

VIRTUAL RESOURCE MANAGEMENT FOR CELL BROADCAST ALERT HANDLING

Mihai-Virgil NICHITA

*The Special Telecommunications Service, Bucharest, Romania,
National University of Science and Technology Politehnica Bucharest, Romania
mihai_nichita9@yahoo.com*

Adrian-Petru MIHAI

*Faculty of Electronics, Telecommunications and Information Technology,
National University of Science and Technology Politehnica Bucharest, Romania
adrian_petru.mihai@stud.etti.upb.ro*

Cosmin-Alexandru PĂUN

*Faculty of Electronics, Telecommunications and Information Technology,
National University of Science and Technology Politehnica Bucharest, Romania
cosmin.paun@stud.etti.upb.ro*

Florin HARALAMBIE

*Doctoral School of Automatic Control and Computers,
National University of Science and Technology Politehnica Bucharest, Romania
florin.haralambie@upb.ro*

ABSTRACT

This paper introduces an autonomous agent-based system for intelligent redirecting Cell Broadcast (CB) messages to e-mail using a Raspberry Pi 4B (RPi 4B) connected to a modem, addressing the challenge of limited access to emergency alerts. The concept uses a virtual resource that can act alone upon the occurrence of a stimulus and which manages the dissemination of critical public safety information accurately and in a timely manner. The approach combines an affordable computing platform with an Artificial Intelligence (AI) model that acts as a message filter. The RPi 4B monitors the modem via AT commands, allowing the AI module to classify transmissions and forward alerts to a designated e-mail address. Unlike existing academic works, which primarily focus on weather or seismic triggers, which do not provide equivalent ready-made functionality, the proposed system is designed to expand the system's alerting capabilities worldwide. Key contributions include expanding access to CB messages, demonstrating a cost-efficient AI-enhanced architecture and delivering a deployable, user-friendly system. Experimental evaluation indicates redirection delays between 57 and 70 seconds, dominated by the modem acquisition stage, while the internal processing latency, from message reception to database storage, was between 5 and 10 seconds.

KEYWORDS:

agents, broadcast, emergency, IoT, virtual

1. Introduction

Cell Broadcast (CB) is a regulated messaging service supported by mobile networks, designed to deliver short text alerts simultaneously to all devices within a defined geographic area. Unlike traditional Short Message Service (SMS), CB messages are not bound to individual phone numbers, but rather to cells in the network, enabling large-scale dissemination of critical information. As officially described in the standards, such as ETSI (1996) or ETSI (1997) or online, on RO-ALERT website, governments and mobile operators often rely on CB to transmit emergency alerts, such as severe weather warnings, natural disaster notifications or public safety announcements. However, access to these alerts can be inconsistent due to limitations in device compatibility, weak coverage in remote areas or user preference for alternate communication channels. As smart buildings and remote monitoring expand, accessible, resilient CB alerts are increasingly needed.

Even though CB systems are widely used for public safety, ensuring reliable and flexible access to emergency alerts across devices, locations and channels remains challenging. This paper proposes redirecting CB messages to email using a single-board computer (RPI 4B) with a cellular modem that continuously monitors broadcasts from nearby network cells.

However, detecting valid CB emergency messages is difficult because raw modem output contains mixed signalling and technical data. To address this, an AI agent in n8n filtered and classified incoming messages, forwarding verified CB alerts via email so they can be accessed on any internet-connected device, independent of the mobile network.

From a research standpoint, the main issue this paper attempts to solve is to close the accessibility gap for users outside the physical alert area by enabling broader alert reception. The proposed solution adds AI-based filtering, IoT-compatible processing and a scalable architecture for public safety use.

As work of Bopp, Douvinet, Carles, Foulquier and Péroche (2025) stated, current emergency and early warning systems are mostly centralized and focused on direct mobile notifications, with little support for decentralized deployment or intelligent IoT integration. Traditional CB systems restrict alerts to geographic areas, while this approach extends notifications beyond those limits through Internet connectivity.

Therefore, this paper's primary research issue is: Is it possible to expand a CB message utility beyond the initial broadcast area? The proposed system enables decision-makers and caretakers to receive alerts remotely and supports smart building integration. Cost-efficient devices and IoT connectivity enhance safety, allowing buildings and users to respond to CB alerts even when owners are away or local systems lack awareness.

This paper's primary contributions can be summed up as follows:

- the proposal of a novel remote awareness mechanism that enables individuals to receive CB emergency alerts affecting a specific location even when they are not physically present within the broadcast area, by introducing an extension of the traditional location-bound CB dissemination model;
- the development of an inexpensive, self-sufficient system for locally recording CB messages at the monitored area using commodity IoT hardware, demonstrating that reliable CB acquisition and storage can be achieved without specialized or proprietary infrastructure;

- the incorporation of an artificial intelligence (AI) agent to filter and categorize valid CB warnings from unprocessed modem signalling data before redistribution, operating directly on raw modem data at the edge to reduce false positives and enable intelligent alert handling;
- an experimental evaluation demonstrating reliable operation, with end-to-end redirection delays ranging between 57 and 70 seconds, providing results that encourage the adoption of the proposed system in an operational context.

By integrating mobile networks with internet-based communication channels, the proposed system improves emergency alerting inclusiveness, resilience and adaptability. The paper reviews related technologies, describes the system design and methodology, presents experimental results, discusses findings against existing work and concludes with future research directions.

2. Literature Review

This section reviewed the state of the art in communication and alerting technologies for public safety and emergency management. The literature regarded four complementary perspectives: core public safety communication infrastructures, mobile public alerting mechanisms, decision support and multi-agent coordination approaches and IoT and edge-based emergency alert systems.

These four directions were selected because they cover the main components of modern emergency alerting and management systems: communications infrastructure, transmission of alerts to the population, decision-making support for authorities and the integration of emerging technologies such as IoT and edge computing. Within this structure, both theoretical aspects related to the addressed concepts and relevant empirical results reported in the literature were presented and discussed.

2.1. Public Safety Communications

In accordance with works of Friedman (2022) and Swan (2023), the concept of public safety is associated with *“the function of protecting or safeguarding people against violent harm to themselves or their property caused by third parties or nature”*. This concept became the main concern of all states, which primarily directed their attention to protecting the population.

In specialized literature, such as work of Gourevitch, Kleiman and Falco (2022), the concept of public safety is often presented in the context of health or security, which is associated with feelings of physical, emotional, social and material security, also generated by the support offered by the community or society. In this context, Savoia, Lin and Viswanath (2013) said that it was important to have the greatest possible capacity of the authorities to quickly inform the population in critical situations, by carrying out several types of public communication efforts to announce people, encouraging the adoption of certain behaviours that could prevent potential problems, as well as limit the effects of unwanted events.

What is more, recent studies, such as the one of Boboc, Tataru, Bogdan and Simion (2026), have emphasized that preserving communication continuity during critical events is important for public institutions and other key services, especially when the primary network becomes unavailable. Resilient emergency infrastructures equipped with automated failover mechanisms can reduce downtime and maintain access to voice, messaging and data services during disruptive situations.

In emergency situations, telecommunications and informatics systems are mandatory because they provide the prompt dissemination of data and the compatibility of security-related information systems, forming the backbone of modern public safety communications. In accordance with work of Zhang, Li and Chen (2020), communications transmitted in emergency situations include both the information itself and the promotion or education of the public to increase public safety and awareness of emergency situations, all these activities having the role of shaping the behaviour of citizens to protect their health. In accordance with the work of Liu and Dong (2024), through these emergency communications, government departments ensured that they communicated directly and officially with the population, receiving authorized information.

In an emergency communications network, in accordance with the work of Wang et. al (2023), which is described as a heterogeneous network with a dynamic and varied composition, a series of communication technologies are used, these communicating through existing public or private networks. Communications carried out in a crisis situation must be effective clear, concise, at the right time, these having the role of reducing panic, confusion and providing society with clear indications on what it should do.

At the European level, communications in emergency situations involve the activity of Public Protection and Disaster Relief (PPDR) services, whose role is to provide rapid immediate assistance when the existence of a risk is determined that may affect individual or public life, health or safety, as well as public or private property, maintaining peace and order and providing support through communication activities carried out together with the police, firefighters or medical services.

2.2. Previous Work

The research began with identifying end-user needs and reviewing relevant scientific literature. Sources included Google Scholar and international journals such as the International Journal of Disaster Risk Reduction and the International Journal of Interactive Mobile and Computers. The collected materials were analysed and organised to support the research framework.

Recent studies indicated an evolution of public safety communications towards distributed architectures, capable of supporting rapid information exchange and coordination between entities involved in emergency management.

In this regard, Zhang, Zhang and Sun (2025) demonstrated that integrating IoT sensors, edge computing and cloud services can significantly improve the timeliness and operational effectiveness of public safety alerting systems. Based on a distributed network of heterogeneous sensors, edge computing nodes and cloud integration, they proposed and assessed a real-time IoT system for emergency response and public safety warning. Using secure MQTT communications, a developed prototype was tested in a smart city simulation testbed on four scenarios. The results of the paper highlighted constraints for public safety communications, including infrastructure dependability and large-scale scalability in actual crisis scenarios.

In addition, Damaševičius, Bacanin and Misra (2023) took a conceptual review approach to public safety communications, presenting the idea of the Internet of Emergency Services (IoES) as a framework for combining sensors, processing platforms and communications to facilitate coordination among emergency services. The study emphasized how real-time data-driven communications could enhance situational awareness and inter-agency cooperation, but it also highlighted enduring

issues with public safety communications infrastructures, including security, interoperability and the absence of extensive operational validations.

Carreras-Coch, Navarro, Sans and Zaballos (2022) examined emergency communication technology from the standpoint of public safety-specific needs, including reduced latency, dependability and agency interoperability. Based on a structured search in the Scopus and Web of Science databases, the paper conducted a systematic review in accordance with PRISMA 2020 standards. This was followed by the steps of identification, screening, eligibility and inclusion. The final research, which comprises 27 articles published between 2017 and 2021, revealed that hybrid architectures are necessary since no single technology could meet all public safety communications requirements. The work also pointed out the necessity for operationally validated implementations by highlighting a significant reliance on conceptual evaluations and a lack of consistent experimental validations.

Esposito, Palma, Belli, Sabbatini and Pierleoni (2022) conducted a systematic review of IoT-based solutions for Early Warning Systems (EWS) dedicated to natural disasters, including floods, earthquakes, tsunamis and landslides. In their research, the authors analyzed works published between 2017-2022, selected from several scientific databases (Google Scholar, IEEE Xplore, Elsevier and MDPI), focusing on adopted IoT architectures, communication protocols and operational requirements specific to real-time alerting. The findings emphasized the important part that cost-efficient devices and mobile IoT sensors played in environmental monitoring and alert production, as well as the benefits of combining Fog/Edge layers to lower latency, boost dependability and reduce dependency on cloud infrastructure. The need for standardized architecture tested in real-world conditions was highlighted by the authors' identification of recurrent limitations in the reviewed literature, such as the lack of interoperability between solutions, evaluations primarily carried out in controlled or simulated environments and insufficient operational validation of large-scale IoT systems.

Filip, Iliescu and Pop (2022) proposed an Internet of Things-based warning system, designed for selective and real-time alerting of users, using cost-efficient devices and efficient communication protocols. They created and executed a cloud-edge architecture that combines data storage in time series databases (InfluxDB), asynchronous communications via MQTT, local sensors linked to Raspberry Pi and secure authentication based on JSON Web Tokens. Analyzing alert latency, scalability and storage costs for up to 100 devices, the system was experimentally tested in a controlled environment using simulated data and actual external sources (OpenWeather API). The findings showed that leveraging inexpensive IoT devices for community alerting systems is feasible and the suggested design could provide real-time alerting with minimal latency and moderate resource requirements. Nonetheless, the work draw attention to pertinent constraints, including reliance on outside data sources, testing primarily in simulated scenarios and the absence of system validation in actual large-scale emergency operational contexts.

The literature then in publication showed a dearth of large-scale operationally proven solutions that could concurrently guarantee interoperability, scalability and dependability under actual crisis conditions, despite advancements in distributed architectures for public safety communications.

The proposed system improves emergency management through direct agency-citizen communication. Unlike existing solutions relying on sensors, databases or

automated alerts, it distributes notifications validated by emergency agencies themselves. This ensures greater authority, credibility and public trust, while community-generated or indirect-source alerts may reduce message reliability and impact.

3. Materials and Methods

This section presents the resources, infrastructure and methodology used to develop and validate the intelligent CB alert redirection system. After designing and evaluating the architecture, a laboratory environment was configured and software components implemented iteratively. The study focused on integrating the Llama2 7B model on constrained hardware and evaluating the feasibility, reliability and limitations of lightweight on-device LLMs for public-alert dissemination.

3.1. System Design

The system was designed to have a simplistic modular architecture, as depicted in Figure no. 1, in which any of the elements could be easily replaced if any adaptations, innovations or scaling were necessary. Laboratory setup is shown in Figure no. 2.

The signalling unit employed a compact, software-defined 2G cellular base station, YateBTS LabKit, designed for research, development, and educational purposes. This platform provided full control over radio access network functions, allowing configuration of transmission parameters, frequency allocation management and simulation of realistic mobile network scenarios in a controlled laboratory environment. The experiments were conducted in the GSM900 frequency band. The platform supported standard GSM protocols, including voice, SMS and CB functionalities, enabling development with both signalling and user plane traffic. Specifically, CB messages were generated using the Yate command-line interface (Yate Console). For the 2G modem, a Maestro 100 Series GSM/GPRS Modem Lite device was used, which was connected to the signalling unit and interfaced with the GSM network during the experiments. Both the YateBTS LabKit and the Maestro modem were equipped with standard compliant regular antennas.

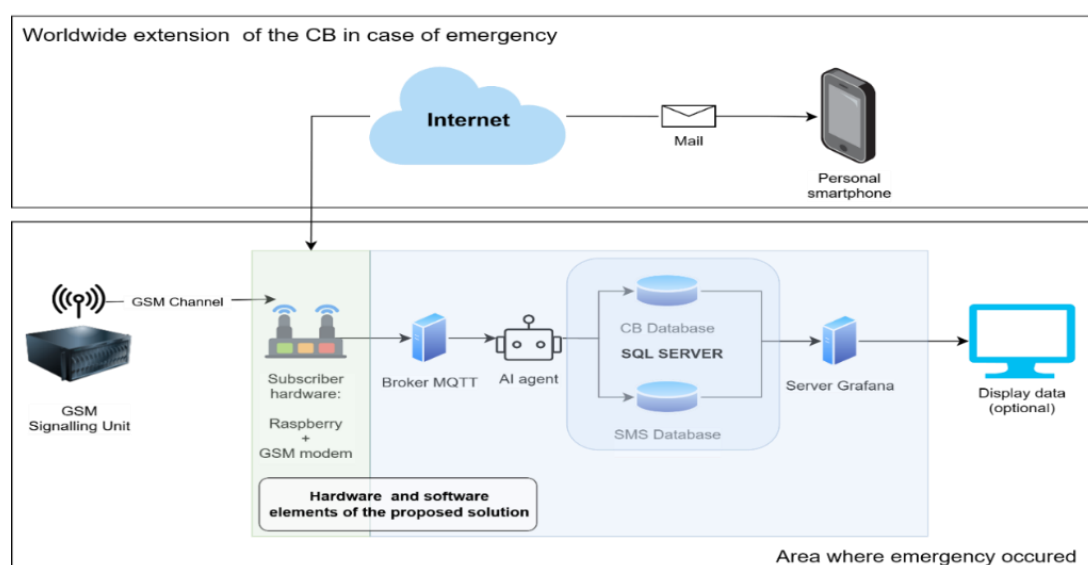


Figure no. 1: High-level system architecture
(Source: Authors' own contribution)

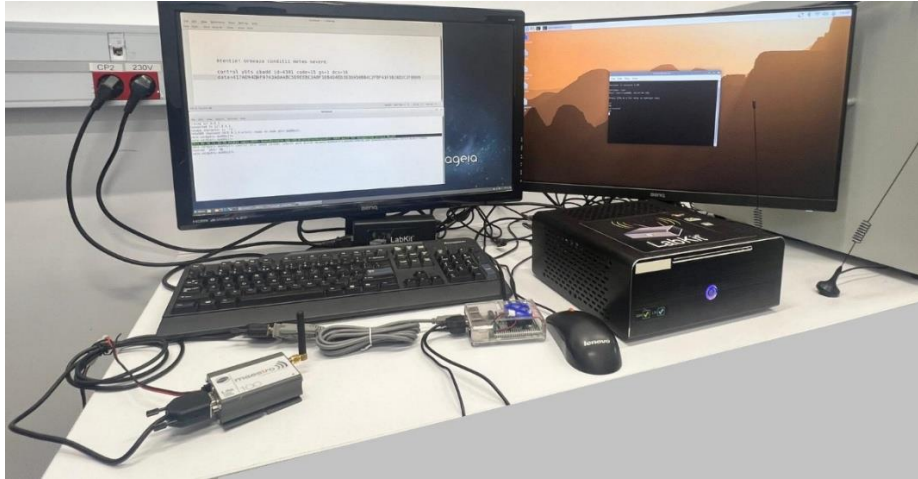


Figure no. 2: Laboratory setup
(Source: Authors' own contribution)

The platform enabled safe experimentation without requiring licensed frequency bands, making it suitable for academic innovation. Combining programmability, accessibility and GSM support, the 2G signalling unit was a versatile tool for exploring wireless communications, IoT integration and experimental automated alert forwarding in emergency management scenarios. It also sped up development by avoiding dependence on real network alerts. The subscriber system used a 2G cellular modem with a single-board computer to create a unified platform for automated reception, decoding and processing of SMS and CB messages. The modem connected via RS-232 serial, providing reliable communication and precise control, as shown in Figure no. 2 and Figure no. 3.

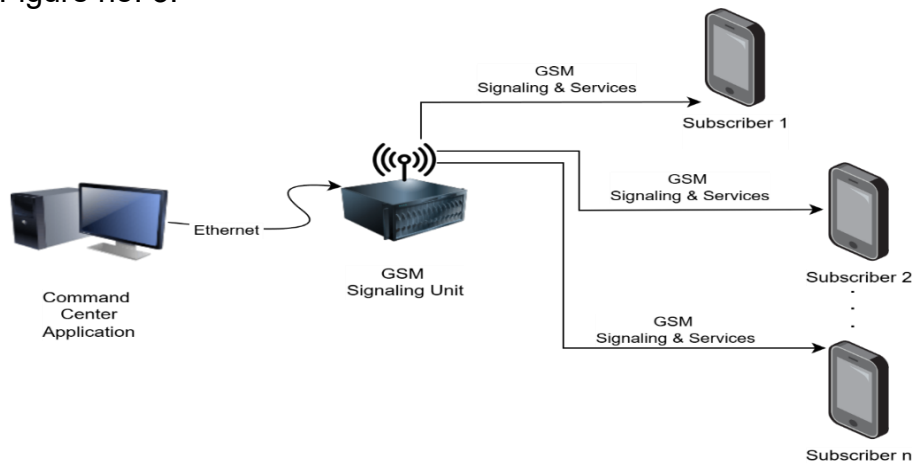


Figure no. 3: Subscriber module topology
(Source: Authors' own contribution)

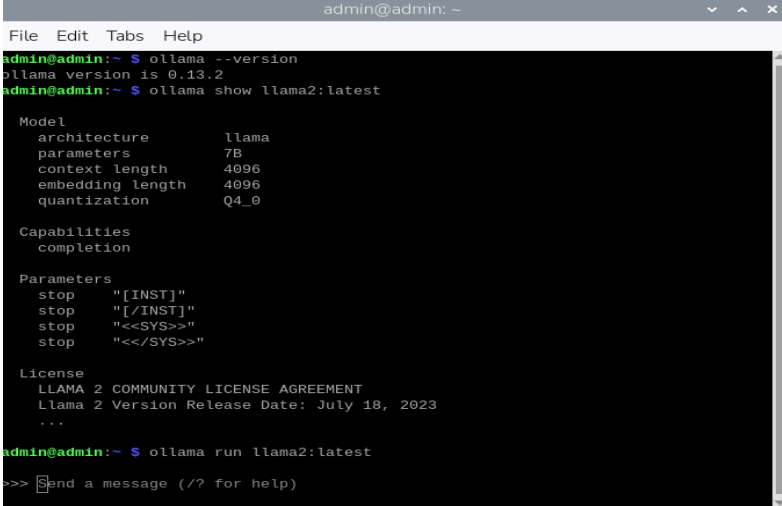
Modem selection was guided by strict compliance requirements with the GSM 07.05 standard, particularly its implementation of the specific AT command set necessary for CB reception. Reliable interoperability depended on compatibility with the signalling unit and workflow. Standardized commands minimized integration risks and enabled consistent message handling. A Python script on the Raspberry Pi controlled the modem, processed incoming network data, filtered irrelevant signals and forwarded messages to an AI-based platform for emergency alert classification.

To support communication between multiple devices, the Eclipse Mosquitto broker implementing the MQTT protocol was integrated for efficient data transport. Incoming payloads were published to the broker and consumed by the workflow automation engine, n8n, where the AI agent determined whether the received message represented an emergency alert or a standard SMS.

A key component of the proposed architecture was the Large Language Model (LLM) which aimed to interpret input data according to a predefined prompt. The purpose was not to use AI solely to distinguish between SMS and CB messages. Rather, the AI component was employed as an additional layer for message filtering, classification and contextual analysis after message reception. AI model was primarily used for contextual interpretation of message content. This can include aspects regarding severity assessment, urgency and relevance of received alerts. Based on this analysis, the system could determine whether further actions should be triggered.

For this paper, Llama 2 7B model was chosen due to relatively small size, quantization compatibility, offline edge inference capability, low power consumption and suitability for privacy preserving, cost-effective deployments. The Llama 2 7B model is a 7-billion-parameter model developed by Meta as part of the Llama 2 family. It is fine-tuned for dialogue applications, making it suitable for tasks such as chatbots, virtual assistants and interactive AI systems.

The model has been chosen as the foundational language model for the application due to a combination of performance, efficiency and flexibility. It was available for local deployment via the Ollama platform, which provided a command-line interface and API for interaction. Additionally, Llama 2 models are open-weight and open-source, enabling custom fine-tuning for domain-specific tasks without decisive limitations. The 7B variant offers an optimal balance between accuracy and computational efficiency, allowing the application to deliver responsive, high-quality interactions while remaining cost-effective.



```
admin@admin: ~  
File Edit Tabs Help  
admin@admin:~ $ ollama --version  
ollama version is 0.13.2  
admin@admin:~ $ ollama show llama2:latest  
  
Model  
architecture      llama  
parameters        7B  
context length    4096  
embedding length  4096  
quantization      Q4_0  
  
Capabilities  
completion  
  
Parameters  
stop              "[INST]"  
stop              "[/INST]"  
stop              "<<SYS>>"  
stop              "<</SYS>>"  
  
License  
LLAMA 2 COMMUNITY LICENSE AGREEMENT  
Llama 2 Version Release Date: July 18, 2023  
...  
admin@admin:~ $ ollama run llama2:latest  
>>> Send a message (/? for help)
```

*Figure no. 4: Ollama tool run on Raspberry Pi board
(Source: Capture from Raspberry Pi 4B terminal)*

As depicted in Figure no. 4 and Figure no. 5, the model may be executed locally on both commercial off-the-shelf (COTS) computing system or single-board computer, according to user's needs, eliminating the need for specialized or proprietary hardware.

As it can be seen in Figure no. 3, Ollama facilitated easy setup and execution of the model, enabling users to integrate it into various applications requiring natural language understanding and generation capabilities. As shown in Figure no. 6, the system was evaluated on hardware using the locally hosted Llama 2 7B model. During inference we observed an average CPU utilization of 98% and a peak memory consumption of approximately 3.27 GB.

All processed data was then stored in a MariaDB relational database, providing persistent storage for both raw messages and classification results. This ensured traceability, supports long-term analysis and enabled flexible query execution for retrospective studies.

```

admin@admin: ~/assistant/MN_teste
File Edit Tabs Help

admin@admin:~/assistant/MN_teste $ time cat /home/admin/assistant/MN_teste/alert.txt | ollama run llama2:latest
YES

real    1m9.120s
user    0m0.222s
sys     0m0.158s

admin@admin:~/assistant/MN_teste $ time cat /home/admin/assistant/MN_teste/sms.txt | ollama run llama2:latest
NO

real    0m57.071s
user    0m0.134s
sys     0m0.195s

admin@admin:~/assistant/MN_teste $

```

Figure no. 5: Inference duration for model llama2: latest running on Raspberry Pi board
(Source: Capture from Raspberry Pi 4B terminal)

```

admin@admin: ~/assistant/llama.cpp/models/7b
File Edit Tabs Help

* admin@a... x admin@ad... x admin@ad... x

0[|||||97.5%] Tasks: 94, 319 thr, 139 kthr; 4 running
1[|||||99.4%] Load average: 4.12 4.32 3.91
2[|||||98.7%] Uptime: 08:04:04
3[|||||97.5%]
Mem[|||||3.27G/7.64G]
Swp[|||||333M/2.00G]

Main 720
PID USER PRI NI VIRT RES SHR S CPU%MEM% TIME+ Command
5411 admin 20 0 6225M 6052M 0 R 97.9 77.4 4:41.56 ./llama-cli -m /home/admin/assistant/llama.cpp/models/7b/llama-2-7b.Q4_K_M.gguf -no-cnv -p You at
5406 admin 20 0 6225M 6052M 3903M R 97.3 77.4 4:45.44 ./llama-cli -m /home/admin/assistant/llama.cpp/models/7b/llama-2-7b.Q4_K_M.gguf -no-cnv -p You at
5410 admin 20 0 6225M 6052M 0 R 91.6 77.4 4:42.39 ./llama-cli -m /home/admin/assistant/llama.cpp/models/7b/llama-2-7b.Q4_K_M.gguf -no-cnv -p You at
5412 admin 20 0 6225M 6052M 0 R 91.6 77.4 4:41.59 ./llama-cli -m /home/admin/assistant/llama.cpp/models/7b/llama-2-7b.Q4_K_M.gguf -no-cnv -p You at
1681 admin 20 0 555M 50720 36572 S 6.4 0.6 4:26.73 /usr/bin/x-terminal-emulator
5302 admin 20 0 1976 263M 121M S 3.8 3.4 2:48.36 /usr/lib/chromium/chromium --type=renderer --crashpad-handler-pid=0 --enable-crash-reporter=buil
5417 admin 20 0 9200 5576 3092 R 3.8 0.1 0:00.68 htop

```

Figure no. 6: Hardware usage during inference
(Source: Capture from **htop** command output, from Raspberry Pi 4B terminal)

Grafana, the monitoring and visualization platform, was connected to the database, offering dashboards for real-time observation of message traffic and classification outcomes. Additionally, MQTT Explorer client application was involved to inspect broker activity, supporting debugging, validation and manual monitoring of message flow.

In accordance with chaos theory, even a negligible error introduced during the initial phase of an analysis may result in divergent conclusions at the culmination of the process. Since the alert system generated CB messages with a confident structure to real ones, the classification prompt was crafted to include instructions referencing emergency phrases, with clearly defined rules and expected response formats to ensure precision and reduce ambiguity during automated processing and validation, as shown in Figure no. 6. This was implemented to align more closely with the model specifications outlined in the official Llama 2 model card. Maturing the application to support messages in more languages can be achieved either by optimizing the chosen model for this purpose by fine-tuning with other languages or by using other multilingual models such as Gemma 2 2B. For either of the two options, a dedicated stage is required.

Is the text in quotes about a Cell Broadcast emergency alert "MESSAGE_FROM_GSM_MODEM"?
If no critical emergency, respond only with NO.
If critical emergency, respond only with YES.

Figure no. 7: Prompt example for classifying messages received by the modem
(Source: Authors’ own contribution)

Testing and validation ensured the system’s reliability and accuracy. Unit and integration tests verified modem communication, message parsing, data transmission and workflow operation across all components. Performance evaluation measured latency, throughput and AI classification accuracy using simulated alerts. Robustness tests under unstable network conditions confirmed resilience against connectivity issues, message bursts and broker overloads. Results demonstrated reliable, accurate and real-time emergency alert management suitable for deployment.

4. Results

The results obtained during system evaluation demonstrated the reliability, efficiency and traceability of the proposed architecture under various operational conditions. Message acquisition and internal routing were successful for both SMS and CB events across multiple test scenarios. As shown in Table no. 1, the system consistently responded, without observable errors, the tasks for which it was designed.

Table no. 1
CB messages from database

ID	Message	Date
1	CBM 1641643701611TEST ST3 ROALERT	2025-07-23 12:06:57
2	CBM 1641843701611TEST ST3 ROALERT	2025-07-23 12:26:55
3	CBM 1642043701611TEST ST3 ROALERT	2025-07-23 13:12:49
4	CBM 1642243701611TEST ST3 ROALERT	2025-07-23 13:29:41
5	CBM 1642343701611TEST ST3 ROALERT	2025-07-23 13:31:38
6	CBM 1642443701611TEST ST3 ROALERT	2025-07-23 13:34:29
7	CBM 1642543701611TEST ST3 ROALERT	2025-07-23 13:36:25
8	ALERTA DE TEST SISTEM FUNCTIONAL	2025-07-26 15:45:49

ID	Message	Date
9	[CB] TEST AUTOMAT DE INFORMARE	2025-07-26 16:01:54
10	[CB] ALERTA SEISMICA SIMULATA	2025-07-26 16:02:03
11	[CB] ALERTA SEISMICA SIMULATA	2025-07-26 16:02:25

(Source: Authors' own contribution)

As Figure no. 7 depicts, the e-mail notification system was validated through repeated testing with a dedicated Gmail account, confirming reliable message generation and delivery. Authentication used an API key instead of passwords and the system maintained an encrypted SMTP connection, improving security. The script automatically dispatched HTML-formatted emails, shown in Figure no. 8, from the classification workflow and supported multiple recipient addresses. CB alert classification triggered near real-time email notifications with only a few seconds of latency, due to the inference process, as depicted in Figure no. 4. Other sub-assemblies involve negligible delays, while failures were rare and mainly due to external network issues.

Table no. 2
Confusion matrix for received messages

	Predicted SMS	Predicted CB	Total
Actual SMS	21	5	26
Actual CB	0	32	32

(Source: Authors' own contribution)

Figure no. 9 presents a live analytics platform for near real-time monitoring of throughput and processing times. A quantitative performance analysis was conducted over a period of approximately three weeks, during which a total of 58 messages were processed (26 SMS and 32 CB alerts). The average internal latency, measured from message reception to database storage, ranged between five and ten seconds. Using the locally deployed LLM, the AI agent classified 21 of the 26 SMS messages correctly (81%) and all 32 CB alerts correctly (100%), corresponding to an overall accuracy of 91.4% (53/58). The full distribution is reported in the confusion matrix in Table no. 2. Notably, no CB alert was misclassified, while the five misclassifications were confined to non-critical SMS traffic. These errors may arise when the content of an SMS closely mirrors the structure, tone and type of information typical of CB messages, so that no clear cue remains to differentiate the two transmission types. A representative case being promotional messages designed for strong customer impact. Given the limited sample size and the short evaluation window, these results should be interpreted as a proof-of-concept indication of feasibility. In an alert-dissemination context the relevant safety property is that no CB alert was missed, an effect further mitigated when human-in-the-loop principles are applied. A broader assessment of reliability and scalability, based on a larger and more diverse dataset, is thought to be a topic for future development.

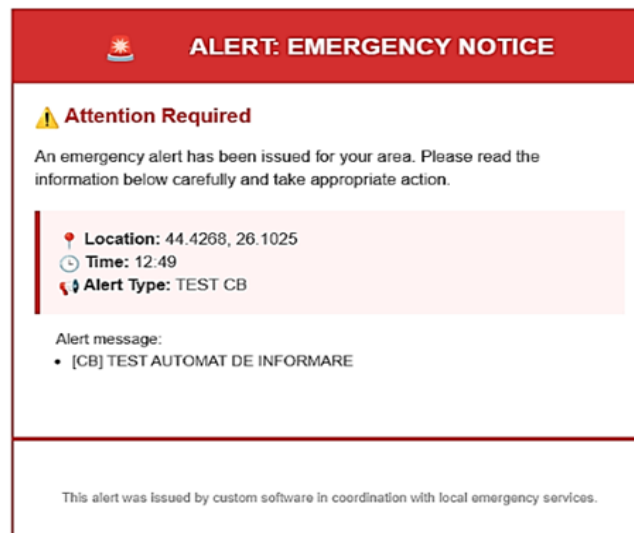


Figure no. 8: E-mail notification
(Source: Authors' own contribution)

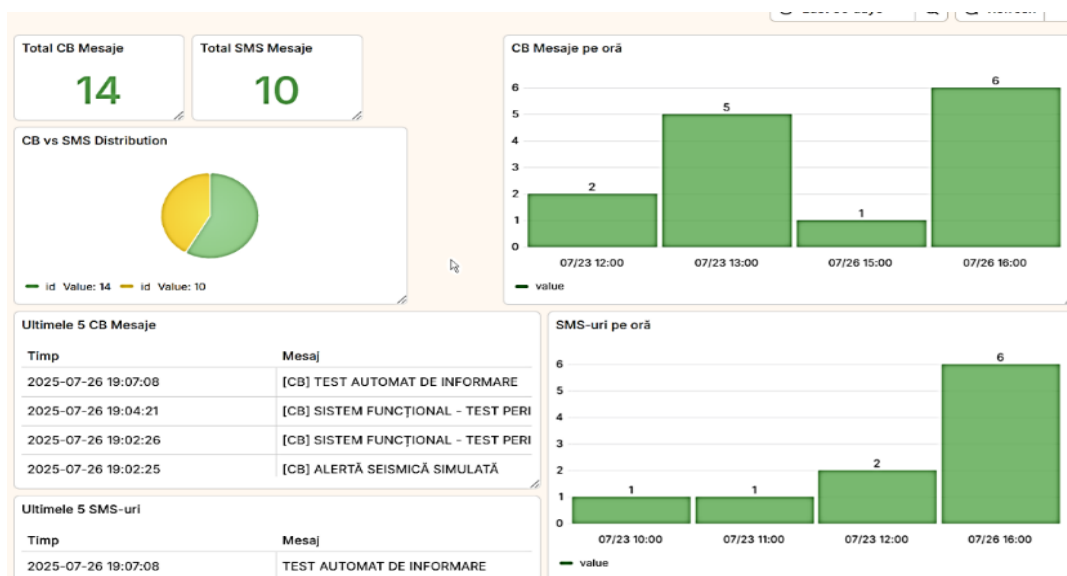


Figure no. 9: Grafana dashboards indicating intermediary results
(Source: Authors' own contribution)

5. Discussion

Two added benefits of the proposed solution are enhanced security and scalability. The integration of an Eclipse Mosquitto broker inside the IoT network created the means for simpler device management. This potential benefit provided modularity and improved connectivity, foreseeing the substantial benefit brought by the emergent mobile communications technologies, converging massive networks and services. The CB receiving modem can be seen as a sensor, which could be connected in the cyber-world, feeding data to a system that acts into the real world, thus enhancing the security.

Security can be enhanced by applying physical protection measures, improving resilience, and securing communications. Although the local laboratory setup did not require SSL/TLS certificates in Eclipse Mosquitto, real-world deployments over

distributed or contested networks should implement certificates and additional security measures. In critical environments, robust cyber protection is needed to ensure data confidentiality, integrity, availability and resilient operation against evolving threats.

What is more, if targeted area has Cyber Physical Systems (CPS) or IoT devices capable of undertaking physical actions, when connected with the CB system, it becomes Cyber-Aware, meaning that actions in physical world are based or triggered by events in the cyber-space. Based on the simpler, more efficient, similarity-based method, events from the real world with events from cyber-space can be correlated using an AI model that comprehends the bigger picture, assesses risks or consequences and even recommends actions. Applied in the enterprise or personal environment, this innovation could consolidate overall security by merging alerts from two domains, the physical world and the cyber world.

Whether it be a Small Office/Home Office (SOHO) or a Security Operations Center (SOC) which has the ability, through IoT devices, to undertake some measures in the case of an event announced by an alert, facilities of any level can benefit from this capability. Despite being impossible to define all the causal relationships between physical and cyber alerts, self-protection for any site is constructive for enhancing security.

6. Conclusions

Evaluation results confirmed that proposed system achieved its objective of reliably acquiring, classifying and disseminating CB alerts and SMS within a lightweight architecture. In laboratory conditions, it demonstrated stable performance, high email notification delivery rates and consistent data integrity, highlighting the feasibility of combining low-cost hardware, workflow automation tools and AI agents for public safety communication.

The system proved useful where conventional mobile devices are limited, extending emergency alerts via Internet-based channels and improving situational awareness through real-time traffic visualization. However, limitations remain, including room for improvement in classification accuracy, dependence on external services such as SMTP and the need for redundancy, scalability and stronger long-term reliability. GSM was selected for its coverage and affordability, especially in remote areas, though the architecture is adaptable to LTE and 5G. Future work will enhance AI classification, expand notification channels and strengthen security, ensuring a more resilient and scalable emergency alert platform overall.

Acknowledgements

The equipment and data used to support the findings of this study cannot be accessed due to commercial confidentiality. The authors would like to thank the two institutions where they are affiliated, The Special Telecommunications Service and National University of Science and Technology POLITEHNICA Bucharest, for the continuous support provided in joint research activities.

Author Contributions

Conceptualization and design of the study and application, research methodology, formal analysis and manuscript preparation, M.-V.N.; data collection and data interpretation, creation and integration of the software modules of the application, A.-P.M. and C.-A.P.; testing and validation of the results, analysis of the security measures related to this application, F.H. All authors have read and approved the final version of the manuscript.

REFERENCES

- Boboc D.N., Tataru I., Bogdan I.C. & Simion E. (2026). A proposal for a scalable emergency infrastructure: ensuring communication continuity in critical situations. *U.P.B. Scientific Bulletin, Series C, Vol. 88, Issue 1*, 161-178. ISSN 2286-354.
- Bopp, E., Douvinet, J., Carles, N., Foulquier, P., & Péroche, M. (2024). Spatial (in) accuracy of cell broadcast alerts in urban context: Feedback from the April 2023 Cannes tsunami trial. *Computers, Environment and Urban Systems*, 107, 102055. Available at: <https://doi.org/10.1016/j.compenvurbsys.2023.102055>.
- Carreras-Coch, A., Navarro, J., Sans, C., & Zaballos, A. (2022). Communication technologies in emergency situations. *Electronics*, 11(7), 1155. Available at: <https://doi.org/10.3390/electronics11071155>.
- Damaševičius, R., Bacanin, N., & Misra, S. (2023). From sensors to safety: Internet of Emergency Services (IoES) for emergency response and disaster management. *Journal of sensor and actuator networks*, 12(3), 41. Available at: <https://doi.org/10.3390/jsan12030041>.
- Esposito, M., Palma, L., Belli, A., Sabbatini, L., & Pierleoni, P. (2022). Recent advances in internet of things solutions for early warning systems: A review. *Sensors*, 22(6), 2124. Available at: <https://doi.org/10.3390/s22062124>.
- European Telecommunications Standards Institute – ETSI. (1999). *Digital cellular telecommunications system (Phase 2+); Technical realization of Short Message Service Cell Broadcast (SMSCB), (GSM 03.41 version 5.9.1 Release 1996)*. Available at: https://www.etsi.org/deliver/etsi_i_ets/300900_300999/300902/05_60/ets_300902e05p.pdf.
- European Telecommunications Standards Institute – ETSI. (1997). *Digital cellular telecommunications system (Phase 2+); Use of Data Terminal Equipment – Data Circuit terminating; Equipment (DTE - DCE) interface for Short Message Service (SMS) and Cell Broadcast Service (CBS), GSM 07.05 version 5.3.0*. Available at: https://www.etsi.org/deliver/etsi_gts/03/0338/05.02.00_60/gsmmts_0338v050200p.pdf.
- Filip, I.D., Iliescu, C.M., & Pop, F. (2022). Assertive, Selective, Scalable IoT-Based Warning System. *Sensors*, 22(3), 1015. Available at: <https://doi.org/10.3390/s22031015>.
- Friedman, B. (2022). What is public safety?, *Boston University Law Review*, 102, 725. Available at: <https://gretchen.law.nyu.edu/fac-articles/441>.
- Gourevitch, M.N., Kleiman, N., & Falco, K.B. (2022). Public health and public safety: Converging upstream. *American Journal of Public Health*, 112(5), 716-718.
- Liu, J., & Dong, C. (2024). Cross-departmental emergency coordination characteristics formed by multiple risks: evidence from production safety special emergency campaigns across government levels in China. *International Journal of Disaster Risk Reduction*, 111, 104672. Available at: <https://doi.org/10.1016/j.ijdr.2024.104672>.
- Savoia, E., Lin, L., & Viswanath, K. (2013). Communications in public health emergency preparedness: a systematic review of the literature. *Biosecurity and bioterrorism: biodefense strategy, practice and science*, 11(3), 170-184. DOI: 10.1089/bsp.2013.0038.
- Swan, S.L. (2023). Public duties for the new city. *Michigan Law Review*, 122(2), 315. Available at: <https://doi.org/10.36644/mlr.122.2.public>.

Wang, Q., et al. (2023). An overview of emergency communication networks. *Remote Sensing*, 15(6), 1595. Available at: <https://doi.org/10.3390/rs15061595>.

Zhang, H., Zhang, R., & Sun, J. (2025). Developing real-time IoT-based public safety alert and emergency response systems. *Scientific Reports*, 15(1), 29056. Available at: <https://doi.org/10.1038/s41598-025-13465-7>.

Zhang, L., Li, H., & Chen, K. (2020, March). Effective risk communication for public health emergency: reflection on the COVID-19 (2019-nCoV) Outbreak in Wuhan, China. *Healthcare*, 8(1), 64. MDPI. DOI: 10.3390/healthcare8010064.