

## END-TO-END SECURE WIRELESS SENSOR NETWORK USING PKI INFRASTRUCTURE AND RASPBERRY PI PICO W

Emil Gocan <sup>1</sup>

Gabriela Bucur <sup>1\*</sup> 

Cristina Popescu <sup>1</sup>

<sup>1</sup> Petroleum-Gas University of Ploiesti, Romania

\* e-mail: gbucur@upg-ploiesti.ro

DOI: 10.51865/JPGT.2025.01.23

### ABSTRACT

Industry 5.0 is the evolution of the industrial revolution that goes beyond automation and smart systems (Industry 4.0). It focuses on human-machine collaboration, sustainability, resilience, and security. The proposed security system also aligns with the vision of Industry 5.0, which emphasizes not only automation and efficiency but also cyber-resilience, sustainability, and human-centric design. By employing a Public Key Infrastructure (PKI) combined with JWT-based authentication and lightweight cryptographic techniques, the proposed system enhances the trustworthiness and adaptability of Wireless Sensor Networks (WSNs). These features are critical for Industry 5.0 environments, where secure collaboration between humans and intelligent devices is expected to be seamless, scalable, and resilient against emerging cybersecurity threats.

This paper proposes a secure, lightweight, end-to-end architecture for WSNs using a Raspberry Pi Pico W microcontroller, digital certificates and a Public Key Infrastructure (PKI) server. The system uses AES and RSA cryptography, JWT-based authentication, and HTTPS communication to protect data from MITM, replay, spoofing, and injection attacks. Data collected from sensors is encrypted and sent via a REST API to a secure server with MySQL integration. The paper details the implementation, testing, and performance of this model and discusses its limitations and future improvements, including extended sensor coverage and blockchain-based trust models.

**Keywords:** WSN, MITM, replay attack, injection, spoofing, PKI server, WSN security, IoT, Industry 5.0

### INTRODUCTION

The history of wireless sensor networks (WSNs) dates back to the 1970s, with the initial research on wireless sensor and communication technologies. However, the development of wireless sensor networks experienced significant expansion only in the 1990s-2000s, due to advances in microelectronics technology, wireless communications, and energy management. Since 2000, wireless sensor networks have evolved significantly due to the improvement of processing and communication technologies, and the increasing demands of the Internet of Things (IoT) sector [1], [4], [6], [17], [25]. Their importance stems from

several key features: WSNs are inherently distributed, cost-effective, resilient to faults, capable of self-organization, simple to deploy, scalable, and can operate independently without relying on pre-existing infrastructure [8].

Wireless Sensor Networks (WSNs) are communication systems consisting of a series of sensor nodes interconnected via wireless channels. Each node in the network is equipped with sensors that collect data from the environment (such as temperature, humidity, pressure, motion or other physical variables) and transmit them to a central node or to other nodes in the network for processing or storage [21], [9].

Similar to conventional networks, Wireless Sensor Networks (WSNs) face various security threats, including eavesdropping, data tampering, and unauthorized packet insertion. However, these systems are often constrained by limited processing capacity, power consumption, and bandwidth. Due to these resource limitations, safeguarding data becomes more challenging. To overcome this, encryption techniques are employed to secure data transmission and defend against potential malicious activities [13], [24].

Wireless sensor networks are characterized by the following features: **Autonomy:** Sensor nodes are usually powered by batteries and operate autonomously, without requiring a constant external power source; **Scalability:** Networks can comprise a large number of nodes, which can be placed in various locations to cover a large area; **Wireless communication:** Nodes are interconnected through a wireless communication network, which allows for flexible operation without cables; **Low size and cost:** Sensor nodes are often small and economical, which makes them easy to deploy on a large scale in various applications; **Data processing systems:** Sensor nodes can process the data collected locally and send the relevant information to a central server or processing device.

Typically, IoT devices function as simple data collectors and to communicate efficiently in transmitting and receiving data over long distances, accessible from anywhere in the world, they need the computing power of the cloud [5], [7]. However, the cloud itself is not just a storage space. To make sense of the dispersed information gathered by various IoT devices, this data must be processed and analyzed in an efficient way, as can be seen in Figure 1 [17], [19], [20], [29].

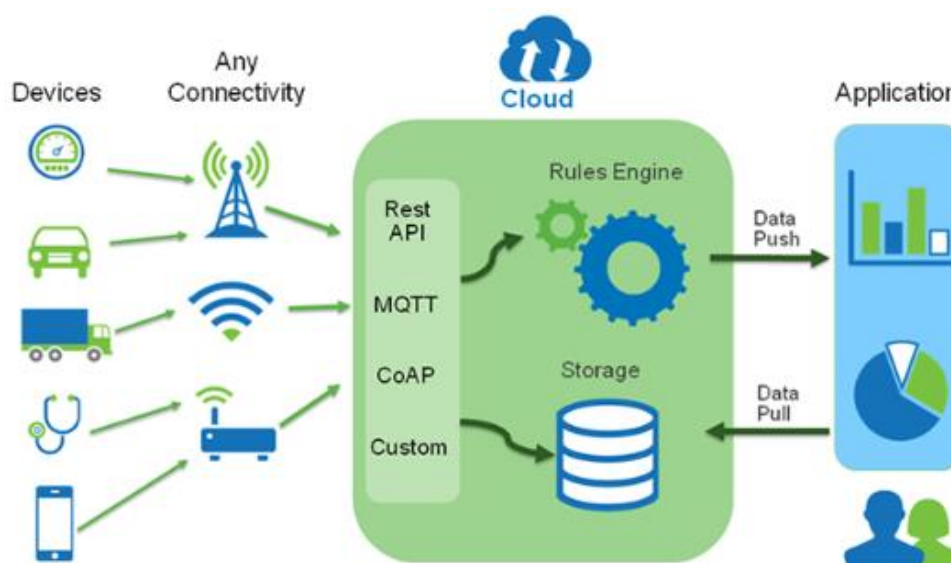


Figure 1. The role of the Cloud in the communication process of smart devices [19]

In an Industry 5.0 smart factory, wireless sensors are deployed across critical zones to monitor equipment and worker safety. [18] The architecture of a wireless sensor networks is shown in Figure 2 that illustrates a generic WSN architecture. Our implementation builds upon this by integrating digital certificate-based authentication and secure data transmission, which are typically not represented in generic models.

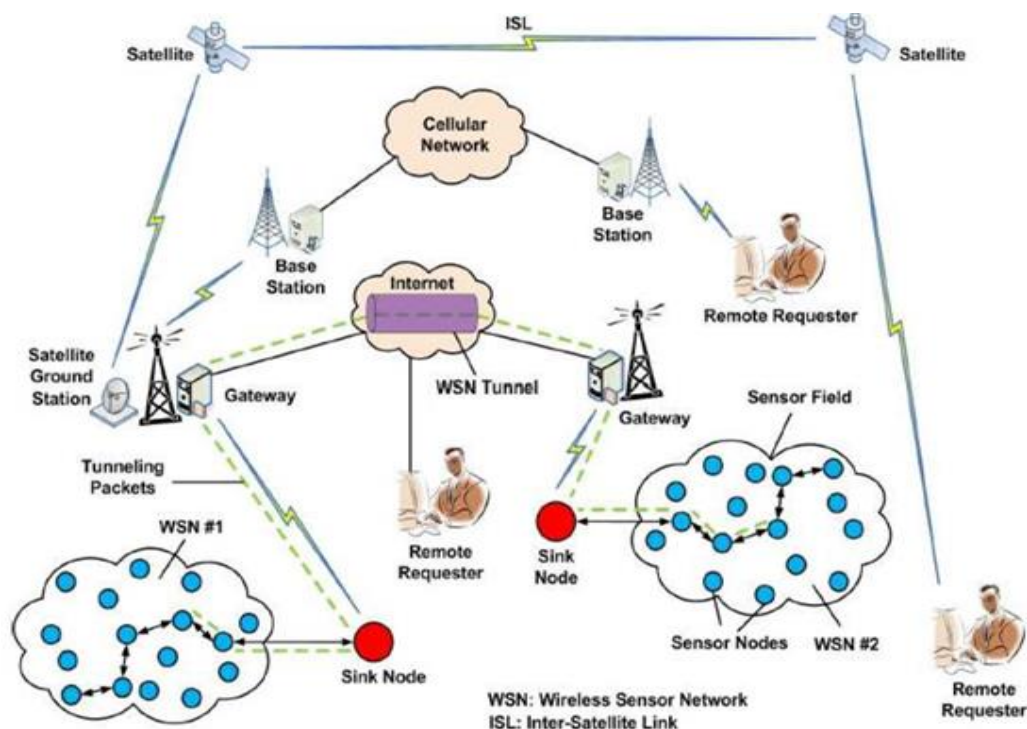


Figure 2. Architecture of a wireless sensor network [10]

Figure 3 illustrates a basic wireless sensor node communication setup using Arduino Nano modules and 433 MHz RF transmission, but lacks robust security features such as encrypted transmission, authentication, or protection against attacks.

Both academia and industry have recognized the potential for such networks and have formed joint efforts to address the engineering challenges. Examples of these academic/industrial initiatives include [15]: UCLA Wireless Integrated Sensor Network (1993), the Pico Radio program at the University of California at Berkeley (1999); the  $\mu$  Adaptive Multi-Domain Power Aware Sensors program at MIT (2000); NASA Sensor Webs (2001); ZigBee Alliance (2002); Center for Embedded Network Sensing (2002).

The goal of many of these initiatives and standardization organizations is to enable high-volume deployment of WSNs in light industrial and consumer applications by reducing cost and energy per sensor while simplifying development and maintenance tasks [15], [22] (Figure 4).

Thus, wireless sensor networks have evolved from experimental concepts to widely implemented technology solutions, being essential in creating intelligent and interconnected systems in various fields [15].

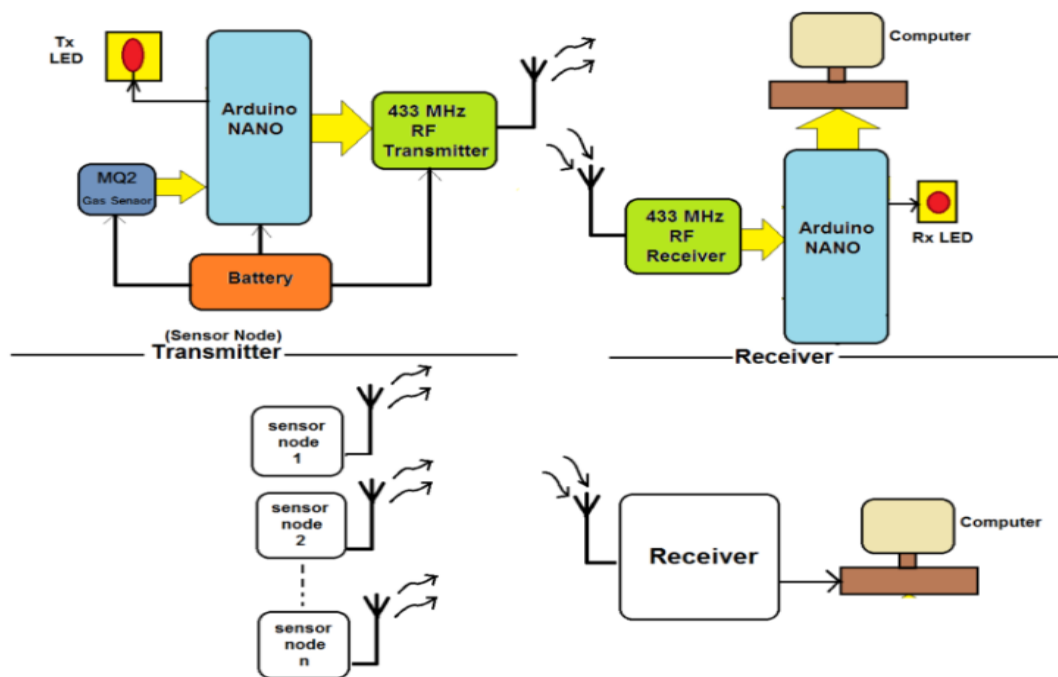


Figure 3. Block diagram of transmitter and receiver type between wireless nodes [11]

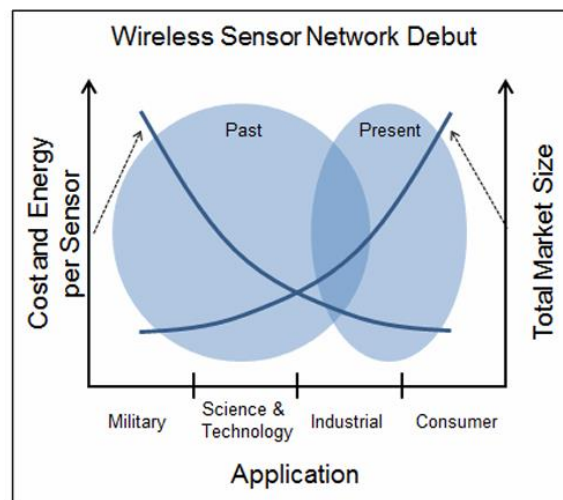


Figure 4. Trends in reducing energy costs per sensor [22], [26]

The number of applications in which wireless communication protocols are used or can be implemented has increased considerably, as methods have been sought to optimize the parameters of the wireless environment: transmission speed, limiting interference between channels, size of transmitted packets, etc. Although the performance of wireless solutions will probably never reach the level of twisted copper, coaxial or optical fiber cables, they represent a viable alternative for medium-distance communications, without creating inconvenience to users [23].

The need for wireless protocols has grown exponentially over the past decade, due to the ability of current technologies to support a large number of sensor-equipped devices capable of communicating over relatively short distances. Although the transmission

speed in wireless networks is generally lower than transmission over copper or fiber optic wires, there are other technical advantages regarding their faster interconnection, without physical paths.

Wireless Sensor Networks (WSNs) are critical components in the oil and gas industry, offering scalable and cost-effective solutions for real-time data acquisition and remote monitoring of assets and environmental parameters in geographically dispersed, hazardous, or inaccessible locations. By leveraging distributed sensing, low-power communication protocols, and edge processing capabilities, WSNs enable early detection of anomalies such as equipment malfunctions, pressure deviations, or gas leaks—thus enhancing operational safety and reducing downtime. These networks support end-to-end visibility and control across all operational phases—upstream exploration, midstream transportation, and downstream processing—while ensuring compliance with stringent environmental and safety regulations. Their modular architecture, autonomous power management (e.g., energy harvesting), and integration with predictive analytics platforms make WSNs a foundational element in the digitalization and Industry 5.0 transformation of the petroleum sector.

By analyzing the relevant literature on the implementation of advanced security in wireless sensor systems, the following Research Questions (RQs) are identified: can a microcontroller implement full PKI-based authentication and encrypted REST communication? what are the trade-offs between RSA and ECC for low-power devices?

The study fills a notable gap in current literature and practical implementations, where many existing solutions either lack lightweight deployment options for resource-constrained devices or fail to integrate a complete end-to-end security framework. By developing a system that combines robust cryptographic techniques, digital certificate-based authentication, and PKI infrastructure, this work provides a holistic and scalable approach to secure sensor data transmission.

The novelty of this study lies in its practical and integrated implementation of an advanced security system using a Raspberry Pi Pico W microcontroller, a temperature, humidity and light sensors, and a secure RestAPI over HTTPS for data communication. Furthermore, the use of a PKI server interfaced with a MySQL database represents a real-world and extensible model that bridges theoretical security principles with IoT-level execution. This solution demonstrates how embedded systems can achieve high security standards without compromising performance, laying the groundwork for more secure, scalable, and resilient WSN deployments.

## **THE IMPORTANCE OF SECURITY IN WSN NETWORKS**

The current state of research in the field of advanced security of wireless sensor networks (WSNs) is in continuous expansion, due to their increasing use in critical applications such as environmental monitoring, healthcare, military security and other sensitive areas. These networks are vulnerable to a wide range of threats due to their wireless nature, limited node resources and exposure to often unsecured or dangerous environments.

Security challenges in wireless sensor networks (WSNs) are varied and complex, due to the specific characteristics of these networks, such as the limited resources of nodes, the

nature of wireless communications, and their use in sensitive or hazardous environments. The main security challenges in sensor networks are detailed below:

- *Limited node resources*: Sensor nodes are devices with limited processing, storage, and power resources, making it difficult to implement traditional security mechanisms. Encryption and authentication protocols, which are essential for protecting data and preventing unauthorized access, can be resource-intensive and can quickly drain node batteries.
- *Wireless communications vulnerability*: Communication over wireless networks is more susceptible to attack because radio signals can be easily intercepted by an attacker in close proximity. This can lead to man-in-the-middle attacks, or the interception and manipulation of data transmitted between nodes.
- *Internal and external attacks*: In addition to external threats, sensor networks also face risks associated with internal attacks. An attacker could compromise a valid node in the network, manipulating it to transmit false data or disrupt the operation of the network. In addition, nodes may be installed in a location that is easily accessible for physical attacks, making them vulnerable to damage or seizure.
- *Scalability and security management*: As the number of nodes in the network increases, security management becomes more complex. It is difficult to implement effective security measures on a large sensor network, given the large number of devices involved and the need to ensure interoperability between them.
- *Authentication and access control*: One of the fundamental aspects of sensor network security is node authentication and access control. Without a robust authentication mechanism, an attacker could introduce fake nodes into the network, thus compromising the entire infrastructure. It is crucial to implement solutions that ensure that only authorized nodes can participate in the network.
- *DoS (Denial of Service) attacks*: In a sensor network, DoS attacks can severely disrupt operations by overloading nodes or the network, preventing data transmission, or denying access to resources. Given the limited resources of nodes, they can quickly become vulnerable to such attacks. [3]
- *Security of transmitted data*: Protecting the data collected and transmitted by nodes is essential. In many applications, the data is sensitive and may include personal information or information critical to the operation of a system. Data encryption is an important security measure, but implementing encryption in a sensor network must be resource-efficient so as not to affect performance and battery life.
- *Physical security of nodes*: In certain environments, sensor nodes may be placed in inaccessible or dangerous locations, which can make it difficult to physically protect them. These nodes may be easily accessible to attackers or may be subject to natural hazards (wind, rain, extreme temperatures), which adds an additional layer of complexity to their protection.
- *Data confidentiality and integrity*: Protecting the confidentiality and integrity of data collected by sensor nodes is a central concern in any wireless sensor network, especially when this data is transmitted over insecure networks. Implementing encryption and digital signature solutions is essential to prevent unauthorized access and modification of data.

The most important types of cyber-attacks on WSNs are:

- *Passive attacks*: interception of transmitted data
- *Active attacks*: modifying, injecting, or redirecting packets
- *Man-in-the-Middle (MITM) attacks* [12]: interception and alteration of communication
- *Replay attacks*: retransmission of captured messages to induce unwanted behaviors
- *Injection and spoofing attacks*: inserting false data or falsifying the identity of nodes

### Energy Cost Comparison of Primitive RSA [23] and ECC Operations

Based on Arvinderpal et al. [2] research, Tables 1, 2 and 3, presents a comparison of the energy consumption [26] associated with different cryptography for signature generation and verification. In Table 3 are presented energy numbers for AES [23] with 128-bit keys (including key-setup) and SHA-1. The numbers were averaged over inputs ranging from 64 to 1024 bytes. [2]

**Table 1.** Energy cost of digital signature computations [2]

| Algorithm | Sign [mJ] | Verify[mJ]          |
|-----------|-----------|---------------------|
| RSA-1024  | 304       | 11.9                |
| ECDSA-160 | 22.82     | 45.09 <sup>3</sup>  |
| RSA-2048  | 2302.7    | 53.7                |
| ECDSA-224 | 61.54     | 121.98 <sup>3</sup> |

**Table 2.** Energy cost of key exchange computations [2]

| Algorithm    | Client [mJ] | Server [mJ] |
|--------------|-------------|-------------|
| RSA-1024     | 15.4        | 304         |
| ECC-160 ECDH | 22.3        | 22.3        |
| RSA-2048     | 57.2        | 2302.7      |
| ECC-224 ECDH | 60.4        | 60.4        |

**Table 3.** Energy numbers for AES [23] with 128-bit keys and SHA-1.

| Algorithm       | Energy                 |
|-----------------|------------------------|
| SHA-1           | 5.9 $\mu$ J/byte       |
| AES-128 Enc/Dec | 1.62/2.49 $\mu$ J/byte |

Although the energy required for RSA [24] signature verification is relatively low, it is outweighed by the much higher cost of the signature generation process. Both operations are necessary for authentication purposes. In contrast, the energy cost of ECDSA2 signatures is substantially lower than that of RSA signatures, while ECDSA verification falls within a reasonable range of RSA verification in terms of energy consumption [2],[14].

It is important to note that when upgrading from RSA-1024 to RSA-2048, the energy required for signing increases by more than a factor of seven. On the other hand, ECDSA-224 signing is less than three times more expensive than ECDSA-160 signing. To provide a clearer perspective, the energy cost of one RSA-1024 signing operation is equivalent to

transmitting 5,132 bytes of data, while a single ECDSA-160 signing operation consumes the energy required to transmit only 385 bytes. For example, the energy required for an RSA-1024 and ECC-160 signature operation is equivalent to encrypting 191kB and 14kB of data with AES-128, respectively [2], [14].

## DESIGN AND SIMULATION OF A WSN SECURITY SYSTEM

The bellow graphical abstract illustrates data flow in implemented WSN security system (Figure 5). As seen in Figure 6, the PKI ecosystem includes not only software and hardware, but also all individuals involved with digital certificates.

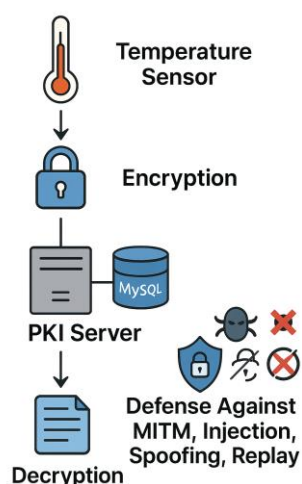


Figure 5. Graphical abstract of implementation

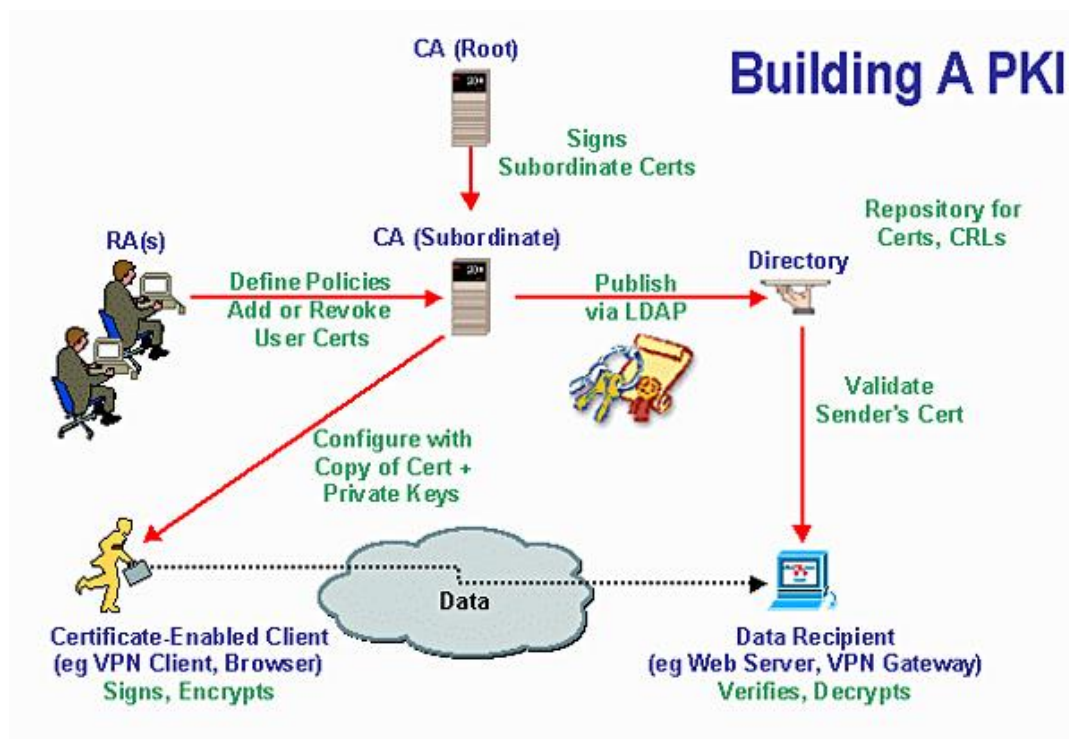


Figure 6. Building a PKI Server [28]

## Public Key Infrastructure (PKI)

The diagram illustrates the Public Key Infrastructure (PKI) process. It features a central 'Request Registration Authority' (represented by a magnifying glass over three people) and a 'CA - Certificate Authority' (represented by a blue document with a gold seal). The CA holds a 'Private key' (represented by a blue key with a gold seal) and issues a 'Public Key' (represented by a blue key with a gold seal). The Sender (represented by a person at a laptop) sends a 'Request' to the CA. The CA responds with 'Request Ok' and 'Request Registration Authority'. The Sender then sends 'Signed Data' (represented by a blue folder) to the Receipt (represented by a blue envelope with a white seal). The Receipt sends a 'Signature' (represented by a blue arrow) back to the CA. The CA sends a 'Signature Ok' (represented by a blue arrow) back to the Sender. The Sender also sends a 'Signature' (represented by a blue arrow) to the Receipt.

```
graph TD
    CA[CA - Certificate Authority]
    Sender[Sender]
    Receipt[Receipt]
    RegAuth[Request Registration Authority]
    PublicKey[Public Key]
    PrivateKey[Private key]
    SignedData[Signed Data]
    Signature[Signature]
    Request[Request]
    RequestOk[Request Ok]
    SignatureOk[Signature Ok]

    CA -- Public Key --> PublicKey
    CA -- Private key --> PrivateKey
    Sender -- Request --> CA
    CA -- Request Ok --> Sender
    Sender -- Request --> RegAuth
    RegAuth -- Request Registration Authority --> Sender
    Sender -- Signed Data --> Receipt
    Receipt -- Signature --> CA
    CA -- Signature Ok --> Sender
    Sender -- Signature --> Receipt
```

Raspberry Pi Pico W

Humidity  
Light  
Temperature  
Sensors

Encryption

Plaintext

Ciphertext

Wi-Fi Router

REST-API

Decryption

MySQL

PKI

PUBLIC KEY INFRASTRUCTURE

MITM REPLY INJECTION

349

To simulate a system like the one presented above in Figure 9, a PKI server was implemented on a laptop using Python code with cryptography mechanisms and digital certificates, respectively protection mechanisms against attacks.

For real-time data transmission, a Raspberry Pi Pico W (RP2040) microcontroller was utilized. The device performs server-side authentication to verify certificate validity and request a JWT token. Upon successful validation, it initiates sensor data acquisition (temperature, humidity, and light), which is subsequently encrypted using custom cryptographic mechanisms developed in MicroPython. The encrypted data is transmitted via the integrated Wi-Fi module over the internet to a PKI-enabled server. This server listens on a predefined port, verifies the authenticity of the JWT token, decrypts the incoming data, and applies security countermeasures—implemented in Python—to mitigate Man-in-the-Middle (MITM), replay, injection, and spoofing attacks. Finally, the processed data is forwarded to a MySQL server via PHP scripts, where it is inserted into the database.

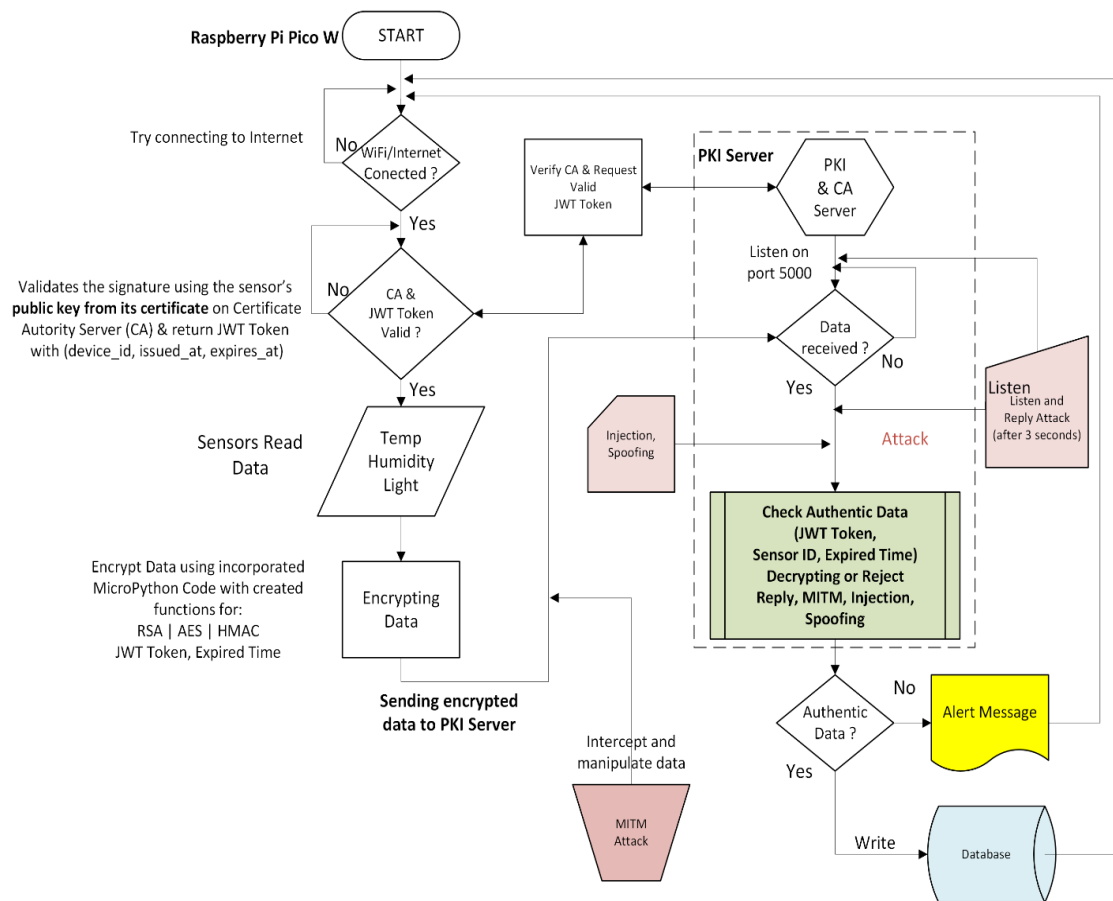


Figure 9. The logic of the data security system

In Figure 9, the following actions of the Raspberry Pi Pico module are highlighted:

- ✓ try connecting to WiFi and Internet;
- ✓ authenticate with public key form its Certificate on Certificate Authority Server (CA) and request JWT Token, containing (device\_id, issued\_at, expires\_at)

- ✓ if is valid, read data from temperature, humidity and light sensors;
- ✓ signs the JWT with the *server's private key & encrypting* data using functions created in Micro Python for AES, RSA, HMAC encoding;
- ✓ sends encrypted sensors data to the PKI server (over HTTPS) through a REST API [16] using the Flask framework in Python to the PKI server that "listens" on a predefined port (the server must have a configured /upload endpoint);
- ✓ Server check data Integrity, JWT Token, Certificate, prevention of Reply, MITM, Injection, Spoofing attacks and decrypt data;
- ✓ insert decrypted data with PHP language into the MySQL database using the mysql.connector library in Python.

Benefits of JWT in WSN:

- Lightweight for resource-constrained nodes,
- Stateless – no session tracking needed,
- Short-lived tokens reduce exposure,
- Can carry roles/permissions in claims.

The authenticity of the digital certificate is verified on the server for each sensor in the network that sends data. To facilitate this, the sensor-specific certificate has been previously inserted into the database as shown in the figure 10.

```

1 INSERT INTO certificates (device_id, certificate, expires_at)
2 VALUES ('sensor_01', '-----BEGIN CERTIFICATE-----\nMIICrjCCAZCYCFD6jmyUzUfer3bpikBsiuWIX/WY+MA0GCSqGSIb3DQEBCwUAMBx
3 ETAPBgNVBAMCE15UetJIEBMB4XDTE1MDIyMjEyMzgwMVoXDTI2MDIyMjEyMzgw
4 MVowFDESMBAGA1UEAwJc2Vuc29yXzAxMIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8A
5 MIIBCgKCAQEAA37xuuKg3/cMDsNyyfRhG76uUWwj6PpG54M9bxF+q8ZpiX2iQWyeF
6 +GHLLi4ddt1MnrpxeKuT6hYuFEL2T12gCYCLbAwTC+XAiMdNp1LuLqkhdeZE78e
7 Cp6KBRD4GquUx/5BA6M0dPCmesar7B7a0buG149kFh1KfFpZVucRtBPKP5E46Qz
8 q5IUi66Uhmik17Egh2mHT18IOqd94/YA0800qL7X/P4CtT9sZGumYdvAsCRHif77
9 DZgwuPISnk5X8KgjARQ1KqPYIRPYcdgrw6/xLFizRab1cuumjPqLoXKwOhwZ9Fr
10 HjmbJeoP7BGCDTw4FNueUXaTyVb5ScsWIIQIDAQABMA0GCSqGSIb3DQEBCwUAA4IB
11 AQAKwenxZr6ZxdORM9kmVef67gbt8jrRwGdYSeLmfSHHKc1YQjZZDZ3++oLm0SmB
12 ty2j8UtyJt6WleznN2gBDEnyQNOLQuw6djH3KISZ2tzSfCurat+Lz0hz1RooPhg5
13 ek3iKYbfK38pCdgqyMakpVNH65x5THE6o8YITHx613g5DuMGnrsKERKtciczZ4AP
14 P2oBX96j81oV/824E7Aem+zkYkwpSZZotYP4q4SyAEZCEAPXwxQbxOUTpr0Z6TW+
15 tbQvcCbHpESGn5UXhau2VbBYdyDz+49fBETWvPzxsW1pYWRsfDBh19tPWnpVbR06
16 kRtWTJD4Zc9NoIjWwIyNZPg\n-----END CERTIFICATE-----',
17     DATE_ADD(NOW(), INTERVAL 1 YEAR));
18

```

Figure 10. Inserted Certificate data for sensor validation into database

To secure communication between the Raspberry Pi Pico and the server, the SSL/TLS protocol was used. [12], [25].

`openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365 -nodes`

This generates two files: **cert.pem** (the SSL certificate) and **key.pem** (the private key). The Flask server will use these files to enable HTTPS.

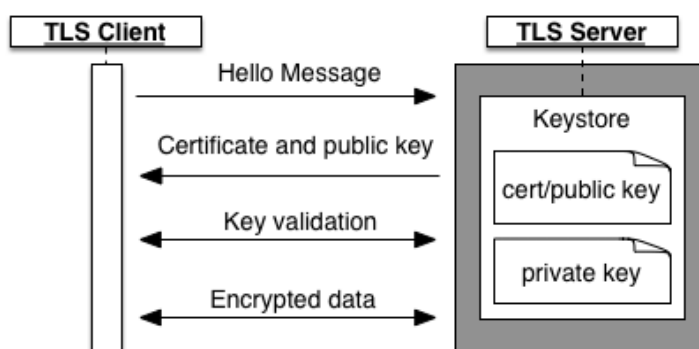


Figure 11. Example of TLS communication between client and server [12]

The endpoint is protected using JWT-based authentication, ensuring that only authorized devices can upload data. Additionally, the request rate is limited to prevent abuse or denial-of-service attacks. Once authenticated, the server extracts the sensor data from the incoming JSON payload and processes it for database insertion via a MySQL connector. This structure enhances both the security and scalability of the WSN.

For testing, the Curl command, available from the Terminal, was used, and it was verified that the RestAPI POST method indeed works correctly:

```

curl -X POST http://localhost:5000/upload ^
-H "Content-Type: application/json" ^
-H "Authorization: Bearer TOKEN_JWT" ^
-d '{"cpu_temp": 25.5, "light": 300, "dht_temp": 24.8, "humidity": 60}'

```

#### Response:

Microsoft Windows [Version 10.0.22631.4751]

(c) Microsoft Corporation. All rights reserved.

C:\Users\emsof>curl -X POST http://localhost:5000/upload ^

More? -H "Content-Type: application/json" ^

More? -H "Authorization: Bearer TOKEN\_JWT" ^

More? -d '{"temp\_cpu": 25.5, "light": 300, "temp\_dht": 24.8, "humidity": 60}'

```

{
  "message": "Data saved",
  "status": "successful"
}

```

The free Thonny integrated development environment (IDE) was used to upload the Python code to the Raspberry Pi Pico W microcontroller. After uploading the code, the microcontroller can run autonomously, being pre-programmed to connect to WiFi, respectively to the internet, request JWT Token from PKI & CA server, read data from sensors, encrypt and retransmit them to the server.

An example of data collected by the Raspberry Pi Pico W and information after processing is shown in Figure 12.



```

Thonny - C:\_@ Master\Lucrare dizertatie\rpi_pico_senzori.py @ 57:5
File Edit View Run Tools Help

rpi_pico_senzori.py
45 # Colectarea datelor
46 def colecteaza_date():
47     lectura_temp = sensor_temp.read_u16() * (3.3 / 65535)
48     temperatura = 27 - (lectura_temp - 0.706) / 0.001721
49     lumina = sensor_lumina.read_u16()
50     sensor_umiditate.measure()
51     temp_dht = sensor_umiditate.temperature()
52     umiditate = sensor_umiditate.humidity()
53
54     return {"temp_cpu": round(temperatura, 2), "lumina": lumina, "temp_dht": temp_dht, "umiditate": umiditate}
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2490
2491
2492
2493
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
2539
2540
2541
2542
2543
2544
2545
2546
2547
2548
2549
2550
2551
2552
2553
2554
2555
2556
2557
2558
2559
2560
2561
2562
2563
2564
2565
2566
2567
2568
2569
2570
2571
2572
2573
2574
2575
2576
2577
2578
2579
2580
2581
2582
2583
2584
2585
2586
2587
2588
2589
2590
2591
2592
2593
2594
2595
2596
2597
2598
2599
2600
2601
2602
2603
2604
2605
2606
2607
2608
2609
2610
2611
2612
2613
2614
2615
2616
2617
2618
2619
2620
2621
2622
2623
2624
2625
2626
2627
2628
2629
2630
2631
2632
2633
2634
2635
2636
2637
2638
263
```

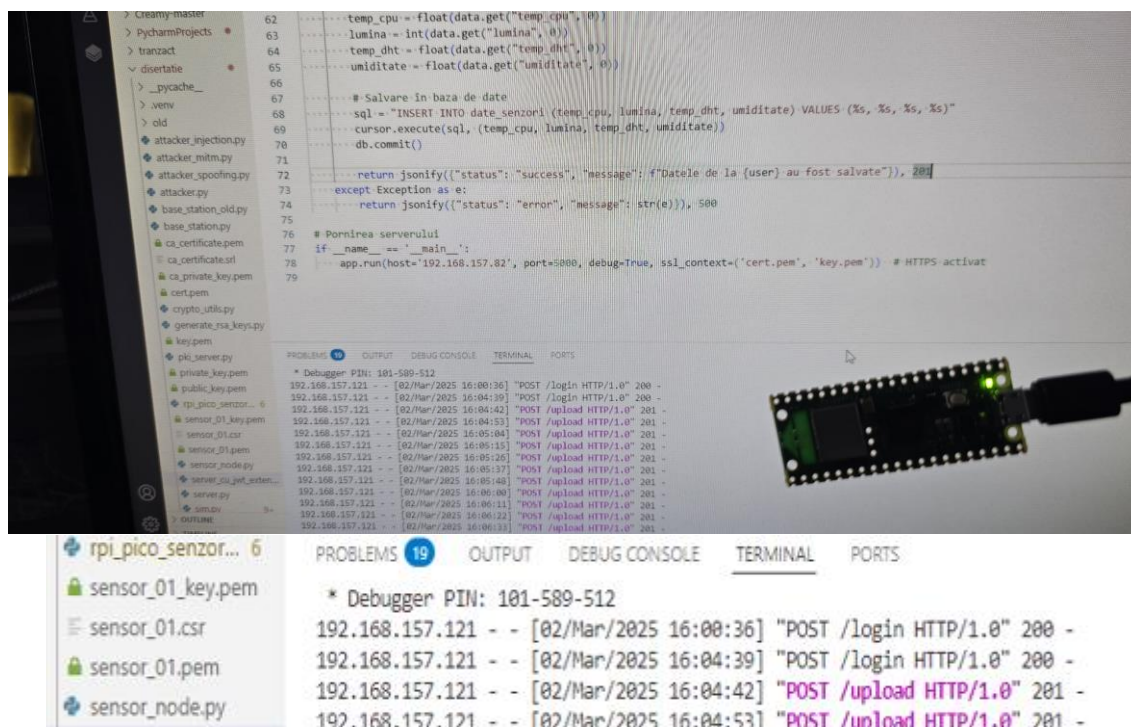


Figure 13. Log capture of operation with sending POST data via API Rest every 5 seconds

Figure 14 shows the display mode of data collected and saved in the database. To view the decrypted data inserted into the MySQL database, a username with a password was also created in the users table, to have the authentication part.

Database Explorer - localhost

emsoftro\_emmhrmg.emsoft.ro

localhost

information\_schema

crud

db\_creamcm

db84318\_art2

dbtranzactionaregc

edgedata

ehr

emil\_disertatie

emil\_disertatie Tables (3)

certificates

date\_senzori

users

Columns

Constraints

Indexes

Triggers

Views

Procedures

Functions

Properties

Start Page

SQL9.sql

SQL8.sql

SQL7.sql

SQL6.sql

SELECT \* FROM emil\_disertatie.date\_senzori;

| id  | temp_cpu | lumina | temp_dht | umiditate | timestamp           |
|-----|----------|--------|----------|-----------|---------------------|
| INT | FLOAT    | INT    | FLOAT    | FLOAT     | TIMESTAMP           |
| 1   | 25,5     | 300    | 24,8     | 60        | 02.03.2025 15:20:17 |
| 2   | 35       | 50     | 30       | 20        | 02.03.2025 16:04:42 |
| 3   | 36,88    | 50     | 30       | 20        | 02.03.2025 16:04:53 |
| 4   | 37,34    | 50     | 30       | 20        | 02.03.2025 16:05:04 |
| 5   | 36,88    | 50     | 30       | 20        | 02.03.2025 16:05:15 |
| 6   | 36,88    | 50     | 30       | 20        | 02.03.2025 16:05:26 |
| 7   | 36,88    | 50     | 30       | 20        | 02.03.2025 16:05:37 |
| 8   | 37,34    | 50     | 30       | 20        | 02.03.2025 16:05:48 |
| 9   | 36,41    | 50     | 30       | 20        | 02.03.2025 16:06:00 |
| 10  | 36,88    | 50     | 30       | 20        | 02.03.2025 16:06:11 |
| 11  | 37,34    | 50     | 30       | 20        | 02.03.2025 16:06:22 |
| 12  | 36,41    | 50     | 30       | 20        | 02.03.2025 16:06:33 |

Figure 14. Example of data collected by Raspberry Pi Pico W and saved in BD

To prevent Man-in-the-Middle (**MITM**) Attack, the system uses asymmetric encryption and digital certificates. Data sent from the sensor node is encrypted with the server's public key, which can only be decrypted by the server's private key. When the server decrypts the message, it also verifies the digital signature or certificate attached to the sender. This ensures that even if an attacker intercepts the transmission, they cannot decrypt or alter the message without the corresponding private key, nor impersonate a trusted entity.

**Injection** attacks are mitigated using message integrity verification techniques like HMAC (Hash-based Message Authentication Code) or digital signatures. After decryption, the system compares a cryptographic hash or signature generated during transmission with the expected one. If the data has been altered – even by a single bit – the hash will not match, and the message is discarded. This prevents attackers from injecting false or malicious data into the system.

To counter **spoofing**, the system relies on identity verification through certificates and secure authentication. Upon decryption, the server checks the certificate or identity token attached to the sender's message. Only nodes registered with the PKI server and holding valid certificates are accepted. If the decrypted data lacks a valid identity or comes from an unrecognized device, it is rejected. This ensures that no unauthorized or impersonated devices can communicate with the server.

**Replay** attacks are prevented through the use of timestamps or nonces (numbers used once) embedded in each message. When the server decrypts a message, it checks whether the timestamp is within an acceptable time window or whether the nonce has been previously used. If the message is outdated or the nonce is reused, the system identifies it as a replayed transmission and drops it. This mechanism ensures that each message is fresh and unique.

An interface was developed using PHP and jQuery AJAX to visualize the data stored in the database, including its evolution over time through graphical representation (Figure 15).

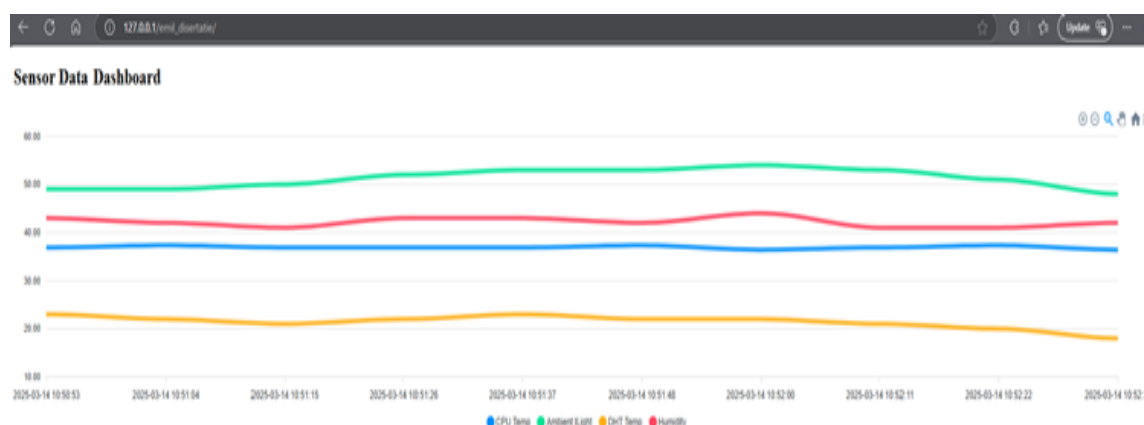


**Figure 15.** Graph with the evolution of inserted data over time (inserted into database in 03/14/2025)

## CONCLUSIONS

The research demonstrates the critical importance of security in Wireless Sensor Networks (WSNs), particularly as these networks become fundamental components in industrial applications, monitoring systems, and autonomous environments. An advanced security system has been successfully designed and implemented to address key vulnerabilities in wireless sensor networks (WSNs).

The system implements multiple layers of protection, including strong cryptographic [10] methods (AES and RSA), digital certificates, and a Public Key Infrastructure (PKI) server. The practical implementation using a Raspberry Pi Pico W microcontroller connected to sensors showcases a real-world application where sensor data is securely transmitted through HTTPS using a REST API [16] with authenticated POST methods.

The main contributions of the paper are: real-world implementation of full-stack secure WSN; custom encryption libraries on Raspberry Pi Pico W; PKI + Certificate Authority (CA) Server + MySQL integration over REST API with decryption functions and attacks prevention logic; dashboard with evolution of received sensors data over time (PHP + JQuery AJAX).

The effectiveness of the proposed system was demonstrated through successful mitigation of common attack vectors, including Man-in-the-Middle (MITM), replay, injection, and spoofing attacks. The solution integrates JWT-based authentication, MySQL database support, and secure communication protocols optimized for execution on resource-constrained devices.

This research contributes significantly to the field by balancing the security requirements of modern IoT ecosystems with the inherent limitations of sensor devices, particularly their processing power, memory, and energy constraints. As WSNs continue to expand in various applications, such security frameworks will be essential for ensuring data integrity, authenticity, and confidentiality in increasingly interconnected systems.

## REFERENCES

- [1] Amin, F., Jahangir, A.H., Rasifard, H., Analysis of Public-Key Cryptography for Wireless Sensor Networks Security, World Academy of Science, Engineering and Technology, International Journal of Computer and Information Engineering, Vol. 2, No.5, 1448-1453, 2008
- [2] Wander S.A., Gura N., Eberle H., Gupta V., Shantz S.C., Energy Analysis of Public-Key Cryptography on Small Wireless Devices, Third IEEE International Conference on Pervasive Computing and Communications, Kauai Island, 8-12 March 2005, pp. 324-328.
- [3] Baydaa et al., New technology for advanced results for security wireless sensor networks, Wasit Journal for Pure Science, Vol. 3, No. 1, p. 83-89, 2024.
- [4] Bucur, G., Moise, A., Popescu, C., Using Ultrasonic Sensors to Develop a Wireless Level Control in Reservoirs with Liquid Chemical Products, Revista de chimie, Vol 70, Nr. 2, 2019.

- 
- [5] Cangea, O., Security Data and Applications in Cloud. Case study, *Romanian Journal of Petroleum & Gas Technology*, vol. 4, no.1, 267-276, 2023.
- [6] Faludi, R., *Building Wireless Sensor Networks*, O'Reilly Publishing, 2011
- [7] Friese, P., Ibanez, F., *Putting the Internet of Things forward to the Next Level – Internet of Things – from Research and Innovation to Market Deployment*, River Publishers Series in Communications, 2014.
- [8] Khaled M.A.H., Mohamed A.M., Sayed A.N., Review of security challenges and solutions in wireless sensor networks, *Journal of Al-Azhar University Engineering Sector*, Vol. 18, No. 69, October 2023, 914-938
- [9] Kalita, H.K., Kar, A., Wireless sensor network security analysis, *International Journal of Next-Generation Networks (IJNGN)*, Vol.1, No.1, December 2009.
- [10] Krit S.A., Jalal, L., Said, H., Design Methodology of Energy Consumption for Wireless Sensor Networks using Renewable Energy, *Journal of Computing*, volume 4, issue 5, May 2012.
- [11] Kumbhar H., Wireless sensor network using Xbee on Arduino Platform: An experimental study, 2016 International Conference on Computing Communication Control and automation (ICCUBE), Pune, India, 2016, pp. 1-5.
- [12] Manesh, T., Signature-Based Wireless Intrusion Detection System Framework, Digital Object Identifier 10.1109/ACCESS.2024.3362803, *IEEE Access*, 2024.
- [13] Modares H., Moravejosharieh, A., et al., Security Overview of Wireless Sensor Network, *Life Science Journal*, 10(2):1627-1632, January 2013
- [14] Nemanja R., Djordje B., Power Consumption Analysis Model in Wireless Sensor Network for Different Topology Protocols and Lightweight Cryptographic Algorithms, Published by Executive Committee, Taiwan Academic Network, Ministry of Education, Taipei, Taiwan, ROC JIT Editorial Office, Office of Library and Information Services, National Dong Hwa University, January 2021
- [15] Orner, R., Grünbacher, E., Guger, C., State of the Art in Sensors, Signals and Signal Processing, in GmbH/Guger Technologies OG, 2009, pp. 9-14.
- [16] Prayogi A.A., Indrabayu N.M., Rijal M., Design and implementation of REST API for academic information system IOP Conf. Series: Materials Science and Engineering vol 875(1) (Bristol: Institute of Physics Publishing), July 2020
- [17] Rosca, C.M., Rădulescu, G., Stancu, A., Artificial Intelligence of Things Infrastructure for Quality Control in Cast Manufacturing Environments Shedding Light on Industry Changes. *Applied Sciences*, 2025, 15, 2068
- [18] Rosca, C.M., Stancu, A., Fusing Machine Learning and AI to Create a Framework for Employee Well-Being in the Era of Industry 5.0. *Applied Sciences*, 2024, 14, 10835.
- [19] Rosca, C.M., Stancu, A., Popescu, M., The Impact of Cloud Versus Local Infrastructure on Automatic IoT-Driven Hydroponic Systems. *Applied Sciences*, 2025, 15, 4016

- 
- [20] Rosca, C.M., Stancu, A., Neculaiu, C.F., Gortoescu, I.A., Designing and Implementing a Public Urban Transport Scheduling System Based on Artificial Intelligence for Smart Cities. *Applied Sciences*, 2024, 14, 8861
- [21] Shereen I., Dawoud, W., Reza H., Securing Wireless Sensor Networks Using Machine Learning and Blockchain: A Review, *Future internet*, 2023
- [22] Shish A., Mohd, R., Qamar A., Energy Saving Secure Framework for Sensor Network using Elliptic Curve Cryptography, *IJCA Special Issue of Mobile Ad-hoc Networks*, 2012.
- [23] Sousi, A.L., Yehya D., Joudi M., AES Encryption: Study & Evaluation, *Cryptography & Network Security Papers*, Rafik Hariri University, November 2020, pp. 3-22.
- [24] Somsuk K., The special algorithm based on RSA cryptography for signing and verifying digital signature, *Heliyon*, Volume 11, Issue 4, 2025, e42481.
- [25] Tiwari S.C., Vijay K.J., An Efficient Signed SSL/Tls-Based Data Security in the Cloud Using Ltt-Ddbm and TECC, Available at SSRN: <https://ssrn.com/abstract=4600314>, December 2023.
- [26] Evolution of Wireless sensor networks [silabs.com]
- [27] SignMyCode, Code Signing with Public Key Infrastructure (PKI), August 2023 [GoogleResearch]
- [28] Public Key Infrastructure (PKI) [GoogleResearch]
- [29] The difference between Encryption, Hashing and Salting [GoogleResearch]

---

Received: April 2025; Revised: June 2025; Accepted: June 2025; Published: June 2025