and a custom algorithm. The system ensures user notification in emergencies [8] and agrees with [9]–[11].

In [12] deployed a motion-based camera-active surveillance system for real-time home security monitoring. It uses a motion-detect sensor synchronized with an ESP32-CAM microcontroller to offer a low-cost solution. It interfaces with an IoT-Cayenne to provide a customized user interface for real-time notification, with rapid responses from emergency services or security forces, enhancing overall security [12]. This system agrees with [13]–[15]. A system to allow each customer to connect a home security system to a distant network using a piezoelectric buzzer, an LCD board, and a PIR sensor at residences and workplaces was designed in [16]. The UNO microcontroller serves as the sole constraint for the framework. Various types of connection point circuits are used to connect each sensor and finder to the microcontroller chip. The microcontroller will continuously control each sensor. If the microcontroller detects any safety risk, it will signal the associated buzzer, which will then turn on. The gatecrasher's availability is indicated on the LCD board. Each interconnected sensor is interfaced with the microcontroller via a variety of connection point circuits. The microcontroller will unendingly direct every sensor. If the microcontroller faculties any kind of safety issue, then it will send a sign to the buzzer connected, and the buzzer turns on. The LCD board shows the gatecrasher's side availability [16]–[18].

An intelligent home automation system with multiple functionalities, including appliance control, environmental monitoring, and intruder detection, was developed in [20]. It uses a deep learning model for recognizing and classifying motion patterns. This model focused on organizing individuals detected by surveillance cameras as either intruders or home occupants based on their walking patterns using an ESP32 camera for surveillance, a PIR motion sensor, an ESP8266, a relay module, and a DHT11 sensor for temperature and humidity measurements. The DHT sensor's accuracy in monitoring environmental conditions and its potential for future weather prediction were found to be excellent [19]–[22]. This agrees with [23]–[25].

An affordable home security system that rapidly notifies users through their GSM cell phones by making phone calls. This security system integrates cutting-edge technology while maintaining a low cost and was designed by [26]. The hardware components include a Passive Infra-Red (PIR) motion sensor, an Arduino sensor for motion detection, and a GSM module

for initiating calls to the user. The programming of this system is accomplished using the Arduino IDE to configure the GSM module. The PIR detects unauthorized individuals access and triggers a phone-call when it senses motion in its vicinity, thereby enhancing home security.

An integrated IoT system aimed at enhancing building safety and security. It uses GSM alerts to notify users of detected anomalies and ensure timely responses to potential threats, which was developed in [27]. Its authentication mechanism restricts unauthorized access of resources to unauthorized users; And the system deploys a Network Intrusion Detection System (NIDS) to detect and provide real-time alerts in the event of malicious activities on the IoT network [26]. This improved building security and user access control, offering enhanced protection against potential threats, is supported by [28]–[30].

2.2. Burglar Security Systems Notification: The Nigerian Frontier

Burglary involves forced entry damaging access points [31]. This poses a significant threat to both homes and facilities, with negative effects on victims ranging from loss of property to loss of money and lives [32], [33]. Thus, this has continued to provoke research interests. The advent, adoption, and adaptation of techs and informatics has led to a rise in the exploration of wireless sensor tech (i.e., IoTs). Together with alert systems, they are now deployed in facilities as anti-burglary systems. Its innovativeness is in its capacity to accurately sense the environment and promptly alert authorized users of intrusion anomalies via real-time notifications [34]. Many burglary systems use a combination of communication modes that improve communication and system resilience in the event of communication component failure. This can be quite the case for a country like Nigeria, where communication channels are both unstable, epileptic, and, in some cases, not available, especially in remote areas [35], [36]. If timely communication fails, the system's aim is completely defeated. So, our study will propose and seek to achieve a multiple-mode alert, anti-burglary system that integrates the four modes to alert its users of intruders, this is to ensure that the user receives timely information for immediate action even if any mode should fail. It is extremely rare for all the communication modes to fail at the same time.

Burglar systems notification modes were reviewed as a foundation to yield a home security system that notifies via the web application. The enhanced intelligent smart home control and security system in [37]–[39] classified intruders based on movement patterns. There was no specified notification mode. But, [34], [40]–[42] detect intruders via motion detection and face recognition. An intelligent home with automated environmental control developed as in [43]–[46] notifies using video calling and Facebook images. The home security systems in [47]–[49] use only email notifications with a photo of the detected object or intruder, while [50]–[54] use SMS as notification mode. Phone calls were used by [55]–[60] to notify the presence of an intruder when movement is detected. Other studies combined 2-or-more modes [61]–[64] to ensure real-time notification for timely action.

3. Proposed Material and Method

3.1. Proposed Architecture

Figure 1 shows how the system is logically related to its environment; its interaction with its environment, and remote notifications on events of intruder detection. It depicts the interaction between the components of the proposed system as supported by [65]–[69]. The proposed system was designed using IoT design methodology to successfully integrate IoT devices with a central control system to process data and trigger notifications based on predefined criteria. The system adopts a three-mode notification form (i.e., email, SMS, and phone call) to establish a robust communication framework that greatly amplifies remote monitoring and alert mechanisms.

3.2. Testbed Specification / Set-Up

The proposed system uses a PIR (Passive Infrared) sensor, which is cost-effective, energy-efficient, and more reliable than a camera for detecting motion or changes within its field of view. Blynk Server Service was employed as an intermediary (third-party server) to provide SSL / TLS encryption between Arduino Boards and the Gmail server since the

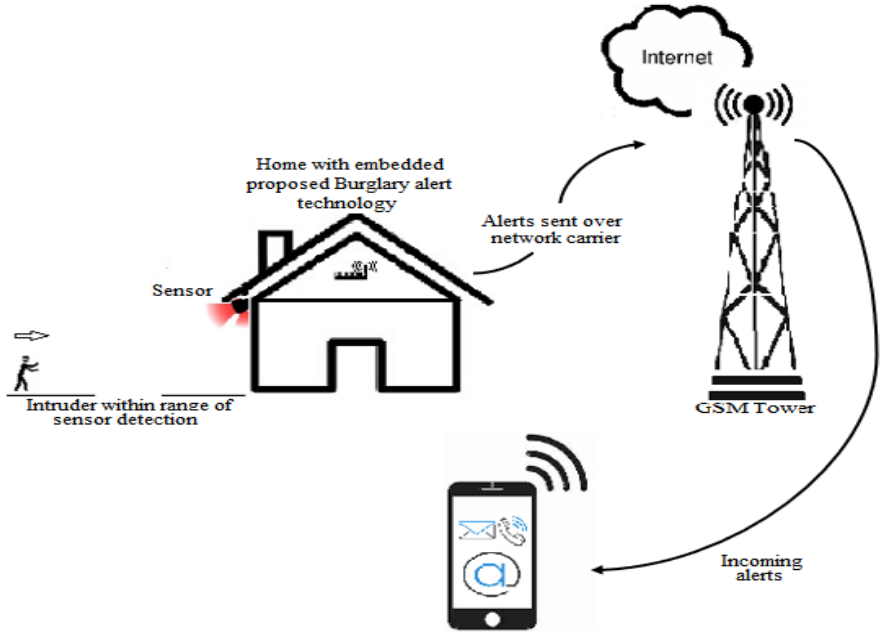


Figure 1. The Proposed System Architecture.

Arduino boards have no SSL/TLS support, which is an important requirement to interface with the Gmail server to ensure security. An account was created on Blynk with the Gmail address to which email notifications will be sent after creating the notification event. SMS and call notifications are enabled using TinyGsm and Python Libray for an Arduino SIM900 GPRS.

The credentials issued by Blynk were then inputted into the system so as to establish a secure connection between Arduino Boards and the Gmail server. The output from the system is the responses to the sensed environment, which include these actions when an intruder is detected.

1. Sending an SMS: The system sends a text message to the homeowner's mobile phone, notifying them of the intruder.
2. Initiating a Call: When an intruder is detected, the system pulls a call across to the designated phone number.
3. Sending an email alert: The system sends an email alert to the homeowner, providing detailed information about the break-in.

This model provides a detailed mathematical representation of a burglary alert system using PIR sensors and multiple notification methods. It includes decision variables, parameters, constraints, and the objective function. The model can be implemented and customized using optimization techniques and appropriate software to find values for the decision variables that minimize the response time while adhering to the constraints.

1. **Notification Indices** provide notification mode parameters. We have the indices for notification set as i_1 for email, i_2 for SMS, and i_3 for phone calls respectively. Also, we have the k-index set for phone numbers and the m-index set for email addresses.
2. **Decision variable(s)**: these parameters reflect the underlying outcome. We have set that X_{ik} yields the binary variable (0 if notification is not sent, and 1 if/when it is sent) indicating whether a notice of type i is sent to phone number k. also, we have that Y_{im} yields a binary variable (0 if not sent or 1 if sent) indicating whether a notification of type i is sent to email address m.
3. **Testbed Ensemble Parameters** – we have that: (a) A is a binary variable (0 or 1) on activation status for a PIR sensor (1 if activated, 0 if not), B_i is a budget constraint for notifications of type i, P_B : Probability of a burglary event being detected by the PIR sensor, D_i : Maximum allowable delay for sending notifications of type i, P_P : Probability that a phone is available (e.g., not in use),

P_E: Probability that an email address is available, N_A : Set of active phone numbers and M_A : Set of active email addresses.

We make the following assumptions:

1. The PIR sensor has two states: activated (1) and not activated (0). It can detect a burglary event with a probability P_B when activated.
2. The system has budget constraints on the number of notifications (B_i) that can be sent for each notification type i.
3. Notifications (Email, SMS, call) can be sent or made immediately upon the detection of a burglary event.
4. The maximum allowable delay for sending each type of notification is D_i for notification type i.
5. Phone availability is considered, and a phone is available with probability P_P.
6. Email address availability is considered, and an email address is available with probability P_E.

We also explore the following constraints:

1. Budget constraints for each notification i yields $\sum_k X_{ik} + \sum_k X_{ik} < B_i$ for all i.
2. Activation constraint for the PIR sensor: $A \in \{0,1\}$.
3. Delay constraints for each notification type i: $\sum_k X_{ik} \leq D_i$ for all i.
4. Constraint for active phone numbers (if a call is made): If $i = 3$, then the phone number must be active: $\sum_k X_{ik} = 1$ for all $k \in N_{Active}$.
5. Constraint for active email addresses (if an email is sent): If $i = 1$, then the email address must be active: $\sum_m Y_{im} = 1$ for all $m \in M_{Active}$

Thus, the function $f(B)$ maximizes the probability of detecting a burglar event by optimizing the activation of the PIR sensor and the selection of notification type while considering phone and email address availability and $f(T)$ minimizes the total time for notifying recipients as seen in Equation (1) and (2) respectively.

$$f(B) = A \cdot P_B \cdot \left(i \sum_k X_{ik} + i \sum_m Y_{im} \right) \tag{1}$$

$$f(T) = i \sum_k X_{ik} \cdot D_i + i \sum_m Y_{im} \cdot D_i \tag{2}$$

This mathematical model uses indices to represent the decision variables, parameters, and constraints, maximizing the probability of detecting a burglary event and minimizing the total time for notifying recipients while adhering to budget, delay, phone, and email address availability considerations. The general algorithm for the burglar alert system is seen as in Algorithm 1.

Algorithm 1. The IMuNoBAS algorithm

INPUT: phone number configuration, internet, and Blynk credentials
OUTPUT: buzzer/siren activation, Led activation, activation of alert sending (SMS, Call, email)

1: Initialize Arduino-Uno microcontroller unit
2: Initialize GSM module
3: Initiate connection to PIR sensor
4: Check continuously for intrusions (objects, individuals)
5: **If** intruder is detected: **Do**
6: **activate** the siren/alarm to alert people of the intruder
7: **activate** the yellow LED to alert people of the intruder
8: **GSM** module establishes the internet connection using internet credentials
9: **set** Arduino board for Blynk communication using <BlynkSimpleTinyGSM.h>
10: **establish** communication with Blynk server using <Blynk.begin.h>
11: **refresh** the GSM module using 'updateSerial()' command

```
12:     run Blynk service using 'Blynk.run()'
13:     activate the alert event for email notification
14:     set the GSM module to SMS mode (AT+CMOS)
15:     send SMS to home_owner or authorized personnel to notify of intrusion
16:     Set GSM to call mode (AT+CMOS)
17:     place call to home_owner or authorized personnel to notify of intrusion
18: Elseif (no intruder detected) Then Do:
19:     activate the green LED to normal functioning
20:     deactivate yellow LED if previously activate.
21:     deactivate previously activated buzzer
22: continue search for intrusion: Stop
```

3.3. Experimental Procedure

Our Arduino unit ATmega328p has 14 digital I/O pins, 6-of-which are used as PWM (Pulse Width Modulation) outputs, another six used for analog inputs, a 16MHz oscillator, a USB connection, a power jack, an ICSP header, and a reset button. The buzzer is used for audio notification, to be triggered by a microcontroller based on predefined criteria. The PIR sensor detects motion via sensing changes in infrared radiation emitted by objects due to their temperature. The SIM900 helps provide GSM/GPRS communication capability using its SIM900 Shield to facilitate SMS, voice calls, data connectivity, and remote control/monitoring of devices. A SIM card (Subscriber Identity Module) is also integrated for authentication and connection of users to mobile networks for communication using machine-to-machine (M2M) communication. Light-emitting orange and green diodes were used to indicate the system at rest and when a motion has been detected, respectively. We used a 12V adapter to supply the 12V direct current (DC) with a rocket switch to toggle between the "ON/OFF" state.

The software was developed to facilitate seamless integration with the hardware, ensuring timely and accurate event detection and subsequent alert generation using Arduino IDE programming language, a framework based on the C++ language. The IDE compiles our C++ code into assembly language, which is used by Atmel chips mounted over Arduino boards, also known as microcontrollers.

4. Results and Discussion

All the hardware units of the system were first tested to ascertain their good working condition. Then, each unit was interfaced and implemented individually with the microcontroller board and driven with the software according to the necessity of the application. The testing of the application was not done at once after it was completed. Rather, each unit of the application was tested individually. The second unit was not tested until the first unit has given the expected result. Lastly, the units were integrated into full system, which was also tested. Table 1 shows the sensor's coverage in meters. The system is installed 3m above the ground level, hence starting from 3m.

Table 1. Functionality test detection range

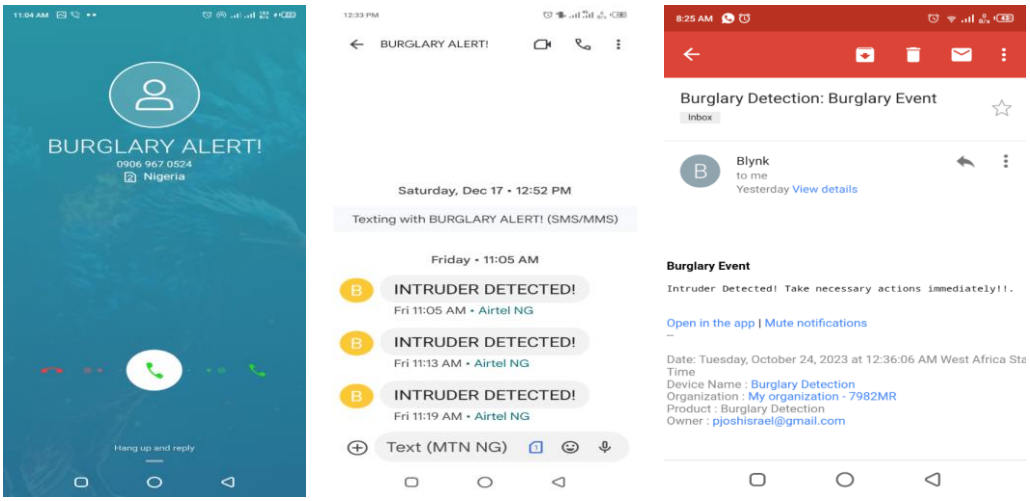
Range in mm	Sensor states				Final adopters
	Trial 1	Trial 2	Trial 3	Trial 4	
3	On	On	On	On	This is the expected action
4	On	On	On	On	This is the expected action
5	On	On	On	On	This is the expected action
6	On	On	On	On	This is the expected action
7	On	Off	Off	On	This is the expected action
8	Off	Off	Off	Off	This is the expected action
9	Off	Off	Off	Off	This is the expected action
10	Off	Off	Off	Off	This is the expected action

Table 1 concludes that the PIR sensor detects an intruder within the coverage 3m to 7m. The intruder beyond this distance is outside the sensor's coverage and cannot be captured. Trial1 to Trial4 is the number of times its coverage for each time it is tested.

Table 2. Functionality Test on Notifications on Intruder Detection

Sensor State	LED Green / Yellow	Sensor states				Final adopters
		Buzzer	Call	SMS	Email	
Low	Green: ON Yellow: Off	Off	Standby	Standby	Standby	This is the expected action
Low	Green: ON Yellow: Off	Off	Standby	Standby	Standby	This is the expected action
High	Green: Off Yellow: On	On	Call Sent	SMS sent	Email Sent	This is the expected action
High	Green: Off Yellow: On	On	Call Sent	SMS sent	Email Sent	This is the expected action
Low	Green: On Yellow: Off	Off	Standby	Standby	Standby	This is the expected action
High	Green: Off Yellow: On	On	Call Sent	SMS sent	Email Sent	This is the expected action

Table 2 concludes that when the PIR sensor detects an intruder, the system activates the buzzer and yellow LED, sends an SMS and email as well as places a call. The system's action when an intruder is detected is shown in Figure 2.



(a) (b) (c)

Figure 2. Sample Notification Results (**a**) by calling; (**b**) by SMS; (**c**) by email.

Table 3. Performance Testing (Researchers)

Alert Name	Time before the alert arrived		
	Email (t_1)	SMS (t_2)	Call (t_3)
Alert 1	12 seconds	21 seconds	38 seconds
Alert 2	8 seconds	23 seconds	41 seconds
Alert 3	13 seconds	20 seconds	46 seconds
Alert 4	10 seconds	18 seconds	55 seconds
Alert 5	9 seconds	20 seconds	37 seconds
Alert 6	14 seconds	16 seconds	50 seconds
Average time (in seconds)	11 seconds	19.7 seconds	44.5 seconds

Table 3 shows the time to send an alert using the three notification modes. Alert1 to Alert6 are six different alerts sent by the system on different occasions of intruder detection, and it was observed that it takes longer to communicate with users through phone calls.

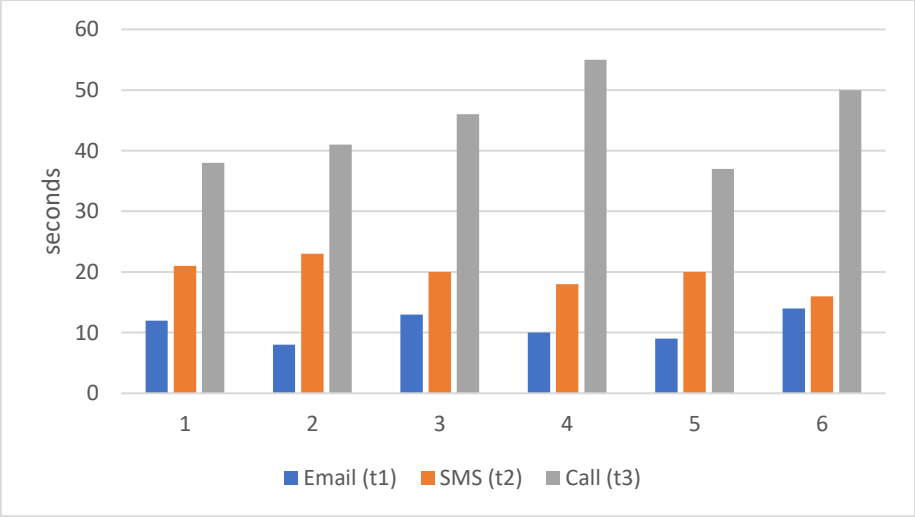


Figure 3. Time taken for different notification modes (Researchers)

Figure 3 is a pictorial representation of what is shown in Table 3, depicting the time taken by the three notification modes, t1, t2, and t3, representing email, SMS, and call, respectively. The X-axis is the different alerts sent, while the y-axis is the time taken to deliver the alerts in seconds. It can be observed that in all the alerts, delivery by Call took most time than others.

System performance evaluation using responsiveness (RESP) can be calculated with Equation (3).

$$\text{RESP} = 1 - \frac{1}{n}\sum_{i=1}^{n}\frac{t(i)}{t(max)} \tag{3}$$

Where n =3 (the total number of notification modes), $t(i)$ is the response time of i-th event or request (i.e., the time it takes for the system to respond to a specific event. (Average Response time for Email (t_1) = 11 seconds; SMS (t_2) = 19.7 seconds; Call (t_3) = 44.5 seconds), and $t(max)$ is the expected maximum response time which is set at 60 seconds.

Thus, responsiveness $\text{RESP} = 1 - \frac{1}{3}\sum_{i=1}^{3}\frac{11+19.7+44.5}{60} \approx 0.83555$, which is 83.56%

This indicates that, on average, the system's responses are about 83.56% as fast as the maximum acceptable response time of 60 seconds. This agrees with [68]–[71].

5. Conclusions

This study enhanced remote monitoring and alert capabilities via 3-distinct modes: SMS, call, and email, thereby creating a robust, real-time communication system to notify users of critical events or status changes detected by their IoT devices. The adaptability offered by this triple notification system can also be reasoned as a failover mechanism for notifications, ensuring reliability. If one notification mode fails, the system ensures that notification is delivered to the user through the other modes. This adaptability proves its valuability, especially in scenarios where immediate awareness of status changes, security incidents, or environmental shifts is paramount. We found from the study that using other MCUs like Raspberry Pi will yield better results by reducing turnaround time as it has an operating system and can run concurrent processes. Email is the fastest delivery mode compared to SMS and Calls. Arduino Uno is used as the MCU due to its low cost since the research is self-sponsored.

Author Contributions: Conceptualization: E.U. Omede, H. Utowen. A.A. Ojugo; Methodology: E.U Omede, H. Utowen, A.E Edje, and M.I Akazue; Software: H.Utowen, E.U Omede, and M.I. Akazue; Validation: A.A. Ojugo, A.E Edje, and E.U. Omede; Formal Analysis: E.U Omede; Investigation: A.A. Ojugo, E.U. Omede, and H. Utowen; Resources: A.E. Edje and M.I. Akazue; Data Curation: H. Utowen and E.U. Omede; Writing—original draft preparation: E.U Omede and A.A. Ojugo, Writing—review and editing: M.I. Akazue and A.E. Edje; Visualization: E.U. Omede and A.A. Ojugo; Supervision: A.A. Ojugo; Project administration: A.A. Ojugo; funding acquisition: All.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] I. J. Onyeacholem and E. U. Omede, "Authenticated and Dynamic Websites : A Sure Control against Website Authenticated and Dynamic Websites : A Sure Control against Website Spoofing Attacks," *J. Softw. Eng. Simul.*, vol. 9, no. 3(2023), pp. 57–60, 2023.

[2] B. Kizilkaya, E. Ever, H. Y. Yatbaz, and A. Yazici, "An Effective Forest Fire Detection Framework Using Heterogeneous Wireless Multimedia Sensor Networks," *ACM Trans. Multimed. Comput. Commun. Appl.*, vol. 18, no. 2, pp. 1–21, May 2022, doi: 10.1145/3473037.

[3] S. S, S. Yamuna, and S. N. George, "An IoT based Active Building Surveillance System using Raspberry Pi and NodeMCU," Jan. 2020, [Online]. Available: http://arxiv.org/abs/2001.11340

[4] R. Kumar and D. Kumar, "Hybrid Swarm Intelligence Energy Efficient Clustered Routing Algorithm for Wireless Sensor Networks," *J. Sensors*, vol. 2016, pp. 1–19, 2016, doi: 10.1155/2016/5836913.

[5] Saba, T., Rehman, A., Sadad, T., Kolivand, H., & Bahaj, S. A. (2022). Anomaly-based intrusion detection system for IoT networks through deep learning model. Computers and Electrical Engineering, 99, 107810.

[6] M. Lei, L. Xu, T. Liu, S. Liu, and C. Sun, "Integration of Privacy Protection and Blockchain-Based Food Safety Traceability: Potential and Challenges," *Foods*, vol. 11, no. 15, pp. 1–31, 2022, doi: 10.3390/foods11152262.

[7] M. I. Akazue, A. A. Ojugo, R. E. Yoro, B. O. Malasowe, and O. Nwankwo, "Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 28, no. 3, pp. 1756–1765, Dec. 2022, doi: 10.11591/ijeecs.v28.i3.pp1756-1765.

[8] A. J. Majumder and J. A. Izaguirre, "A Smart IoT Security System for Smart-Home Using Motion Detection and Facial Recognition," 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 2020, pp. 1065-1071, doi: 10.1109/COMPSAC48688.2020.0-132.

[9] D. Upadhyay and S. Sampalli, "SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations," *Comput. Secur.*, vol. 89, p. 101666, Feb. 2020, doi: 10.1016/j.cose.2019.101666.

[10] A. Ometov *et al.*, "A Survey on Wearable Technology: History, State-of-the-Art and Current Challenges," *Comput. Networks*, vol. 193, p. 108074, Jul. 2021, doi: 10.1016/j.comnet.2021.108074.

[11] C. Joshi, J. R. Aliaga, and D. R. Insua, "Insider Threat Modeling: An Adversarial Risk Analysis Approach," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 1131–1142, 2021, doi: 10.1109/TIFS.2020.3029898.

[12] K. Okokpujie, G.C. Kennedy, D. Ayankoya, E. Noma-Osaghae, I. P. Okokpujie and J.A Kalibbala, Development of a Real-Time Home Security and Safety Management System. In:nPattnaik, P.K, Sain. M., Al-Absi, A.A. (eds). Proceedings of 2nd International Conference on Smart Computing and Cyber Security. SMARTCYBER 2021. Lecture notes in Networks and Systems, vol 395, Springer, Singapore. https://doi.org/10.1007/978-981-16-9480-6_11

[13] P. Joshi, A. Solomy, A. Suresh, K. Kachroo, and P. Deshmukh, "Smart Fuel Station," *SSRN Electron. J.*, 2020, doi: 10.2139/ssrn.3572319.

[14] R. F. R. Suleiman and F. Q. M. I. Reza, "Gas station fuel storage tank monitoring system using internet of things," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 1.6 Special Issue, pp. 531–535, 2019, doi: 10.30534/ijatcse/2019/7881.62019.

[15] A. Hurt, "Internet of Medical Things emerges.," *Dermatology Times*, vol. 40, no. 10, pp. 52–58, 2019, [Online]. Available: http://ezproxy.uct.ac.za/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=cin20&AN=138944526&site=ehost-live

[16] A. A. Ojugo and O. Nwankwo, "Forging a Spectral-Clustering Multi-Agent Hybrid Deep Learning Model To Predict Rainfall Runoff In Nigeria," *Int. J. Innov. Sci. Eng. Technol.*, vol. 8, no. 3, pp. 140–147, 2021.

[17] A.R. Abdul Rashid and F. Zakaria , "Design and Implementation of Home Security System Using Piezoelectric Sensor". MJoSHT, Vol.5 no.1, Feb. 2020. DOI: 10.33102/MJOSHT.V5i1.129

[18] K. Kakhi, R. Alizadehsani, H. M. D. Kabir, A. Khosravi, S. Nahavandi, and U. R. Acharya, "The internet of medical things and artificial intelligence: trends, challenges, and opportunities," *Biocybern. Biomed. Eng.*, vol. 42, no. 3, pp. 749–771, 2022, doi: 10.1016/j.bbe.2022.05.008.

[19] O. D. Voke, M. I. Akazue, E. U. Omede, E. . Oboh, and A. Imianvan, "Survival Prediction of Cervical Cancer Patients using Genetic Algorithm-Based Data Value Metric and Recurrent Neural Network," *Int. J. Soft Comput. Eng.*, vol. 13, no. 2, pp. 29–41, May 2023, doi: 10.35940/ijsce.B3608.0513223.

[20] O. Taiwo and A. E. Ezugwu, "internet of Things-Bsed Intelligent Smrt Home Contro System". Security and Communication Networks, 2021(7); 1-17. DOI: 101155/2021/928254.

[21] M. N. Al-Mhiqani, S. N. Isnin, R. Ahmed, and Z. Z. Abidi, "An Integrated Imbalanced Learning and Deep Neural Network Model for Insider Threat Detection," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 1, pp. 1–5, 2021.
[22] M. Aqib, R. Mehmood, A. Alzahrani, I. Katib, A. Albeshri, and S. M. Altowaijri, *Smarter traffic prediction using big data, in-memory computing, deep learning and gpus*, vol. 19, no. 9. 2019. doi: 10.3390/s19092206.
[23] A. H. Altowaijri, M. S. Alfaifi, T. A. Alshawi, A. B. Ibrahim, and S. A. Alshebeili, "A Privacy-Preserving Iot-Based Fire Detector," *IEEE Access*, vol. 9, pp. 51393–51402, 2021, doi: 10.1109/ACCESS.2021.3069588.
[24] R. A. Alsowai and T. Al-Shehari, "A multi-tiered framework for insider threat prevention," *Electron.*, vol. 10, no. 9, 2021, doi: 10.3390/electronics10091005.
[25] F. O. Aghware, R. E. Yoro, P. O. Ejeh, C. C. Odiakaose, F. U. Emordi, and A. A. Ojugo, "DeLClustE: Protecting Users from Credit-Card Fraud Transaction via the Deep-Learning Cluster Ensemble," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 6, pp. 94–100, 2023, doi: 10.14569/IJACSA.2023.0140610.
[26] Hadi, H. J., Nisa, K. U., & Harris, S. (2023). Autonomous and Collaborative Smart Home Security System (ACSHSS). arXiv preprint arXiv:2309.02899.
[27] D. Sun, M. Liu, M. Li, Z. Shi, P. Liu, and X. Wang, "DeepMIT: A Novel Malicious Insider Threat Detection Framework based on Recurrent Neural Network," in *2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, IEEE, May 2021, pp. 335–341. doi: 10.1109/CSCWD49262.2021.9437887.
[28] A. D. Bhavani and N. Mangla, "A Novel Network Intrusion Detection System Based on Semi-Supervised Approach for IoT," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 4, pp. 207–216, 2023, doi: 10.14569/IJACSA.2023.0140424.
[29] H. Zardi and H. Alrajhi, "Anomaly Discover: A New Community-based Approach for Detecting Anomalies in Social Networks," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 4, pp. 912–920, 2023, doi: 10.14569/IJACSA.2023.01404101.
[30] F. O. Aghware, R. E. Yoro, P. O. Ejeh, C. C. Odiakaose, F. U. Emordi, and A. A. Ojugo, "Sentiment analysis in detecting sophistication and degradation cues in malicious web contents," *Kongzhi yu Juece/Control Decis.*, vol. 38, no. 01, p. 653, 2023.
[31] A. A. Ojugo, M. I. Akazue, P. O. Ejeh, C. Odiakaose, and F. U. Emordi, "DeGATraMoNN : Deep Learning Memetic Ensemble to Detect Spam Threats via a Content-Based Processing," *Kongzhi yu Juece/Control Decis.*, vol. 38, no. 01, pp. 667–678, 2023.
[32] S. Yuan and X. Wu, "Deep learning for insider threat detection: Review, challenges and opportunities," *Comput. Secur.*, vol. 104, 2021, doi: 10.1016/j.cose.2021.102221.
[33] A. A. Ojugo and R. E. Yoro, "Predicting Futures Price And Contract Portfolios Using The ARIMA Model: A Case of Nigeria's Bonny Light and Forcados," *Quant. Econ. Manag. Stud.*, vol. 1, no. 4, pp. 237–248, 2020, doi: 10.35877/454ri.qems139.
[34] A. A. Ojugo and R. E. Yoro, "Extending the three-tier constructivist learning model for alternative delivery: ahead the COVID-19 pandemic in Nigeria," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 3, p. 1673, Mar. 2021, doi: 10.11591/ijeecs.v21.i3.pp1673-1682.
[35] E. . Ihama, M. I. Akazue, E. U. Omede, and D. V. Ojie, "A Framework for Smart City Model Enabled by Internet of Things (IoT)," *Int. J. Comput. Appl.*, vol. 185, no. 6, pp. 6–11, 2023, doi: 10.5120/ijca2023922685.
[36] A. O. Eboka and A. A. Ojugo, "Mitigating technical challenges via redesigning campus network for greater efficiency, scalability and robustness: A logical view," *Int. J. Mod. Educ. Comput. Sci.*, vol. 12, no. 6, pp. 29–45, 2020, doi: 10.5815/ijmecs.2020.06.03.
[37] A. A. Ojugo, R. E. Yoro, D. A. Oyemade, A. O. Eboka, E. Ugboh, and F. O. Aghware, "Robust Cellular Network for Rural Telephony in Southern Nigeria," *Am. J. Networks Commun.*, vol. 2, no. 5, p. 125, 2013, doi: 10.11648/j.ajnc.20130205.12.
[38] S. Gokarn and A. Choudhary, "Modeling the key factors influencing the reduction of food loss and waste in fresh produce supply chains," *J. Environ. Manage.*, vol. 294, p. 113063, Sep. 2021, doi: 10.1016/j.jenvman.2021.113063.
[39] A. Mukherjee, S. K. Shome, and P. Bhattacharjee, "Survey on Internet of Things Based Intelligent Wireless Sensor Network for Fire Detection System in Building," 2022, pp. 193–200. doi: 10.1007/978-981-16-1777-5_12.
[40] P. P. Ray, M. Mukherjee, and L. Shu, "Internet of Things for Disaster Management: State-of-the-Art and Prospects," *IEEE Access*, vol. 5, pp. 18818–18835, 2017, doi: 10.1109/ACCESS.2017.2752174.
[41] S. Zhang, D. Gao, H. Lin, and Q. Sun, "Wildfire Detection Using Sound Spectrum Analysis Based on the Internet of Things," *Sensors*, vol. 19, no. 23, p. 5093, Nov. 2019, doi: 10.3390/s19235093.
[42] B. Prabha, "An IoT Based Efficient Fire Supervision Monitoring and Alerting System," in *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, IEEE, Dec. 2019, pp. 414–419. doi: 10.1109/I-SMAC47947.2019.9032530.
[43] E. U. Omede , "Driving the Skill Acquisition Auto_Tech Resource Sharing System Using the Realtime Web-Based Application," *Niger. J. Sci. Environ.*, no. March, 2022, [Online]. Available: https://delsunjse.com/index.php/njse/article/view/106%0Ahttps://delsunjse.com/index.php/njse/article/download/106/97
[44] E. Omede and U. K. Okpeki, "Design and implementation of autotech resource sharing system for secondary schools in Delta State," *J. Niger. Assoc. Math. Phys.*, vol. 51, no. 5, pp. 325–337, 2019.
[45] C. N. Verdouw, J. Wolfert, A. J. M. Beulens, and A. Rialland, "Virtualization of food supply chains with the internet of things," *J. Food Eng.*, vol. 176, pp. 128–136, May 2016, doi: 10.1016/j.jfoodeng.2015.11.009.
[46] S. G. Kong, D. Jin, S. Li, and H. Kim, "Fast fire flame detection in surveillance video using logistic regression and temporal smoothing," *Fire Saf. J.*, vol. 79, pp. 37–43, Jan. 2016, doi: 10.1016/j.firesaf.2015.11.015.
[47] S. Khan, K. Muhammad, S. Mumtaz, S. W. Baik, and V. H. C. de Albuquerque, "Energy-Efficient Deep CNN for Smoke Detection in Foggy IoT Environment," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9237–9245, Dec. 2019, doi: 10.1109/JIOT.2019.2896120.
[48] S. Sendra, L. García, J. Lloret, I. Bosch, and R. Vega-Rodríguez, "LoRaWAN Network for Fire Monitoring in Rural Environments," *Electronics*, vol. 9, no. 3, p. 531, Mar. 2020, doi: 10.3390/electronics9030531.
[49] G. Roque and V. S. Padilla, "LPWAN Based IoT Surveillance System for Outdoor Fire Detection," *IEEE Access*, vol. 8, pp. 114900–114909, 2020, doi: 10.1109/ACCESS.2020.3003848.
[50] P. K. D. Pramanik, S. Pal, and P. Choudhury, "Beyond Automation: The Cognitive IoT. Artificial Intelligence Brings Sense to the Internet of Things," 2018, pp. 1–37. doi: 10.1007/978-3-319-70688-7_1.

[51] F. M. A. Hossain, Y. M. Zhang, and M. A. Tonima, "Forest fire flame and smoke detection from UAV-captured images using fire-specific color features and multi-color space local binary pattern," *J. Unmanned Veh. Syst.*, vol. 8, no. 4, pp. 285–309, Dec. 2020, doi: 10.1139/juvs-2020-0009.
[52] Sarwar, Bajwa, Jamil, Ramzan, and Sarwar, "An Intelligent Fire Warning Application Using IoT and an Adaptive Neuro-Fuzzy Inference System," *Sensors*, vol. 19, no. 14, p. 3150, Jul. 2019, doi: 10.3390/s19143150.
[53] W. Benzekri, A. El, O. Moussaoui, and M. Berrajaa, "Early Forest Fire Detection System using Wireless Sensor Network and Deep Learning," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 5, 2020, doi: 10.14569/IJACSA.2020.0110564.
[54] F. A. Saputra, M. U. H. Al Rasyid, and B. A. Abiantoro, "Prototype of early fire detection system for home monitoring based on Wireless Sensor Network," in *2017 International Electronics Symposium on Engineering Technology and Applications (IES-ETA)*, IEEE, Sep. 2017, pp. 39–44. doi: 10.1109/ELECSYM.2017.8240373.
[55] G. Sathyakala, V. Kirthika, and B. Aishwarya, "Computer Vision Based Fire Detection with a Video Alert System," in *2018 International Conference on Communication and Signal Processing (ICCSP)*, IEEE, Apr. 2018, pp. 0725–0727. doi: 10.1109/ICCSP.2018.8524216.
[56] A. Imteaj, T. Rahman, M. K. Hossain, M. S. Alam, and S. A. Rahat, "An IoT based fire alarming and authentication system for workhouse using Raspberry Pi 3," in *2017 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, IEEE, Feb. 2017, pp. 899–904. doi: 10.1109/ECACE.2017.7913031.
[57] B. O. Malasowe, M. I. Akazue, E. A. Okpako, F. O. Aghware, D. V. Ojie, and A. A. Ojugo, "Adaptive Learner-CBT with Secured Fault-Tolerant and Resumption Capability for Nigerian Universities," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 8, pp. 135–142, 2023, doi: 10.14569/IJACSA.2023.0140816.
[58] A. A. Ojugo *et al.*, "Forging a User-Trust Memetic Modular Neural Network Card Fraud Detection Ensemble: A Pilot Study," *J. Comput. Theor. Appl.*, vol. 1, no. 2, pp. 1–11, Oct. 2023, doi: 10.33633/jcta.v1i2.9259.
[59] S. Saponara, A. Elhanashi, and A. Gagliardi, "Real-time video fire/smoke detection based on CNN in antifire surveillance systems," *J. Real-Time Image Process.*, vol. 18, no. 3, pp. 889–900, Jun. 2021, doi: 10.1007/s11554-020-01044-0.
[60] I. Ehsan *et al.*, "Internet of Things-Based Fire Alarm Navigation System: A Fire-Rescue Department Perspective," *Mob. Inf. Syst.*, vol. 2022, pp. 1–15, Sep. 2022, doi: 10.1155/2022/3830372.
[61] Y.-J. Kim, H. Kim, S. Lee, and W.-T. Kim, "Trustworthy Building Fire Detection Framework With Simulation-Based Learning," *IEEE Access*, vol. 9, pp. 55777–55789, 2021, doi: 10.1109/ACCESS.2021.3071552.
[62] W.-L. Hsu, J.-Y. Jhuang, C.-S. Huang, C.-K. Liang, and Y.-C. Shiau, "Application of Internet of Things in a Kitchen Fire Prevention System," *Appl. Sci.*, vol. 9, no. 17, p. 3520, Aug. 2019, doi: 10.3390/app9173520.
[63] A. Menon, "Leveraging Facial Recognition Technology in Criminal Identification," Sharda University, Greater Noida, India, 2023. [Online]. Available: https://www.researchgate.net/publication/367148292
[64] A. Shahraki, D. K. Kaffash, and O. Haugen, "A Review on the effects of IoT and Smart Cities Technologies on Urbanism," in 2018 South-Eastern European Design Automation, Computer Engineering, Computer Networks and Society Media Conference (SEEDA_CECNSM), IEEE, Sep. 2018, pp. 1–8. doi: 10.23919/SEEDA-CECNSM.2018.8544932.
[65] P. K. Kosamkar and V. Y. Kulkarni, "Agriculture crop simulation models using computational intelligence," *Int. J. Comput. Eng. Technol.*, vol. 10, no. 3, pp. 3–19, May 2019, doi: 10.34218/IJCET.10.3.2019.015.
[66] L. Kouadio, R. C. Deo, V. Byrareddy, J. F. Adamowski, S. Mushtaq, and V. Phuong Nguyen, "Artificial intelligence approach for the prediction of Robusta coffee yield using soil fertility properties," *Comput. Electron. Agric.*, vol. 155, pp. 324–338, Dec. 2018, doi: 10.1016/j.compag.2018.10.014.
[67] O. Olaewe, S. O. Akinoso, and A. S. Achanso, "Electronic Library and Other Internet Resources in Universities as Allied Forces in Global Research Work and Intellectual Emancipation Senior Lecturer and Senior Research Fellow Department of Science and Technology Education Dean , Faculty of Education Co," *J. Emerg. Trends Educ. Res. Policy Stud.*, vol. 10, no. 1, pp. 41–46, 2019.
[68] S. Kissler, "Revealing contagion," *Science (80-.).*, vol. 378, no. 6620, pp. 611–611, Nov. 2022, doi: 10.1126/science.ade3133.
[69] S. M. Kissler, C. Tedijanto, E. M. Goldstein, Y. H. Grad, and M. Lipsitch, "Projecting the transmission dynamics of SARS-CoV-2 through the post-pandemic period," *Biol. Cell*, vol. 35, pp. 1–30, 2020, doi: 10.1101/2020.03.04.20031112.