International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 10 | Oct 2026 www.irjet.net p-ISSN: 2395-0072

# AI – GSM BASED PROTECTION SYSTEM TO IDENTIFY THE INRUDERS

**Dr. P. Loganthurai[1], Nithish Kumar S J[2], Thirumalai Ayyappan R J[3], Jayavel Prawin N R R[4]**

*[1]Associate Professor, Dept. of Electrical and Electronics Engineering, K.L.N. College of Engineering, Pottapalayam, Sivagangai, Tamil Nadu, India*

*[2,3,4]Final Year B.E. Students, Dept. of Electrical and Electronics Engineering, K.L.N. College of Engineering, Pottapalayam, Sivagangai, Tamil Nadu, India*

---

**Abstract -** *Manual patrolling of long and rugged land borders is tiring, hazardous and unreliable, especially at night and in bad weather, and standalone motion sensors raise too many false alarms to replace it. This paper presents the design and implementation of a fully automated, tiered intrusion detection and early-warning system built around an STM32 microcontroller. The system uses three sensing layers: a microwave Doppler radar that gives the earliest indication of human movement, and two laser and light dependent resistor tripwires that detect physical crossing of an outer and an inner border line. The microcontroller debounces and fuses the three inputs, confirms a threat only when independent sensors agree, and grades the situation into four alert levels. Local alerts are given through a buzzer and a 16 by 2 I2C LCD, and confirmed intrusions are reported to the command post as SMS through a GSM module, so that no soldier needs to be posted at the line. The paper also presents a frequency analysis of the Doppler radar, with calculated beat frequencies for crawling, walking, running and vehicle targets, the effect of the angle of approach, Extensions towards Bayesian sensor fusion, LoRa mesh communication, multilateration and encrypted telemetry are outlined. It can be used in any location but, we are used in border lines because country safety is important to enhance national security and protect human lives by developing actionable public safety frameworks that foster a peaceful and secure socity.*

**Key Words: Border surveillance, Intrusion detection, Doppler radar, Laser tripwire, Sensor fusion, STM32 microcontroller, GSM alert, Embedded systems.**

## 1. INTRODUCTION

India has one of the longest and most difficult land borders in the world, running through deserts, dense forest, rivers and high mountains. Border areas guarded by Indian soldiers face constant risks of secret intrusion, cross-border infiltration and sudden attacks [1], [2]. These incidents also harm local civilians, because enemies often manage to enter Indian territory completely unnoticed. Guarding such a long boundary by manual patrolling alone is tiring, dangerous and unreliable, particularly at night and in bad weather. Automatic electronic surveillance can extend the reach of the soldier, give early warning and reduce the risk to personnel.

A good system must detect a threat early, verify it as it comes closer, and raise a confirmed alarm only when the evidence is strong, so that soldiers are not overloaded with false alarms. No single low-cost sensor can do all three. A Doppler radar sees movement in darkness, fog and smoke but cannot tell a person from an animal, while an optical tripwire is reliable but only reports a crossing at one line.

This paper develops such a system around an STM32 microcontroller. It combines a Doppler radar for early detection of movement with two laser–LDR tripwire lines for detecting physical crossing, and reports the situation locally through a buzzer and an LCD and remotely through a GSM module. The main contributions are: (i) a three-layer sensing architecture with sensor fusion on a 32-bit microcontroller, (ii) a four-level alert scheme with SMS reporting to the command post, (iii) a worked frequency analysis of the Doppler sensor, including the effect of approach angle, and (iv) a low-cost working prototype.

### 1.1 Problem Statement

A large number of attacks happen in cities and cause suffering to ordinary civilians, and the enemy is often able to enter the country unnoticed. The hilly terrain along the Indian border makes enemies difficult to detect, so they can cross into the country easily. An intelligent monitoring and protection system is therefore required, which detects intrusion automatically, grades the threat and alerts the forces in time.

### 1.2 Objectives

1. To design a sensor network capable of automatically detecting human movement or intrusion near the border line.
2. To implement a three-layer sensing arrangement of a Doppler radar and two laser–LDR tripwires on an STM32 microcontroller, with sensor fusion to confirm threats and avoid false alarms.
3. To provide local alerts through a buzzer and an LCD and remote alerts to the command post through GSM SMS.
4. To make the system fully automated so that no soldier needs to be stationed at the monitored line.

5. objective of our project is to enhance national security and foster a peaceful, safe environment where citizens can thrive.

## 2. LITERATURE REVIEW AND EXISTING METHODS

### 2.1 Related Work

Renuka et al. [1] present an autonomous ground robot that uses real-time face detection to secure border perimeters. Devkatte et al. [2] describe a hardware-based border security system in which a multi-sensor network along the boundary detects unauthorized physical crossings. Soldier-oriented systems such as a protection vesture [3] and a smart jacket [4] address the safety of the individual soldier, which is complementary to perimeter monitoring. On the radar side, micro-Doppler signature analysis has been widely studied for target classification, including through-the-wall sensing [5], and Doppler-based moving-target detection that adapts to target speed has been reported [6]. Vedanth et al. [7] built a border surveillance system for soldiers on an Arduino Uno platform. The present work uses a 32-bit STM32 controller and layers a Doppler radar with two laser tripwires, so that a decision needs agreement between independent sensors.

### 2.2 Existing Methods

Present border and perimeter protection relies on manual watch, closed-circuit television, fencing with alarms, simple motion sensors and, for aerial threats, air-defence radar. Each has strengths but also limitations for close-range detection of foot intruders, as compared in Table -1.

**Table -1:** Existing methods compared with the proposed system

| Method | Strength | Limitation |
|---|---|---|
| CCTV / manual visual watch | Simple, widely deployed | Depends on visibility, lighting and continuous human attention |
| Fixed fencing with alarms | Physical deterrent | Static, easily bypassed; no distance or direction information |
| Standalone PIR motion sensors | Low cost, easy to deploy | High false-alarm rate; no distance measurement or tiered response |
| Air-defence radar / missile detection | Excellent for long-range aerial threats | Not designed for near-ground, close-perimeter intrusion by foot soldiers |
| **Proposed tiered multi-sensor system** | Doppler motion detection, dual laser tripwires and GSM reporting for a staged response | Prototype; needs site-specific field calibration; behaviour is context dependent |

## 3. METHODOGOLS

### 3.1 Layered Architecture

The sensors are arranged in layers along the approach to the border line (Fig. 1). **Layer 1** is a microwave Doppler radar that detects human movement in the outer zone and gives the earliest warning. **Layer 2** is the first laser tripwire (Tx1 and Rx1) at the outer border line: a laser beam falls on an LDR receiver, and when the beam is broken while the radar has also seen movement, the intrusion is treated as confirmed. **Layer 3** is a second tripwire (Tx2 and Rx2) at the inner border line; breaking it indicates the closest approach and raises the critical alarm.

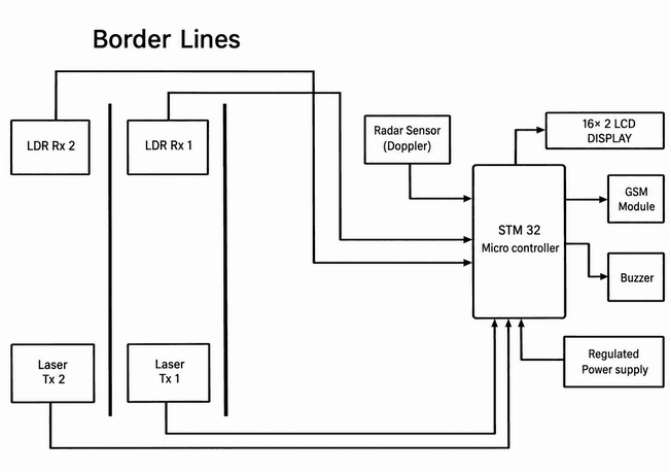



**Fig -1:** Block diagram of the proposed system

The STM32 controls the two laser transmitters and reads the beam status from the two LDR receivers and the radar output. It displays the status on the 16 by 2 LCD, drives the buzzer and sends the alert to the command post through the GSM module, while a regulated power supply feeds the microcontroller and all modules. Because an alarm is raised only when independent sensors agree, false alarms from animals, wind or a single noisy sensor are reduced and the soldiers get enough time to respond.

### 3.2 Alert Levels and Flow of the Program

The program flow is shown in Fig. 2. After power-on the STM32, LCD and GSM module are initialised and the laser transmitters are switched on. The controller then scans the sensors every 50 ms, accepting a reading only after three consecutive samples 50 ms apart (debouncing). It checks the inner tripwire first, then the confirmed condition of the outer tripwire with radar, then the unconfirmed condition, and finally updates the LCD, the buzzer and the SMS. An SMS is sent only when the level escalates, with a 60 s cool-down, so that the command

post is not flooded with repeated messages. The four alert levels are given in Table -4.

**Table -2:** Alert levels of the system

| Level | Condition | Local response | SMS |
|---|---|---|---|
| 0 Clear | sensor active | LCD: area secure; buzzer off | No |
| 1 Alert | Radar motion or a single unconfirmed beam break | LCD warning; area under observation | No |
| 2 Confirmed | Outer beam (Rx1) broken and radar motion within the last 10 s(East) | Intermittent buzzer; LCD: intrusion confirmed | Yes |
| 3 Critical | Inner beam (Rx2) broken(North East) | Continuous buzzer; LCD:intruders in border lines and measures the which direction | Yes |

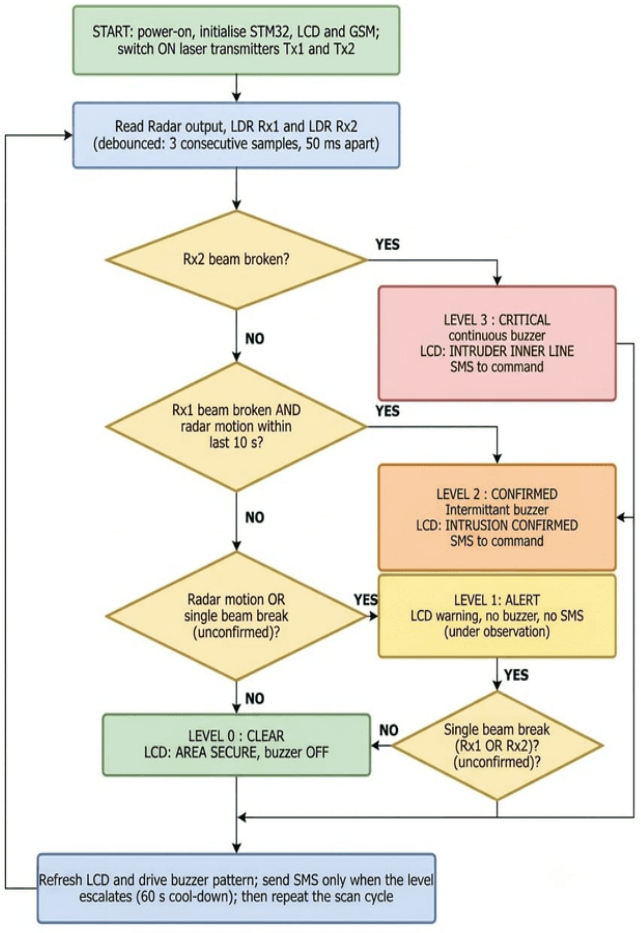



**Fig -2:** Flowchart of the decision logic

### 3.3 Firmware

The firmware is written in C++ using the Arduino IDE with the STM32duino core. The LCD is driven through the LiquidCrystal_I2C library at address 0x27 (or 0x3F, depending on the I2C backpack), the buzzer is driven from a GPIO pin and the GSM module is connected to USART1 at 9600 baud. To send a message the STM32 sets text mode with AT+CMGF=1, starts the message with AT+CMGS followed by the stored command-post number, sends the message body, and ends it with the ASCII character 26. A delay is kept after each step to give the module time to process and broadcast the text. When both beams are restored the buzzer is switched off and scanning resumes.

## 4. HARDWARE DESCRIPTION

### 4.1 Hardware modules

The modules and their roles are listed in Table -3. The STM32F103C8 ("Blue Pill") is a 32-bit ARM Cortex-M3 microcontroller running at up to 72 MHz with three USART interfaces, two I2C interfaces, SPI, timers with PWM and a 12-bit ADC, working at 3.3 V logic level [8]. Compared with an 8-bit controller it can read several sensors, run the decision logic and handle the GSM serial link at the same time. It is programmed through an ST-LINK V2 programmer using the SWD interface.

**Table -3:** Hardware modules and their roles

| Module | Key points | Role |
|---|---|---|
| STM32F103 C8 | Cortex-M3, 72 MHz, 3.3 V logic, 3 USART, 2 I2C, 12-bit ADC | Processing and decision logic |
| Laser Tx1, Tx2 | Low-power red laser-diode modules, narrow collimated beam | Light source of the tripwires |
| LDR Rx1, Rx2 | LDR with LM393 comparator and preset threshold; digital output | Beam-break detection |
| Doppler radar | RCWL-0516, continuous wave, about 3.2 GHz, digital output | Early motion detection |
| GSM module | SIM800, quad-band, AT commands over UART | SMS to command post |
| 16 by 2 LCD | I2C backpack using SDA and SCL lines | Local status display |
| Buzzer | Audible output device | Local alarm |
| Buck regulator | Adjustable DC–DC, more efficient than a linear regulator | Stable supply |

The laser module emits a narrow, highly collimated beam that can travel a long distance in a straight line and fall on a small receiver, which makes it a good source for an optical tripwire. Both lasers are switched on at start-up

and stay on during operation. Only low-power red modules are used and the beam must never be pointed at the eyes. In the LDR module a photoresistor, whose resistance falls as light increases, forms a voltage divider. An LM393 comparator with a potentiometer sets the threshold, so the digital output changes state when the beam is interrupted.

The SIM800 GSM module works with a standard SIM card and is controlled by AT commands over a serial link. It draws short current bursts of up to about 2 A during transmission and needs a supply of roughly 3.4 V to 4.4 V, so it is fed from the regulated supply with a bulk capacitor and not from the microcontroller board. As mobile carriers retire 2G networks, a 4G LTE module can replace it. The buck regulator output is set and checked with a multimeter before the modules are connected, and a common ground is kept between all modules.

### 4.2 Deployment Concept and Prototype

Fig. 3 shows how the prototype principle extends to a real border deployment. Laser sensor systems and radar sensors along the fence line pass their detections to a command centre, where alarms, control units, monitors, wireless communication and the GSM network are available to the operators, and the detections can be linked with the response systems of the forces. The assembled prototype is shown in Fig. 4, with all components mounted on one board and interconnected with colour-coded wires.




**Fig -3:** Conceptual deployment architecture along the border line

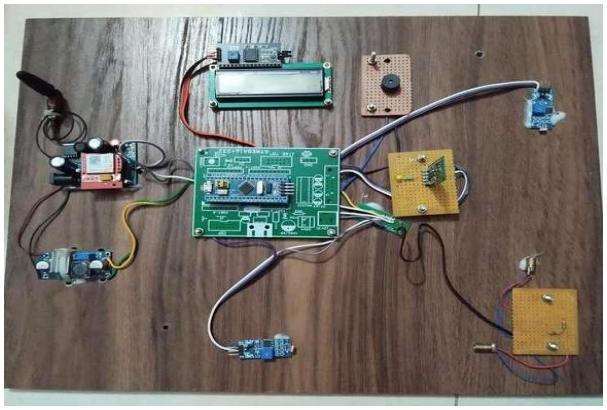


**Fig -4:** Assembled hardware prototype

## 5. DOPPLER RADAR FREQUENCY ANALYSIS

### 5.1 Principle and Operating Frequency

A Doppler radar bounces a microwave signal off a target and analyses how the motion of the target has altered the frequency of the returned signal, which gives the radial component of the target velocity. The RCWL-0516 is a continuous-wave (CW) module built around the RCWL-9196 chip. It transmits at a carrier frequency $f_c$ near 3.2 GHz (S-band), mixes the reflected wave with the transmitted wave, and outputs a low-frequency beat tone equal to the Doppler shift $f_d$. The shift for a target moving at speed v at an angle θ to the line of sight is

$$f_d = 2v \cos\theta / \lambda = 2v f_c \cos\theta / c \qquad (1)$$

where $c = 3 \times 10^8$ m/s and λ is the wavelength. The factor 2 accounts for the two-way path of a radar; without it the frequencies come out half of what the sensor produces. For this sensor $\lambda = c / f_c = 93.7$ mm, so $f_d = 21.33$ Hz for every 1 m/s of radial speed. The same 1 m/s target would give 6.67 Hz at 1 GHz, 70.17 Hz at 10.525 GHz (HB100, X-band) and 160 Hz at 24 GHz. A stationary target such as a wall, fence or parked object gives $f_d = 0$ and is rejected automatically, whereas a walking person produces a beat of tens of hertz that the on-board amplifier and comparator turn into a digital HIGH or LOW. A CW radar measures speed but not distance. The stock module outputs only the digital level, so the frequency analysis here is based on calculation and simulation of the amplified analog beat signal.

### 5.2 Calculated Doppler Data

Using $f_d = 21.33$ v, the speed of a target follows from $v = f_d \lambda / 2 = 0.046875 f_d$. The beat frequencies for different targets and the class boundaries derived from them are given in Table -3.

**Table -4:** Doppler beat frequency, speed and target class

| Class | $f_d$ band (Hz) | Speed (m/s) | Example target and $f_d$ |
|---|---|---|---|
| Clutter / noise | 0 – 3 | < 0.14 | Foliage or wind clutter, below 3 Hz: rejected |
| Slow / crawling | 3 – 15 | 0.14 – 0.70 | Slow crawl, 0.3 m/s: 6.4 Hz (hardest case) |
| Walking | 15 – 60 | 0.70 – 2.8 | Normal walk, 1.5 m/s: 32.0 Hz; fast walk or jog, 2.8 m/s: 59.7 Hz |
| Running | 60 – 160 | 2.8 – 7.5 | Run, 5.0 m/s: 106.7 Hz |
| Vehicle | > 160 | > 7.5 | Vehicle, 15 m/s (54 km/h): 320.0 Hz |

### 5.3 Effect of the Angle of Approach

The radar measures only the speed component along its line of sight, so $f_d = 21.33\ v \cos\theta$. A person walking at 1.5 m/s gives 32.0 Hz at $\theta = 0°$, 16.0 Hz at 60° and 0 Hz when walking straight across the beam (90°). A runner at 5 m/s and 60° gives 53.3 Hz. With an example noise floor of 5 Hz, the walking signal is lost when $\cos\theta = 5/32 = 0.156$, that is $\theta \approx 81°$, and a runner is lost near $\theta \approx 87°$. The sensor should therefore be aimed along the expected approach path, or two sensors at different angles should be used.

### 5.4 Role and Limits in the System

The Doppler node is the first trigger in the outer zone. It is cheap, works day and night, and rejects stationary objects. It gives no range or direction, cannot tell a person from an animal by itself, and the RCWL-0516 range is only a few metres. Received signal power falls as $1/R^4$, so doubling the distance cuts the return by a factor of 16 [9]. A single-channel sensor cannot tell approaching from receding; two signals 90 degrees out of phase (I/Q) give the sign of $f_d$. Two or more sensors at different angles each measure a radial speed $v_1 = v \cos\theta_1$ and $v_2 = v \cos\theta_2$, and solving these gives speed and heading. For these reasons the radar output is combined with the laser tripwires so that a decision needs agreement.

## 6. RESULTS AND DISCUSSION

Fig. 5 shows the LCD of the prototype. In the scanning state the second line shows the scanning status, and after a tripwire is broken the LCD shows the intruder area together with the message that the SMS has been sent, while the buzzer sounds. The SMS alerts received at the command-post numbers are shown in Fig. 6. The messages state the direction of the intrusion, and the receiving carrier application labelled the repeated identical messages as spam. This confirms the need for the escalation-only reporting and cool-down in Section 5.1.




**Fig -5:** LCD output: (a) intruder area with scanning status, (b) alert with SMS sent

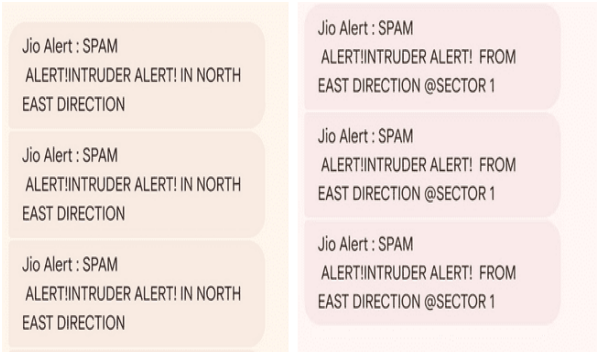



**Fig -6:** SMS alerts received: (a) north-east direction, (b) east direction at sector 1

The tripwire channels with the LCD, buzzer and SMS were demonstrated on the bench. The radar-confirmed Level 2 branch and the SMS cool-down are defined by the flowchart in Fig. 5 and still have to be added to the firmware and tested in the field. The reduction in false alarms is expected from the sensor fusion by design and has not yet been measured. A real site also needs calibration of the LDR thresholds, beam alignment and radar sensitivity for the local environment, and a real deployment needs long-range sensing nodes because the RCWL-0516 range is only a few metres. The SMS link depends on mobile network coverage.

## 7. CONCLUSIONS AND FUTURE WORK

A tiered intrusion detection and protection system for border areas has been designed and built around an STM32 microcontroller. The prototype integrates a Doppler radar, two laser–LDR tripwire lines, a 16 by 2 I2C LCD, a buzzer, a GSM module and a regulated power supply into one working unit. The system is designed to detect movement early, double-check the threat as it comes closer and raise an alarm only when independent sensors agree. Its four alert levels grade the response, and confirmed intrusions are reported to the command post by SMS, so the monitoring is automated and does not need soldiers at the line. The frequency analysis shows how beat frequency identifies the speed class of a target and

how the approach angle limits detection. Early warning reduces the risk to deployed soldiers (SDG 3), the embedded multi-sensor architecture upgrades local security infrastructure (SDG 9), and early detection of infiltration protects border settlements (SDG 11) and supports peaceful border management (SDG 16).

**Future work.** (i) Bayesian sensor fusion, which weights each sensor by its reliability and adds thermal, acoustic or seismic sensors. (ii) LoRa mesh communication between sensing nodes, so that alerts reach the command post where mobile coverage is poor. (iii) TDOA multilateration, to give the direction and position of the threat and not only its presence. (iv) AES-128 encrypted telemetry, so that alerts and location data cannot be intercepted or spoofed. (v) Solar power with battery backup for remote posts. (vi) A map-based command-centre dashboard with alert history, and vibration alerts for patrolling soldiers.

## REFERENCES

[1] B. Renuka, B. Sivaranjani, A. Maha Lakshmi and N. Muthukumaran, "Automatic Enemy Detecting Defense Robot by using Face Detection Technique," vol. 2, no. 2, pp. 495–501, Apr.–Jun. 2018, ISSN: 2456-883X.

[2] A. B. Devkatte, N. H. Chavan and M. K. Jha, "Defence Security System: Border Security," International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), vol. 5, no. 8, pp. 15054–15057, Aug. 2016, doi:10.15680/IJIRSET.2016.0508146.

[3] C. N. Thakur, A. S. Sirsat, M. Yadrami and S. Mudhol, "Soldier Protection Vesture," RTESIT-2019 Conference Proceedings, vol. 7, no. 8, Special Issue, 2019, ISSN: 2278-0181.

[4] U. I. Satteekar, S. Hussainnaik, A. Farhat and Ayeshabegum, "Smart Jacket for Soldiers," International Journal of Creative Research Thoughts (IJCRT), vol. 6, no. 2, pp. 706–710, Apr. 2018, ISSN: 2320-2882.

[5] C. Clemente, A. Balleri, K. Woodbridge and J. J. Soraghan, "Developments in target micro-Doppler signatures analysis: radar imaging, ultrasound and through-the-wall radar," EURASIP Journal on Advances in Signal Processing, vol. 2013, no. 47, pp. 1–18, Mar. 2013, doi:10.1186/1687-6180-2013-47.

[6] T. Xing, M. Jin, D. Fang, X. Zheng, X. Chen and K. Zhao, "Doppler Effect based Moving Target Detection Adaptive to Speed," CSAR '15: Proceedings of the 2015 ACM Workshop on Context-Aware Security and Applications, pp. 41–46, Nov. 2015, doi:10.1145/2820716.2820722.

[7] V. A. Vedanth, C. Chellaswamy, B. Ramasubramanian, G. Vikram and T. Ramachandran, "Border Surveillance System Using Arduino Uno for Soldiers," NCERC International Journal of Advanced Science, Engineering and Technology (NIJASET), vol. 1, no. 1, pp. 1–14, 2022.

[8] STMicroelectronics, "STM32F103x8 / STM32F103xB Datasheet."

[9] M. I. Skolnik, Introduction to Radar Systems, 3rd ed. New York, NY, USA: McGraw-Hill, 2001.

[10] Dirk Hovy, "The Enemy in your Owp Camp: How Well Can We Detect Statically- Generated Fake Reviews – An Adversarial Study," Procedings of the 54th Annual Meethigs of the Association for Computational Linguistics (ACL),pp. 351-356,Berlin ,Germany,August 2016.