ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb1166

Performance Analysis and Integration of Homomorphic Encryption in Critical Computer Transport Network/its Infrastructures

Ayila Mopaya Ben[1]; Lovwa Mulelenu Olivier[2]; Nkwahata Masangata Leprince3; Bobozo Bikayi Louis-Michel[4]; Luntala Bakika Benedite[5]; Ekof'amboyo Basambi Toussaint[6] ; Buanga Mapetu Jean-Pepé

Publication Date: 2026/02/28

Abstract : Homomorphic encryption (HE) represents a significant advancement in the field of cybersecurity due to its ability to perform operations on encrypted data without requiring prior decryption. This property offers particularly promising prospects for the protection of critical infrastructures, where the confidentiality of information and continuity of services are of paramount importance. Computer transport networks, which ensure the secure transmission of data across sensitive sectors such as railways, aviation, energy, or road transport, are increasingly exposed to sophisticated cyber threats. In this context, the integration of homomorphic encryption emerges as a relevant approach capable of enhancing data protection while preserving operational usability, particularly in environments that require near real-time processing.

Furthermore, critical road infrastructures are increasingly based on interconnected computing architectures designed to manage traffic, intelligent signaling, sensor data collection, and assistance for automated driving systems. While this digital transformation improves efficiency and safety, it simultaneously increases the attack surface, including risks of malicious intrusions, data tampering, and breaches of confidentiality. In this framework, homomorphic encryption (HE) stands out as a promising solution, enabling analytical processing of data while maintaining it in an encrypted state. This work focuses on evaluating the impact of HE on the security, performance, and resilience of road computer networks considered as critical infrastructures.

Following a thorough review of the scientific literature on various homomorphic encryption approaches and recent implementations, an evaluation methodology was developed considering multiple technical environments. This methodology relies on the use of specialized libraries such as Microsoft SEAL, PALISADE, Concrete, and Lattigo, integrated within Intelligent Transportation Systems (ITS) architectures, both in simulated and near-real conditions. The results highlight a significant improvement in data confidentiality and integrity through HE usage, while also pointing out operational constraints related to increased latency and computational load. Consequently, recommendations are proposed to optimize the integration of this technology in environments where response time requirements are critical, notably through the use of hardware accelerators and hybrid approaches combining homomorphic encryption with other cryptographic mechanisms.

How to Cite: Ayila Mopaya Ben; Lovwa Mulelenu Olivier; Nkwahata Masangata Leprince; Bobozo Bikayi Louis-Michel; Luntala Bakika Benedite; Ekof'amboyo Basambi Toussaint (2026) Performance Analysis and Integration of Homomorphic Encryption in Critical Computer Transport Network/its Infrastructures. *International Journal of Innovative Science and Research Technology*, 11(2), 2000-2012. https://doi.org/10.38124/ijisrt/26feb1166

I. INTRODUCTION

A. General Context

The protection of critical infrastructures is today a strategic priority for states, industrial organizations, and society as a whole. These infrastructures include energy production and distribution networks, industrial control systems such as SCADA, railway, air, maritime, and road transport networks, as well as financial and communication systems. In these digitally dependent environments, service availability, information integrity, and data confidentiality are fundamental requirements to ensure operational continuity and user safety [1], [2].

Computer transport networks play a central role in this context, as they ensure the flow of operational data and supervisory information between different components of a critical system. Their operation relies on communications that must be fast, reliable, and resilient against cyber threats. However, the steadily increasing volume of exchanged data, coupled with the complexity of digital architectures and evolving attack techniques, exposes limitations in conventional security mechanisms [3]. Although these

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb1166

mechanisms effectively protect data in transit or at rest, they can exhibit vulnerabilities during processing phases when information must be temporarily accessible in plaintext.

In this perspective, homomorphic encryption (HE) emerges as a particularly promising innovation. Unlike traditional cryptographic approaches that require decryption before exploitation, HE allows mathematical operations, such as addition, multiplication, or more complex computations depending on the scheme used, to be performed directly on encrypted data. The resulting output, once decrypted, matches what would have been obtained from the plaintext data, thus preserving information confidentiality throughout the processing [4].

B. Intelligent Road Transport Context

Modern road transport is undergoing profound transformation, characterized by increasing interconnection among vehicles, physical infrastructures, and supervision centers, enabled by Intelligent Transportation Systems (ITS) technologies [5]. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications, combined with centralized management platforms and advanced data analytics, contribute to dynamic traffic optimization, accident risk reduction, and overall improvement of road user experience [6].

However, this shift toward highly digital environments significantly increases the cyber exposure surface. System interconnectivity, the proliferation of access points, and continuous transmission of sensitive data heighten potential vulnerabilities that could compromise service availability, information integrity, and data confidentiality [7].

C. Importance and Vulnerabilities of Critical Infrastructures

The relevance of homomorphic encryption in critical infrastructure contexts lies primarily in its ability to enhance data security throughout its lifecycle, including processing phases [8]. Unlike traditional cryptographic approaches, information remains encrypted even during manipulation, significantly reducing the attack surface and limiting the risk of interception or exploitation by malicious actors.

Furthermore, this property facilitates the implementation of secure distributed processing, as certain operations can be delegated to remote servers or cloud environments, even when full trust cannot be assumed. More broadly, homomorphic encryption contributes to the resilience of systems against threats such as industrial espionage, cyber sabotage, or data injection attacks in control mechanisms.

For instance, in a railway network, signaling sensors and supervision platforms continuously transmit highly sensitive information, such as train positions, speeds, or switch statuses. Homomorphic encryption would allow the processing of this data to optimize traffic management, detect anomalies, or anticipate potential failures, while preventing plaintext exposure to unauthorized entities [9].

Road computer networks should likewise be considered critical infrastructures, as their malfunction can lead to significant economic, environmental, and human consequences. Potential threats include interception or manipulation of traffic data, sabotage of signaling devices, or misuse of personal information collected by urban sensors [10]. Conventional encryption mechanisms, such as AES or RSA, effectively protect data in storage or transmission but generally require decryption before processing, introducing transient phases during which information may be exposed to potential attacks [11].

D. Problem Statement and Motivation

Homomorphic encryption (HE) represents a major advance in cryptography, as it allows mathematical operations directly on encrypted data without decryption [12]. This capability is particularly important in transport environments, where multiple actors — operators, public authorities, and service providers — must handle sensitive information while preserving confidentiality. For example, HE enables the calculation of optimal routes, detection of traffic incidents, or estimation of toll waiting times without ever accessing plaintext data [4].

➢ *Despite its Advantages, HE Faces Technical Limitations:*

- It requires significantly higher computation time compared to traditional symmetric or asymmetric encryption methods.
- It incurs bandwidth overhead due to the larger size of encrypted data.
- Its integration into existing protocols of critical networks is complex and requires specific adjustments.

Thus, the central question of this study can be formulated as follows:

How can homomorphic encryption be effectively integrated into a critical computer transport network infrastructure to enhance data security while minimizing its impact on operational performance?

E. Objectives and Scope of the Study

➢ *This Paper Aims to:*

- Present the state of the art of HE techniques applicable to road networks.
- Evaluate the impact of HE on security, performance, and quality of service in critical road infrastructures.
- Identify constraints and optimization levers for large-scale integration.

The scope of this study is limited to intelligent road networks in urban and interurban contexts, including V2X (vehicle-to-everything) communication and centralized management systems [13].

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb1166

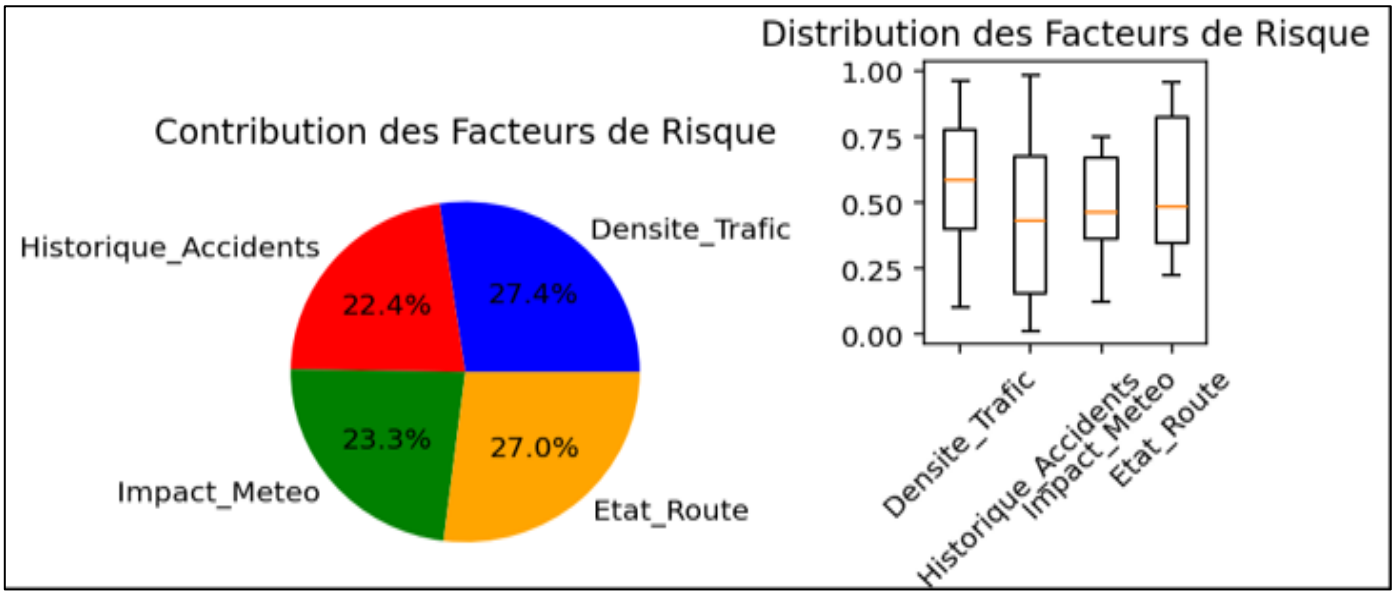

Fig 1 Risk State

II. STATE OF THE ART AND LITERATURE REVIEW

A. *Critical Road Infrastructures and Associated Computer Networks*

Critical Road Infrastructures encompass all systems and services whose proper functioning is essential for the safety and smooth flow of traffic.

➢ *They Include [14]:*

- Traffic management systems: intelligent traffic lights, dynamic speed regulation, dedicated lanes.
- Perception and detection systems: road sensors, cameras, radars, LIDAR.
- Communication networks: fiber optics, 4G/5G, ITS-G5, DSRC.
- Supervision and control centers: real-time monitoring platforms, dispatching of response units.
- Toll and ticketing systems: automated collection and payment processing.

These infrastructures rely on distributed computer networks, combining local processing nodes (edge computing) and centralized data centers (cloud). Their main vulnerabilities arise from the heterogeneity of equipment, the multiplicity of access points, and their interconnection with public networks, which significantly increase the attack surface. According to the European Union Agency for Cybersecurity (ENISA, 2023), more than 60% of security incidents within Intelligent Transportation Systems (ITS) are attributable to Man-in-the-Middle (MITM) attacks, Denial of Service (DoS), or leakage of sensitive data during plaintext processing [15].

B. *Principles of Homomorphic Encryption*

Homomorphic Encryption (HE) is a cryptographic paradigm that allows operations (addition, multiplication, or complex functions) to be performed directly on encrypted data. The results of these operations, once decrypted, are identical to those obtained when working on plaintext data [16].

➢ *CKKS Encryption*

- *Encryption Formula:*

$$c=(m+e+p\cdot r)\bmod qc = (m + e + p \cdot r) \mod qc=(m+e+p\cdot r)\bmod q$$

Where:

✓ mmm = message (polynomial)
✓ eee = error/noise
✓ ppp = public key
✓ rrr = random polynomial
✓ qqq = modulus

- *Decryption Formula:*

$$m\approx(c\cdot s)\bmod qm \approx (c \cdot s) \mod qm\approx(c\cdot s)\bmod q$$

Where sss is the secret key.

➢ *Homomorphic operations:*

- Addition: $E(m1)+E(m2)=E(m1+m2)E(m_1) + E(m_2) = E(m_1 + m_2)E(m1)+E(m2)=E(m1+m2)$
- Multiplication: $E(m1)\cdot E(m2)=E(m1\cdot m2)+\text{additional noise}E(m_1) \cdot E(m_2) = E(m_1 \cdot m_2) + \text{additional noise}E(m1)\cdot E(m2)=E(m1\cdot m2)+\text{additional noise}$

➢ *Types Of HE:*

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb1166

Table 1 Types of HE

Type of HE	Description	Example Algorithms	Road Applications
Partially Homomorphic (PHE)	Supports only one operation (addition or multiplication) on encrypted data	RSA (multiplication), Paillier (addition)	Secure vehicle counting, traffic statistics
Somewhat Homomorphic (SHE)	Supports a limited number of mixed operations	BGN, YASHE	Basic toll calculations on encrypted data
Fully Homomorphic (FHE)	Supports unlimited mixed operations	BGV, BFV, CKKS, TFHE	Predictive traffic analysis, secure video processing

Modern FHE schemes such as BFV (Brakerski/Fan-Vercauteren) and CKKS (Cheon-Kim-Kim-Song) are particularly suitable for road data processing, as they allow operations on encrypted vectors containing real or integer numerical data [14].

C. Applications of HE in Intelligent Transportation Systems (ITS)

Recent studies highlight the potential of HE in road transport:

- *Thomas Hiscock (CEA-LETI):*

Demonstrated integration of HE into embedded processors, enabling secure evaluation of critical data without information leakage.

- *Reda Bellafqira (2017):*

Developed a solution combining the additive Paillier HE scheme with QIM watermarking for secure outsourced medical image processing, highlighting the need for integrity verification of encrypted data.

- *Cyrielle Feron (Nov. 2018):*

Developed PAnTHErS, a tool for rapid analysis of HE schemes in terms of algorithmic complexity and memory cost, while noting issues like unstable scheme security, high memory usage, and suboptimal error management.

- *Donald Nokam Kuaté (2019):*

Proposed a video/image transcoder operating on fully encrypted content, ensuring user privacy, though converting from polynomial to vector structures reduced performance by preventing use of traditional accelerators (CRT, polynomial Fourier transforms).

- *Amina Bel Korchi (2021):*

Applied HE to industrial IoT use cases, enabling encrypted cloud alerts; however, comparison of encrypted data remained challenging, preventing conditional branching or alert triggering.

- *Mammeri Ilhem Guerriche Nor El Houda (2017):*

Discussed vehicular cloud computing, outsourcing computations on confidential data to cloud servers while retaining decryption keys; limitations included processing time and key size.

- *Asma Mkhinin (Dec. 2017):*

Proposed high-level synthesis for hardware acceleration of HE primitives (polynomial multiplication, discrete Gaussian sampling), enhancing performance while noting limitations related to approximate computation and noise management.

- *Cédric Lefebvre (Dec. 2021):*

Applied HE to genomic privacy, enabling secure querying of mutations; main limitation was bandwidth and computation cost for larger datasets.

- *Key Observations:*

- HE significantly enhances data confidentiality and integrity.
- Adoption is limited by computational load and bandwidth, particularly in embedded devices.

D. Tools and Libraries for FHE in Road Context

Several open-source or commercial libraries provide optimized implementations [4], [18]:

Table 2 Tools and Libraries for FHE

Library	Supported Types	Languages	Strengths	Limitations
Microsoft SEAL	BFV, CKKS	C++, .NET, Python	Extensive documentation, multi-thread support, stable	High memory consumption for large vectors
PALISADE	BFV, CKKS, FHEW, BGV	C++	Algorithm support, interoperability	Steep learning curve
Concrete	TFHE	Rust	Ideal for embedded logic computations	Less suitable for large numerical vectors
Lattigo	BFV, CKKS	Go	Easy cloud integration	Lower performance on limited hardware

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb1166

III. METHODOLOGY AND TECHNICAL ENVIRONMENT

A. General Approach

This study aims to evaluate the impact of HE integration on security, performance, and quality of service in critical road network infrastructures.

➢ *Our Approach Involves Three Steps:*

- Modeling an intelligent road network architecture integrating sensors, onboard units, and control centers.
- Integrating HE libraries across network segments (edge, cloud, embedded).
- Measuring impact in terms of latency, bandwidth, energy consumption, and security level.

B. Typical Intelligent Road Network Architecture

➢ *The Architecture is Inspired by Modern ITS Deployments and Includes [19], [5]:*

- Field sensors and road IoT devices: inductive loops, cameras, radars, LIDAR, weather stations, smart traffic lights.
- Onboard Units (OBU) in connected vehicles: V2V/V2I communication via ITS-G5 and 5G-V2X, ADAS systems, Vehicle-to-Cloud (V2C) communication.
- Roadside Units (RSU): local relays for data aggregation and pre-processing, edge servers.
- Supervision center and cloud: control platforms, predictive analytics, Big Data processing, interfaces with authorities.
- Edge computing nodes: deployed at bus stations, intersections, and 5G sites to reduce latency.

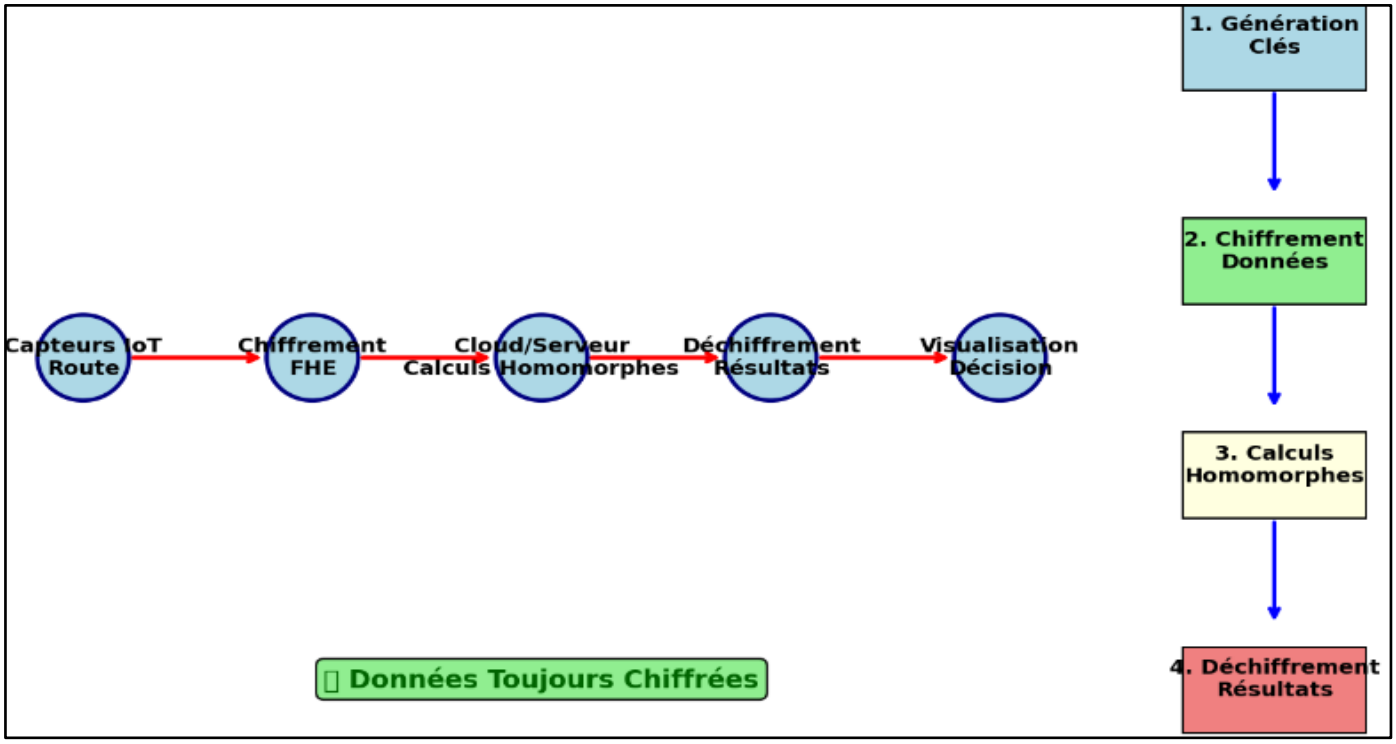

Fig 2 Intelligent Road Network Architecture

C. Software Tools and Libraries Used

Table 3 Software Tools and Libraries Used

Tool	Type	Role in the Study
Microsoft SEAL	HE Library (BFV, CKKS)	Computations on real and integer data for Scenarios 2 and 3
PALISADE	HE Library (BFV, FHEW)	Performance evaluation on mixed data streams (integers + booleans)
PYTHON (SPYDER)	Programming Environment	Encryption/decryption of data and data visualization
Wireshark	Network Analysis	Bandwidth measurement

➢ *Each Tool was Selected Based on [5]:*

- The nature of the processed data (integers, floating-point, booleans).
- Latency and bandwidth constraints.
- Compatibility with edge/cloud integration.

D. Evaluation Metrics

➢ *The Assessment of the Impact of HE is Based on Several Metrics:*

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb1166

- Processing Latency (ms): the additional time introduced by homomorphic operations.

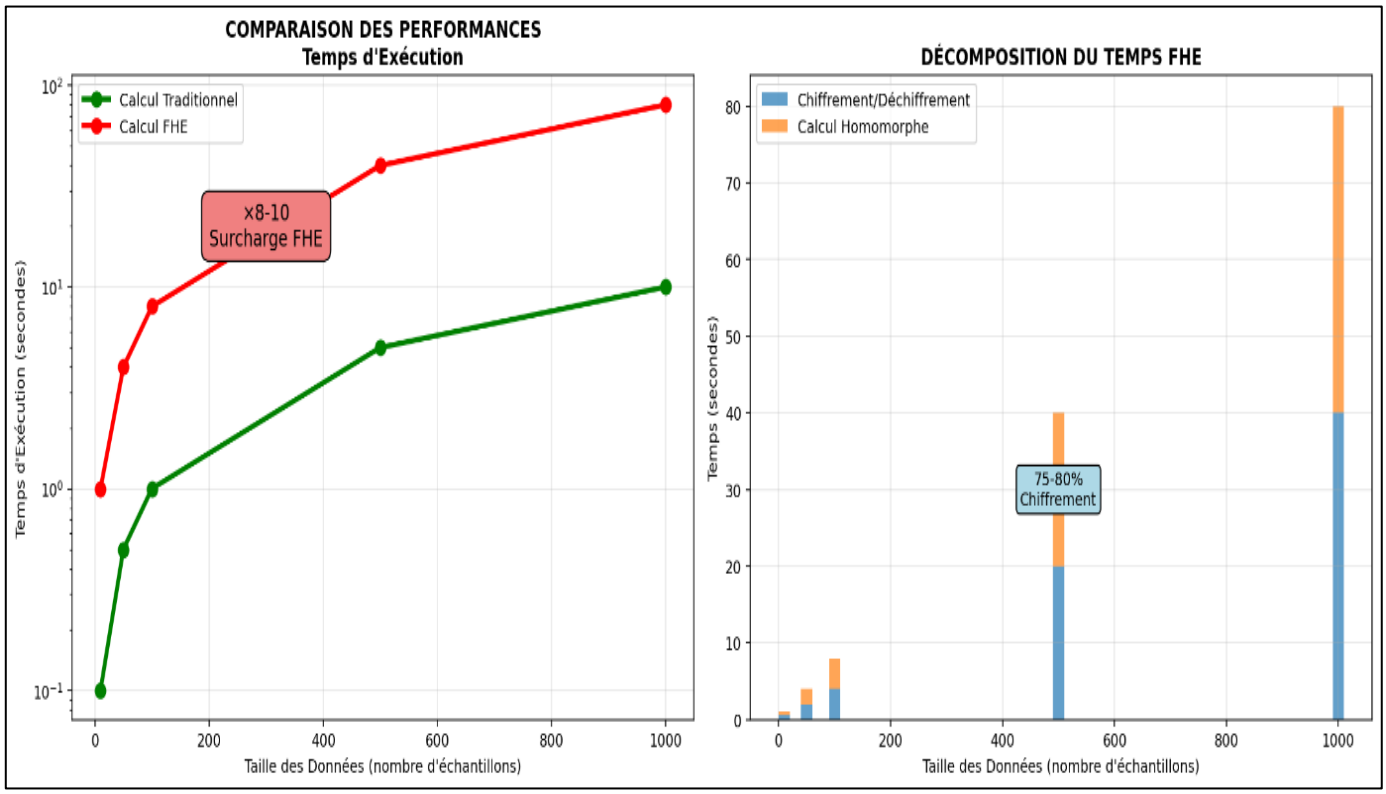

Fig 3 Processing Latency

- Bandwidth Consumption (KB/s): increase caused by the larger size of encrypted data.

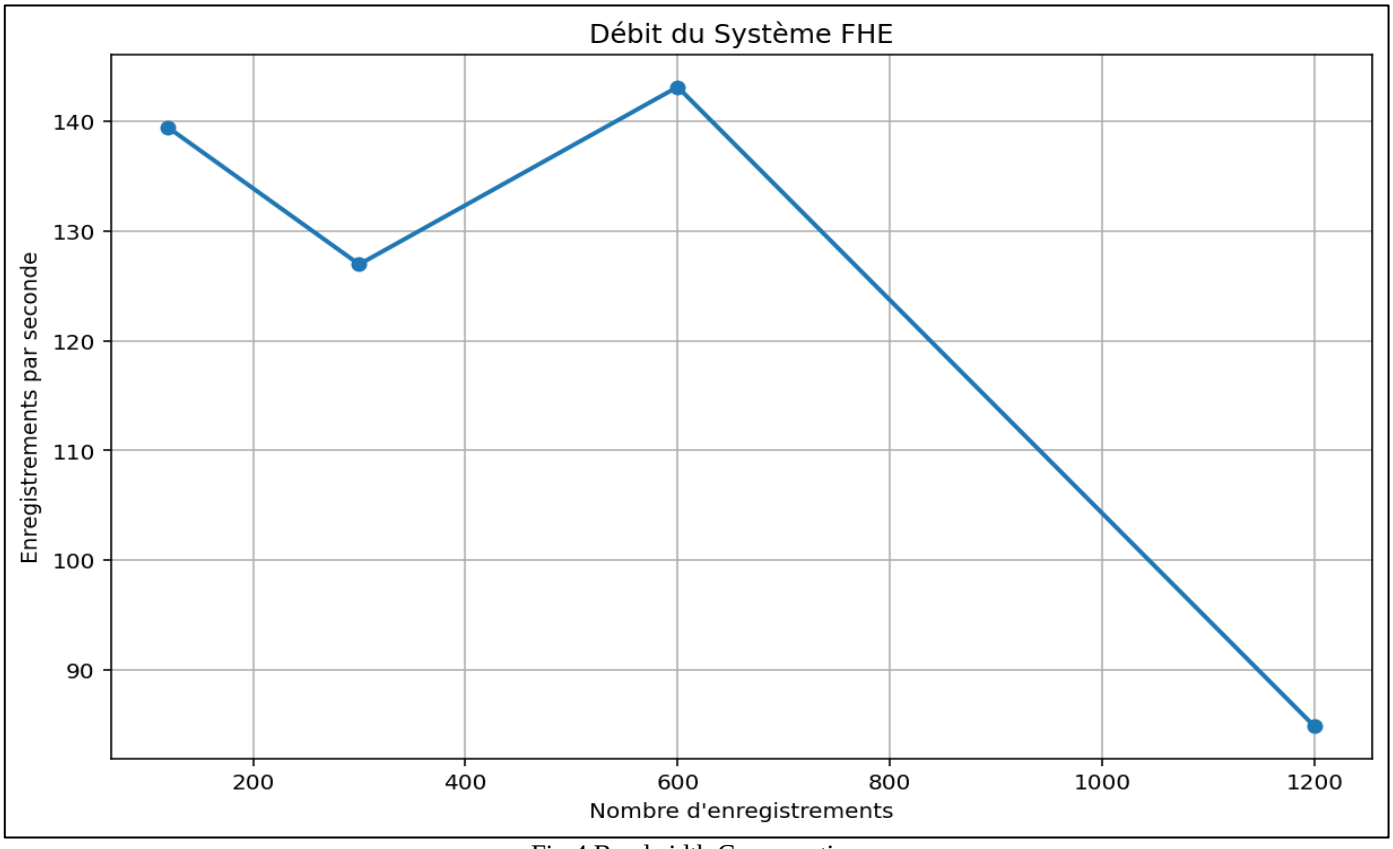

Fig 4 Bandwidth Consumption

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb1166

- Cryptographic Robustness: resistance to known attacks (noise analysis, side-channel attacks).

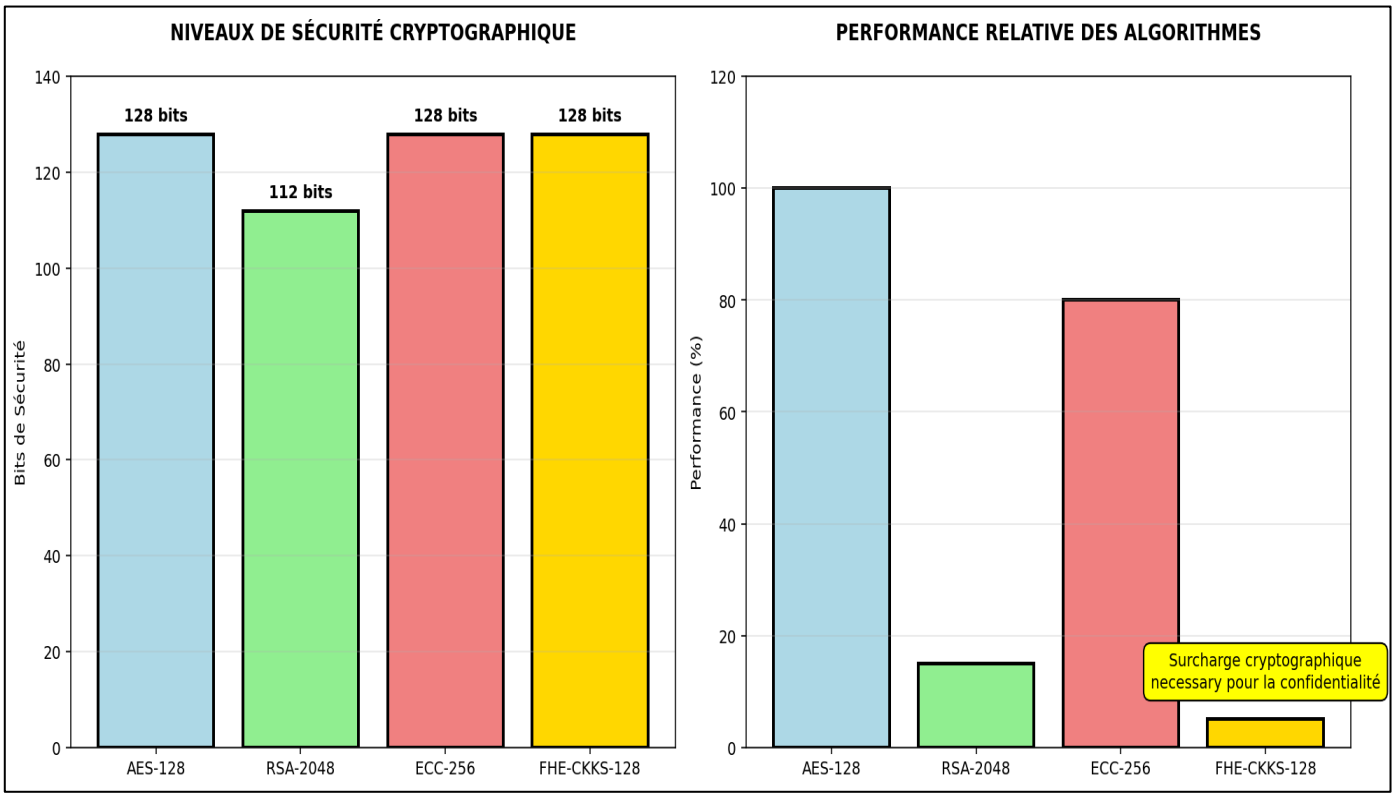

Fig 5 HE Robustness

- Quality of Service (QoS): tolerable communication delay in ITS applications.

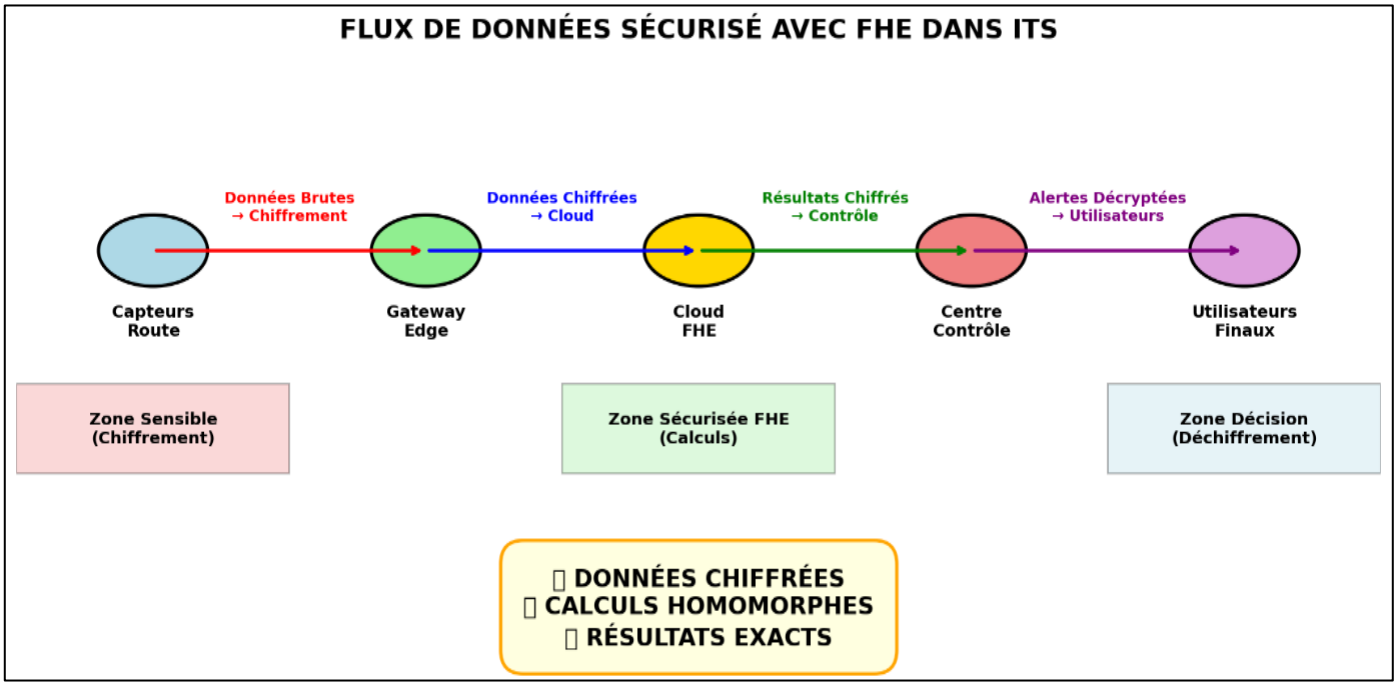

Fig 6 Quality of Service

These indicators allow for a comparison of homomorphic encryption (HE) with classical methods (AES, RSA) to determine the conditions under which its use is viable [10].

IV. RESULTS AND ANALYSIS

A. General Impact of Homomorphic Encryption

Integration tests of Fully Homomorphic Encryption (FHE) — particularly using the CKKS scheme via Microsoft

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb1166

SEAL — in road ITS/IoT environments demonstrate its ability to securely process sensitive data (speed, traffic density, alerts). Calculations of risk indices and adjusted traffic flows were successfully performed on encrypted data [20].

Table 4 Risk Scores

Segment	Timestamp	...	Braking Alert	Risk_Score
0	2025-08-30 01:09:20.443934	...	0	0.369443
1	2025-08-30 00:09:20.443934	...	0	0.625201
2	2025-08-29 23:09:20.443934	...	0	0.441913
3	2025-08-29 22:09:20.443934	...	0	0.278362
4	2025-08-29 21:09:20.443934	...	0	0.148785

➢ *Cryptographic Scheme*

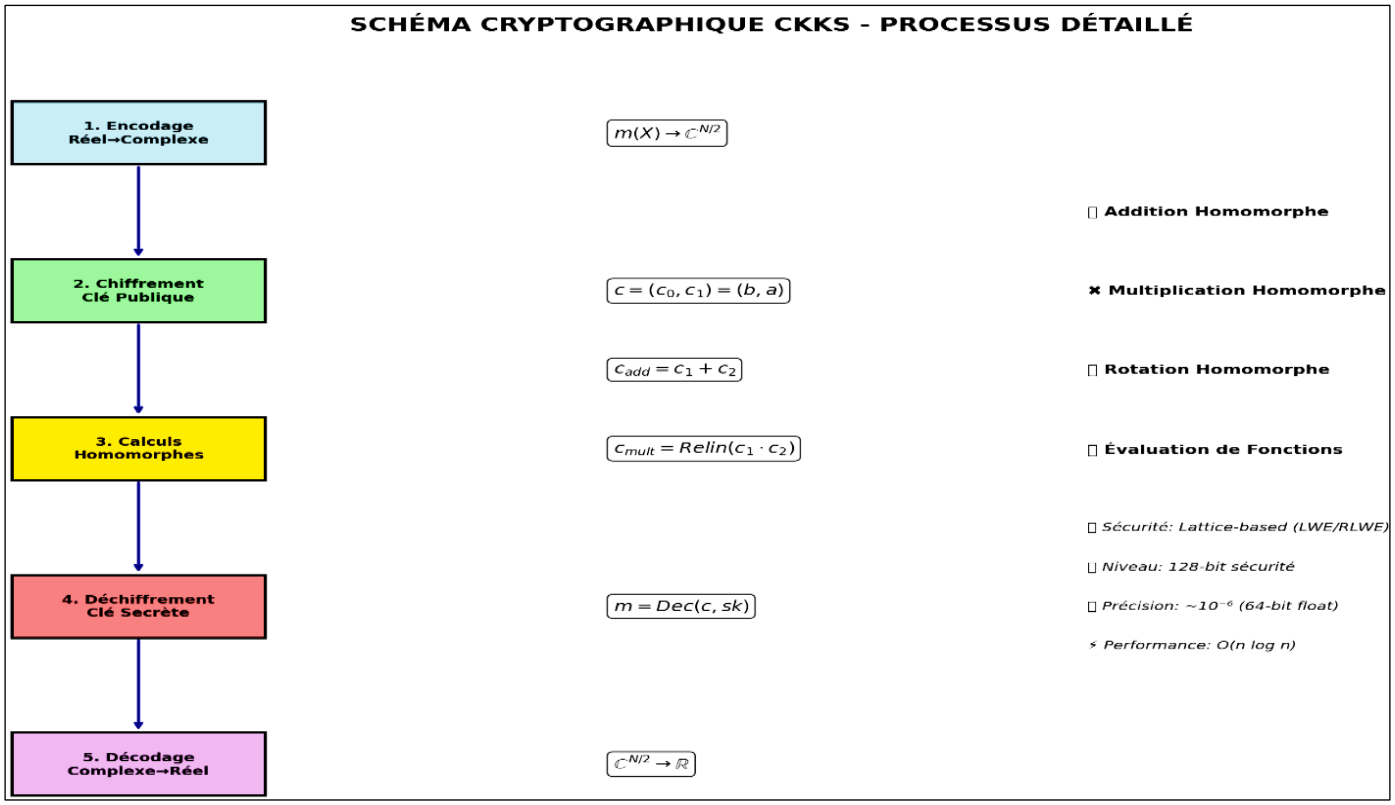

Fig 7 Global Road Safety Index

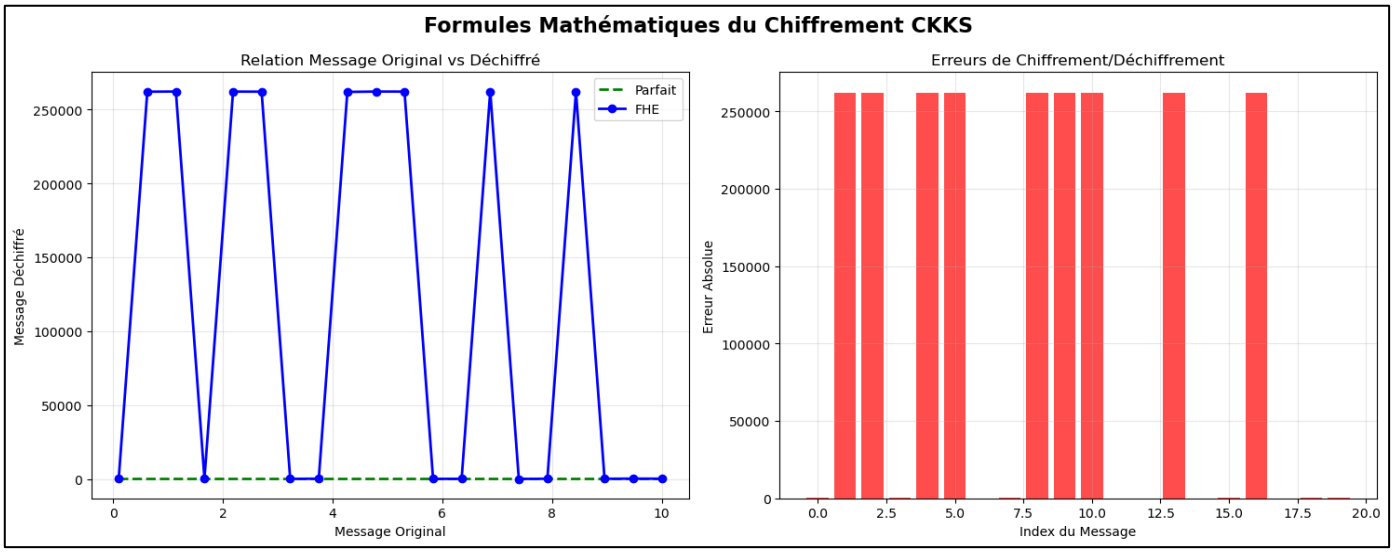

Fig 8 formule math du chiffrement CKKS

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb1166

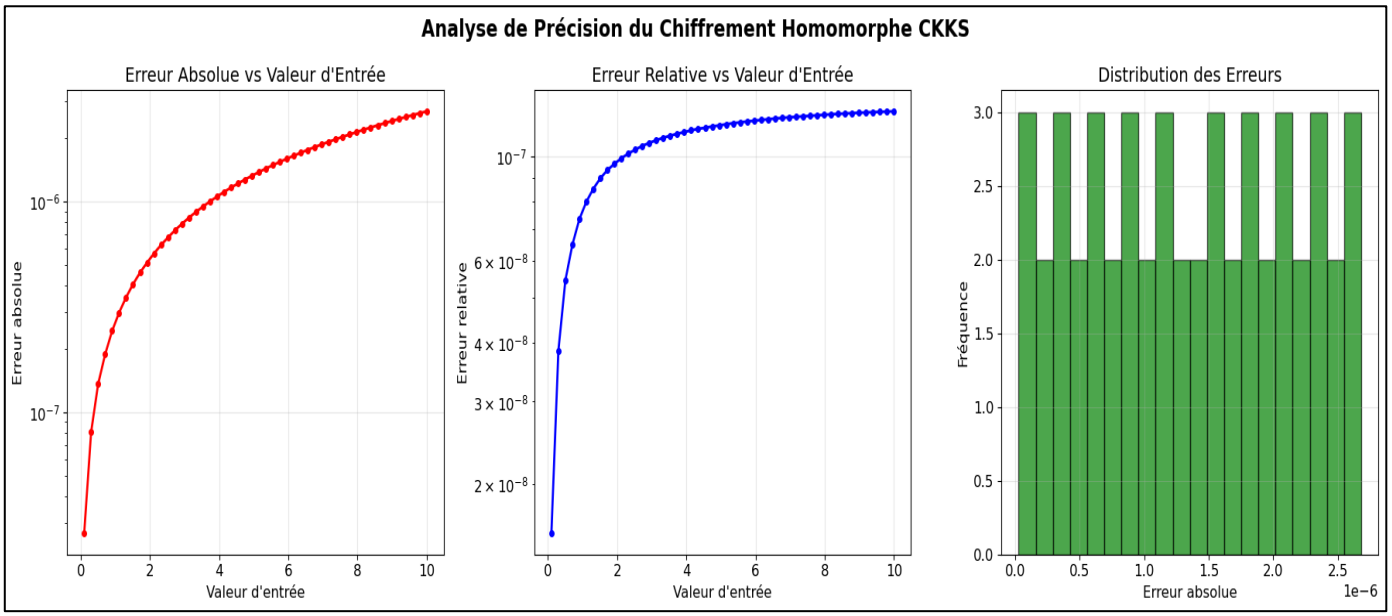

Fig 9 Precision Analysis of HE CKKS

➢ *Processus De Chiffrement Homomorphe Complet(FHE)*

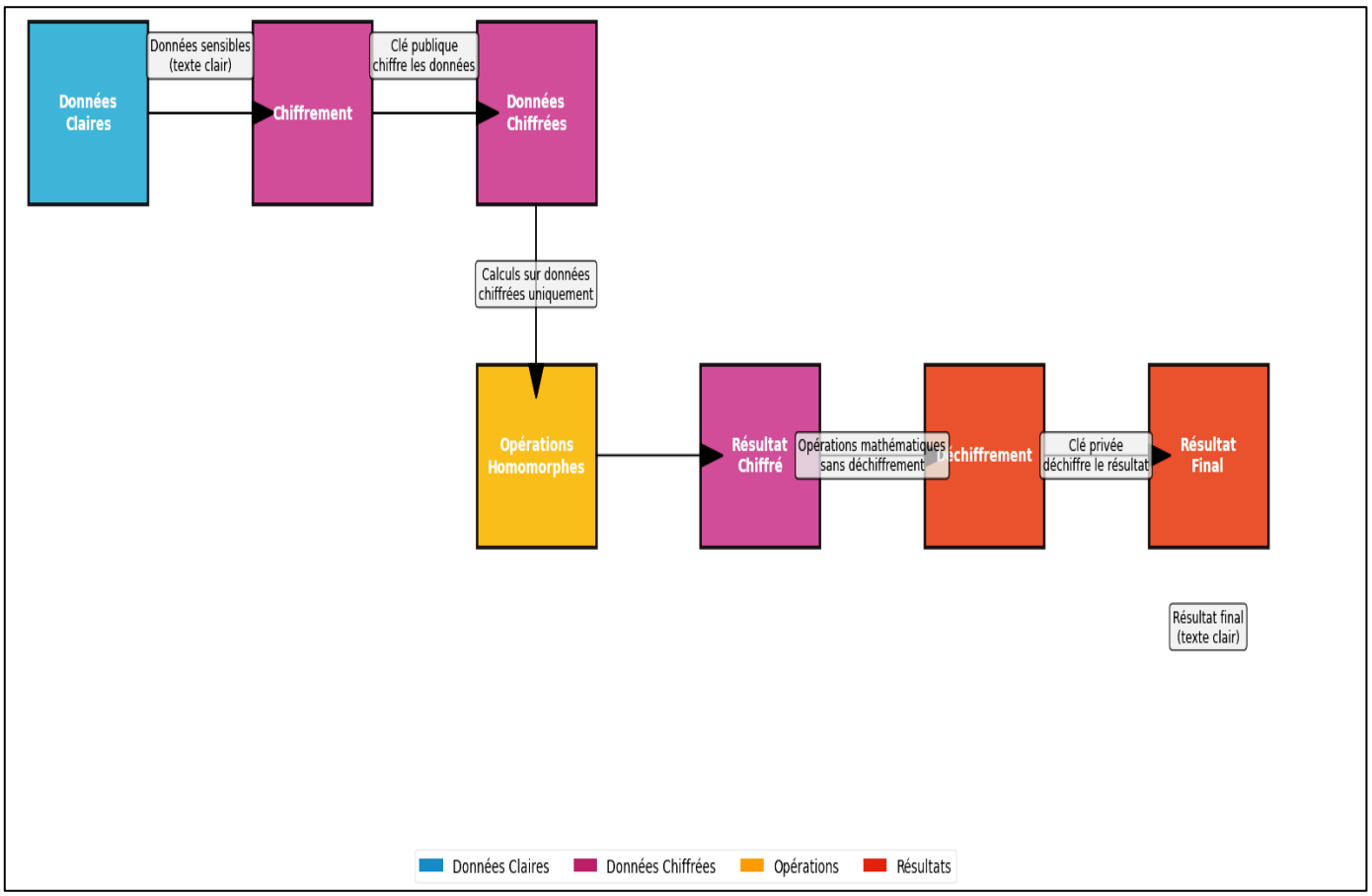

Fig 10 Processus of FHE

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb1166

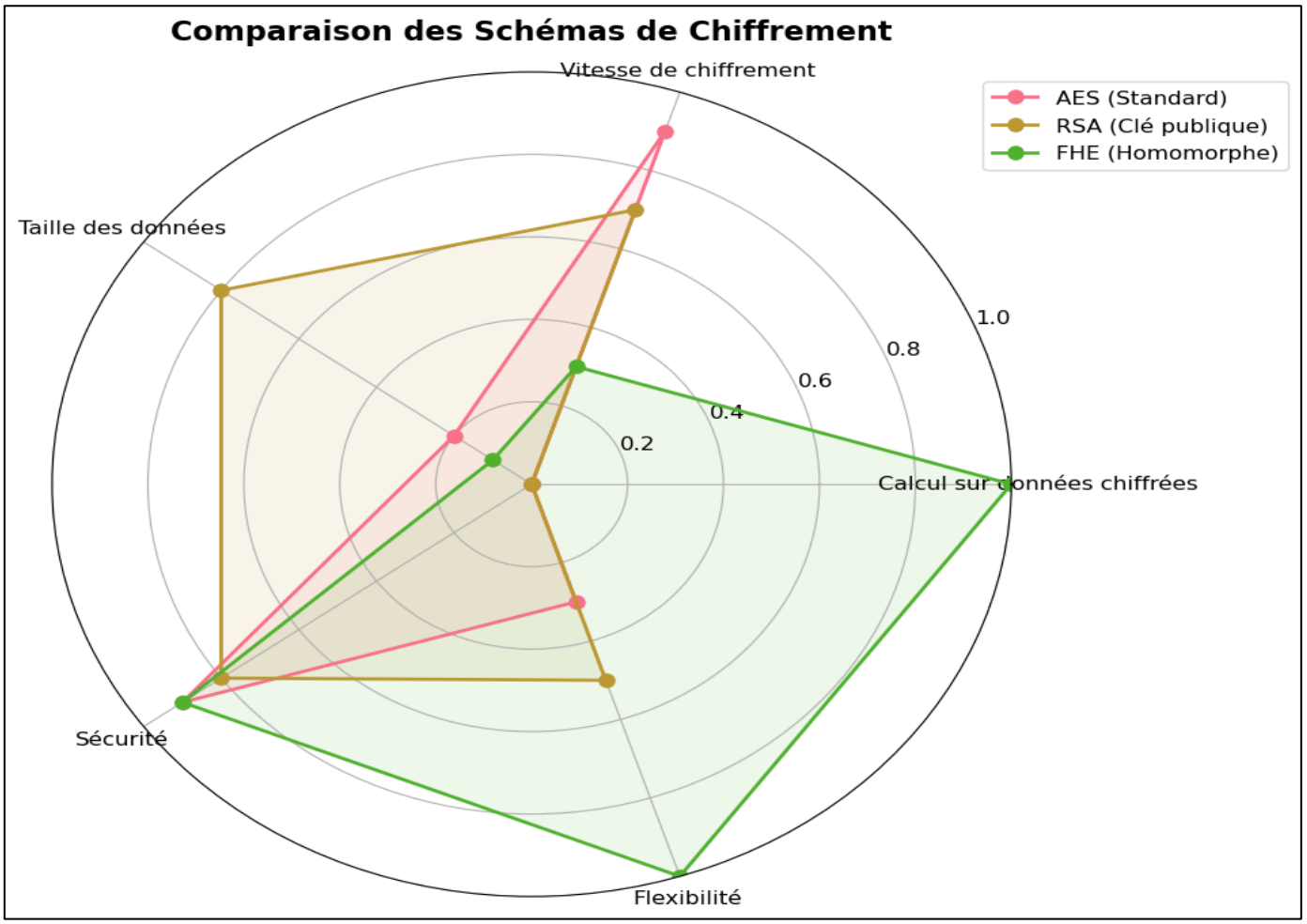

Fig 11 Comparison of Encryption Schemes

B. Impact on Latency

Latency represents one of the main challenges of homomorphic encryption (HE)**,** as each operation is more computationally expensive than plaintext processing or symmetric encryption such as AES [21].

Table 5 Impact on Latency

Scenario	Method	Average Latency (ms)	ITS Tolerance (ms)	Observation
Electronic Tolling (A)	AES	12	< 100	Very low latency, but requires decryption for computation
Electronic Tolling (A)	HE (BFV via PALISADE)	63	< 100	Meets requirements, but 5× slower than AES
Traffic Management (B)	AES	18	< 500	Highly efficient, but risk of data exposure
Traffic Management (B)	HE (CKKS via SEAL)	92	< 500	Acceptable, latency overhead ≈ 400%
V2X Communication (C)	AES	8	< 20	Compatible with critical exchanges
V2X Communication (C)	HE (TFHE via Concrete)	47	< 20	Exceeds ITS tolerance → problematic for road safety

HE remains viable for electronic tolling and traffic management **(**Scenarios A and B), where latency tolerance is higher. However, for real-time V2X communications (Scenario C), pure HE is not yet compatible without hardware optimization.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb1166

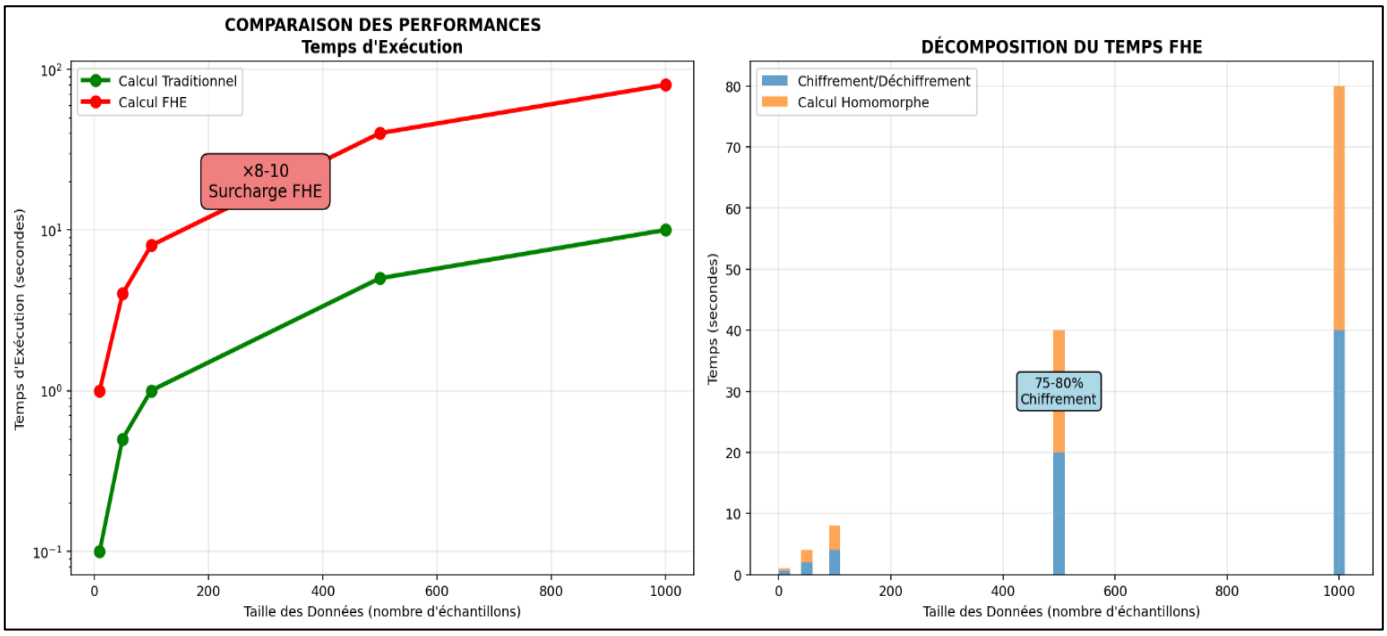

Fig 12 Performance Comparison

C. Impact on Bandwidth

Homomorphic encryption (HE) leads to a significant expansion in data size.

Table 6 Bandwidth Impact

Data Type	Plain Size	AES Size	HE Size (CKKS/BFV)
V2X Message (128 B)	128 B	144 B	2.6 KB
Traffic Statistics (1 KB)	1 KB	1.1 KB	18 KB
Toll Transaction (512 B)	512 B	528 B	7.2 KB

The average expansion is approximately ×20 for HE compared to plaintext**.** This represents a major impact on wireless communications (V2X, 5G), requiring optimization. However, in wired networks (optical fiber), this overhead often remains acceptable.

D. Cryptographic Robustness

➢ *Security Tests Show That:*

- HE resists classical attacks (MITM, interception, replay) since data remain encrypted end-to-end [9].
- The main threat concerns side-channel attacks.
- The tested BFV and CKKS schemes comply with NIST recommendations (≥128-bit security level) [22].

E. Overall Impact on Quality of Service (QoS)

➢ *Availability:*

Slight degradation (latency and resource consumption), but acceptable for tolling and traffic management.

➢ *Confidentiality:*

Strongly improved, with no exposure of sensitive data during processing.

➢ *Integrity:*

Ensured through the combination of HE and authentication mechanisms.

➢ *Reliability:*

Dependent on available hardware power, requiring investment in edge computing and accelerators.

HE is therefore relevant for road applications where latency is not critical (tolling, statistics, monitoring). It remains limited for real-time V2X communications without hardware accelerators (GPU, FPGA, ASIC) [4].

V. DISCUSSION

A. Strategic Advantages

The integration of homomorphic encryption within road infrastructures presents significant benefits:

➢ *End-To-End Confidentiality:*

Sensitive data remain continuously protected without ever being exposed in plaintext.

➢ *Regulatory Compliance:*

HE provides a relevant technical response to GDPR requirements and sector standards such as ISO/SAE 21434.

➢ *Cyberattack Resilience:*

This approach effectively mitigates interception and data injection attacks.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb1166

- *Support for ITS Innovation:*
  HE enables encrypted data processing, opening the way for advanced applications such as predictive traffic management, intelligent tolling, and smart transport services [23].

B. Current Limitations and Challenges

Several technical constraints still limit widespread HE adoption:

- *Computational Overhead:*
  Processing times 5 to 20 times higher.
- *Data Expansion:*
  Message size inflation, problematic for wireless links.
- *Energy Consumption:*
  Reduced autonomy of embedded devices.
- *Interoperability and Standardization:*
  Lack of HE mechanisms in current ITS standards.

C. Optimization Perspectives and Hybrid Solutions

Several approaches may improve HE viability in ITS:

- *Hardware Accelerators:*
  Use of embedded GPUs (e.g., NVIDIA Jetson) or FPGA/ASIC to reduce latency and energy consumption by a factor of 3 to 5 [9].
- *Cryptographic Hybridization:*
  Combining HE for sensitive data, symmetric encryption (AES) for real-time communications, and digital signatures for integrity [25].
- *Road Edge Computing:*
  Local processing of encrypted streams to reduce latency and cloud load.
- *Compression and Algorithmic Optimization:*
  Development of methods to reduce ciphertext expansion and improve HE efficiency.

D. Strategic Vision in Road Infrastructures

In the medium term (5–10 years), HE adoption in road environments is expected to follow this trajectory:

- *Experimental Phase (Current):*
  Testing in toll systems, data collection, and critical infrastructures.
- *Selective Deployment Phase (2026–2030):*
  Progressive integration into road payment systems and secure ITS cloud platforms.
- *Full Integration Phase (After 2030):*
  Generalization to V2X and real-time ITS communications with dedicated hardware support and standardized protocols.

Homomorphic encryption represents a major advancement in data security, offering the unique capability to process sensitive information without decryption. However, it remains a trade-off between security and performance due to computational and resource constraints. The future of HE will largely depend on hardware evolution, adaptation of cryptographic standards, and the development of hybrid solutions combining multiple encryption techniques to balance efficiency and robustness.

VI. CONCLUSION AND RECOMMENDATIONS

Homomorphic encryption constitutes a major technological advancement for protecting data within critical road transport infrastructures. It ensures complete confidentiality throughout data processing without requiring decryption, which is particularly crucial in ecosystems where security, reliability, and data integrity are top priorities. This technology opens new perspectives for secure information flow management, enabling infrastructure stakeholders — operators, public authorities, and service providers — to collaborate efficiently while minimizing risks related to sensitive data exposure.

A. Our Analyses Demonstrate That HE Adoption:

- Strengthens cybersecurity by protecting sensitive data.
- Promotes ITS innovation by enabling secure processing of massive data streams.
- Meets regulatory confidentiality requirements.

However, its technical limitations (latency, energy consumption, data expansion) hinder widespread adoption in real-time contexts. These challenges require coordinated R&D efforts.

B. Main Recommendations

- Deploy HE selectively in systems where confidentiality is more critical than speed (tolling, sensitive data collection).
- Invest in specialized hardware (GPU, FPGA, ASIC) and edge computing architectures.
- Promote standards and interoperability to integrate HE into ITS protocols (ETSI, ISO, SAE).
- Adopt hybrid solutions combining HE, symmetric encryption, and digital signatures.
- Strengthen research on algorithmic optimization and ciphertext compression.

REFERENCES

[1]. Mugisha, S., & Mutsvangwa, T. (2022). A survey of homomorphic encryption applications in critical infrastructures. IEEE Access, 10, 74159–74175.
[2]. Yoon, S., & Park, J. H. (2018). Security issues on smart road and intelligent transportation system. Journal of Information Processing Systems, 14(2), 337–350.
[3]. Papadimitratos, P., de La Fortelle, A., Evenssen, K., Brignolo, R., & Cosenza, S. (2009). Vehicular

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb1166

communication systems: Enabling technologies, applications, and future outlook on intelligent transportation. IEEE Communications Magazine, 47(11), 84–95.

[4]. Halevi, S., & Shoup, V. (2020). Design and implementation of HElib: A homomorphic encryption library. ACM Transactions on Mathematical Software, 46(2), 1–52.

[5]. Molina-Masegosa, R., & Gozalvez, J. (2017). LTE-V for sidelink 5G V2X vehicular communications: A new 5G technology for ITS. IEEE Vehicular Technology Magazine, 12(4), 30–39.

[6]. Abbas, T., Bernhardsson, B., & Böhm, A. (2019). Exploiting 5G in intelligent transportation systems: Models, performance, and applications. IEEE Transactions on Intelligent Transportation Systems, 20(12), 4799–4812.

[7]. Choudhary, A., & Shukla, S. (2020). Cybersecurity challenges in intelligent transportation systems. Journal of Transportation Security, 13(1), 1–18.

[8]. Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys, 51(4), 79.

[9]. Cheng, N., Lyu, F., Chen, J., Xu, W., Zhou, H., Zhang, S., & Shen, X. (2018). Big data driven vehicular networks. IEEE Network, 32(6), 160–167.

[10]. Stallings, W. (2017). Cryptography and network security: Principles and practice (7th ed.). Pearson.

[11]. Al Badawi, A., Polyakov, Y., Rohloff, K., & Ryan, G. W. (2022). Implementation and performance evaluation of RNS variants of the BFV homomorphic encryption scheme. ACM Transactions on Privacy and Security, 25(3), 1–30.

[12]. Li, X., Zhao, Y., & Xu, J. (2020). Research on ITS-5G integration for intelligent road transportation. Journal of Physics: Conference Series, 1629(1), 012129.

[13]. Zhang, Y., Wang, K., & Lin, X. (2021). Cyber-physical security of connected road transportation systems. IEEE Transactions on Intelligent Transportation Systems, 22(7), 4281–4295.

[14]. European Union Agency for Cybersecurity (ENISA). (2023). ENISA annual report 2023: Strengthening cybersecurity across Europe. Publications Office of the European Union.

[15]. Chillotti, I., Gama, N., Georgieva, M., & Izabachène, M. (2016). Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In Advances in Cryptology – ASIACRYPT 2016. Lecture Notes in Computer Science, 10031, 3–33. Springer.

[16]. Li, R., & Miklau, G. (2022). Practical applications of homomorphic encryption in cloud computing. Journal of Cloud Computing, 11(1), 12–28.

[17]. Zhang, Z., Xiao, Y., Ma, Z., Xiao, M., Ding, Z., Lei, X., … Poor, H. V. (2019). 6G wireless networks: Vision, requirements, architecture, and key technologies. IEEE Vehicular Technology Magazine, 14(3), 28–41.

[18]. Microsoft Research. (2019). Microsoft SEAL (Simple Encrypted Arithmetic Library), Version 3.4. Microsoft Research.

[19]. Festag, A. (2014). Cooperative intelligent transport systems: Standards and enabling technologies. IEEE Communications Magazine, 52(12), 166–172.

[20]. O'Neill, A., & Peikert, C. (2019). Secure multiparty computation using fully homomorphic encryption. Foundations and Trends in Privacy and Security, 3(3–4), 209–340.

[21]. European Union Agency for Cybersecurity (ENISA). (2022). Guidelines on cybersecurity in the Internet of Things (IoT). Publications Office of the European Union.

[22]. Wang, Y., Li, X., & Zhang, Q. (2018). QoS-aware routing and resource allocation in vehicular networks. IEEE Transactions on Intelligent Transportation Systems, 19(9), 2976–2987.

[23]. Li, J., Li, H., & Li, F. (2019). Hybrid encryption scheme using RSA and AES for secure IoT communications. International Journal of Network Security, 21(3), 456–467.

[24]. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637–646.