International Journal of Engineering Trends and Technology
ISSN: 2231-5381/ https://doi.org/10.14445/22315381/IJETT-V74I11P109

Volume 74 Issue 11, 128-134, November 2026
© 2026 Seventh Sense Research Group®

Original Article

LLM-Assisted Federated Learning with Severity-Driven Adaptive Hardware Security

Srividya B V[1], Upendra Kumar[2]

[1]*Lincoln Global Postdoctoral Research (LGPR), Lincoln University College, Malaysia.*
[2]*Institute of Engineering and Technology, Lucknow, India, Adjunct research faculty, Lincoln University College, Malaysia.*

[1]*Corresponding Author: srividyabv@gmail.com*

Received: 29 May 2026 Revised: 20 August 2026 Accepted: 18 September 2026 Published: 25 November 2026

Abstract - *This work presents a hybrid intelligent security framework integrating Large Language Models (LLMs), Federated Learning (FL), and hardware-based adaptive cryptography for malware detection in distributed healthcare environments. Federated Learning enables privacy-preserving distributed threat detection among healthcare clients through collaborative decentralized model training. The LLM performs context-aware threat analysis by processing heterogeneous data sources such as system logs, network activity, and sensor telemetry to estimate malware and anomaly probabilities. These probabilities are utilized to compute a severity index that drives an FSM-based hardware security module for real-time adaptive security enforcement. Based on the evaluated threat level, the proposed system dynamically selects suitable encryption strength and key management mechanisms while maintaining data privacy through secure federated aggregation. By combining context-aware intelligence, decentralized learning, and hardware acceleration, the framework effectively addresses non-IID data challenges, improves threat responsiveness, and enables scalable, privacy-preserving cybersecurity for medical IoT systems.*

Keywords - *Hardware-Assisted Federated Learning (FL), Large Language Model (LLM), Malware detection, Adaptive cryptographic hardware, Privacy-Preserving security.*

1. Introduction

The rapid digitization of healthcare systems, driven by the rise of IoT-enabled medical devices, Electronic Medical Records (EMRs), and networked clinical infrastructures, has significantly increased the attack surface for cyber threats. Malware attacks and anomalous behaviors in such environments can compromise sensitive patient data, disrupt critical services, and pose serious risks to patient safety. Traditional centralized security mechanisms are often inadequate in these settings due to data privacy concerns, heterogeneous data distributions, and the need for real-time threat detection.

Federated Learning (FL) has emerged as a promising prototype to address these challenges by enabling collaborative model training across distributed clients without sharing raw data. However, existing FL-based security frameworks often struggle with non-IID data, limited adaptability to dynamic threat conditions, and lack of integration with intelligent threat analysis mechanisms. Recent advances in Large Language Models (LLMs) provide powerful capabilities for analyzing unstructured and heterogeneous data sources, such as system logs and network telemetry, enabling improved estimation of malware and anomaly probabilities.

In this work, a hybrid framework is proposed that integrates LLM-based threat intelligence with federated learning and hardware-accelerated adaptive security mechanisms. The LLM processes diverse data inputs to generate probabilistic indicators of malicious and anomalous behavior.

These probabilities are used to compute a severity index, which serves as the central decision parameter for a hardware module. The hardware layer enables real-time adaptive selection of cryptographic protection schemes, including dynamic key generation and varying encryption strength, based on the assessed threat level. Additionally, secure aggregation techniques are employed to ensure privacy-preserving model updates within the federated learning framework.

The proposed approach addresses key limitations of existing systems by combining context-aware intelligence, decentralized learning, and hardware-level enforcement of security policies. It enhances robustness against evolving threats supports non-IID data environments, and ensures scalable, privacy-preserving cybersecurity for modern healthcare systems.

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

2. Literature Survey

This section describes the work proposed by several researchers in the domain of LLM-based malware detection with federated learning in health care and hardware-accelerated cryptographic systems.

In the paper entitled "Federated learning for malware detection in IoT devices," the authors recommended the use of a federated learning framework, where all the concerned IoT devices work in collaboration for training a global malware classifier without any exchanging any information, such as raw data, recorded précised measurements, interaction cost, and poisoning resilience under realistic environments with non-IID data distributions [1].

Malware detection using federated learning is not restricted to only the Internet of Things. Several authors have used Convolution Neural Network and a variant of recurrent neural network to target personal computers, Smart grids, servers, and Android. According to the survey, FL models very often accomplish high accuracy and an F1-score that is very near to the optimal response when data from all clients is balanced [2-4]. When dealing with large volumes of non-IID data, a slight decrease in accuracy, which is around 3 to 10%, is observed with the conventional FL. According to the survey, a variety of optimizers are available, which work on the client drift. Among them, FedAvg, FedEx, MOON, SCAFFOLD, and Personalized layers are very significant. Each client dealing with their private non-IID data determines the probability of malware being either benign or malicious. Also, the presence of malware in a compromised node demands the detection of any behavioural anomaly. Based on the severity of the threat, adaptive cryptographic protection methods with dynamic key generation are used.

The authors of [5] have integrated LLMs with federated learning to enhance anomaly and malware detection across distributed systems. It leverages LLM-generated insights to improve threat detection while maintaining data privacy.

In the article [6], the authors approach is to combine federated learning with multimodal LLMs to analyze heterogeneous data such as logs and network traffic. It achieves high detection accuracy in distributed environments but does not address adaptive cryptographic protection.

SecureLLM [7] focuses on ensuring privacy and security in LLM-based systems by incorporating secure processing and data protection techniques. It highlights risks in LLM deployment but does not integrate with federated learning or hardware-based security mechanisms.

The article [8] reviews privacy threats and security challenges in federated learning for healthcare applications. It discusses techniques like encryption and secure aggregation, but lacks intelligent threat assessment using LLMs or adaptive hardware-based solutions.

MedShieldFL [9] proposes a secure federated learning framework with encryption mechanisms to defend against attacks such as data poisoning and interception. While it enhances FL security, it does not incorporate LLM-based threat intelligence or dynamic hardware-level adaptation.

The article [10] applies federated learning for malware detection in distributed IoT environments, improving privacy and scalability. However, it does not include advanced AI models like LLMs or adaptive cryptographic strategies.

The authors of [11] have used homomorphic encryption in federated learning. Though it is computationally expensive, it is secured. Modular multiplication is optimised; hence, it resulted in a reduction of up to 71% in the encryption time, using this approach.

The authors of [12] have discussed the implementation of scalar multiplication in ECC algorithm, its implementation on FPGA, latency, and throughput.

S. Joshi [13] have implemented RSA cryptographic accelerator and analysed its performance by comparing area, timing, and power on 45nm, 90nm and 180nm technology. The authors of [14] have implemented AES encryption and decryption algorithms in Cadence Virtuoso by designing Shift register, Key generation module, XOR and NOR gates as leaf nodes. They have functionally verified the working of the module and also have determined the power consumed for the complete analysis.

The authors of [15] have implemented 3-bit counter and full adder concurrently using Finite State Machine approach and have generated an RTL to GDS-II file. Using this approach, performance analysis with respect to area, power and timing have been carried out. The authors concluded that using FSM approach, the overall power consumed has reduced. While prior works integrate LLMs with federated learning for intelligent threat detection, they have not covered hardware-level enforcement of adaptive security policies. This work bridges that gap by incorporating a severity-driven Verilog-based cryptographic framework. The Adaptive cryptographic system is designed using Finite State Machine approach. Performance of the system is evaluated in terms of power, area and delay using Cadence Genus, including generation of the system from RTL to GDS-II.

The proposed system integrates LLM-assisted federated threat detection with a severity-driven FSM-based adaptive cryptographic hardware framework. The RTL design is synthesized and evaluated using Cadence tools for power, area, delay, and RTL-to-GDS-II implementation performance.

3. Proposed Work

This research work is about Severity aware Federated Security architecture in health care systems that combine threat analysis and hardware based protection, as shown in Figure 1. Federated learning is extensively employed in a distributed health care system, where each client trains their own private data locally and communicates only the necessary weights/gradients to the global system. Upon detection of malware as benign or malicious, the anomaly detection is performed on the infected network. Severity index is computed using the Malware and anomaly probabilities, which in turn dynamically drives adaptive cryptographic mechanisms. Based on threat levels, encryption schemes such as AES, ECC, and Edwards curve cryptography are selected. The system is implemented using a hardware security engine, enabling real-time, scalable, and secure protection.

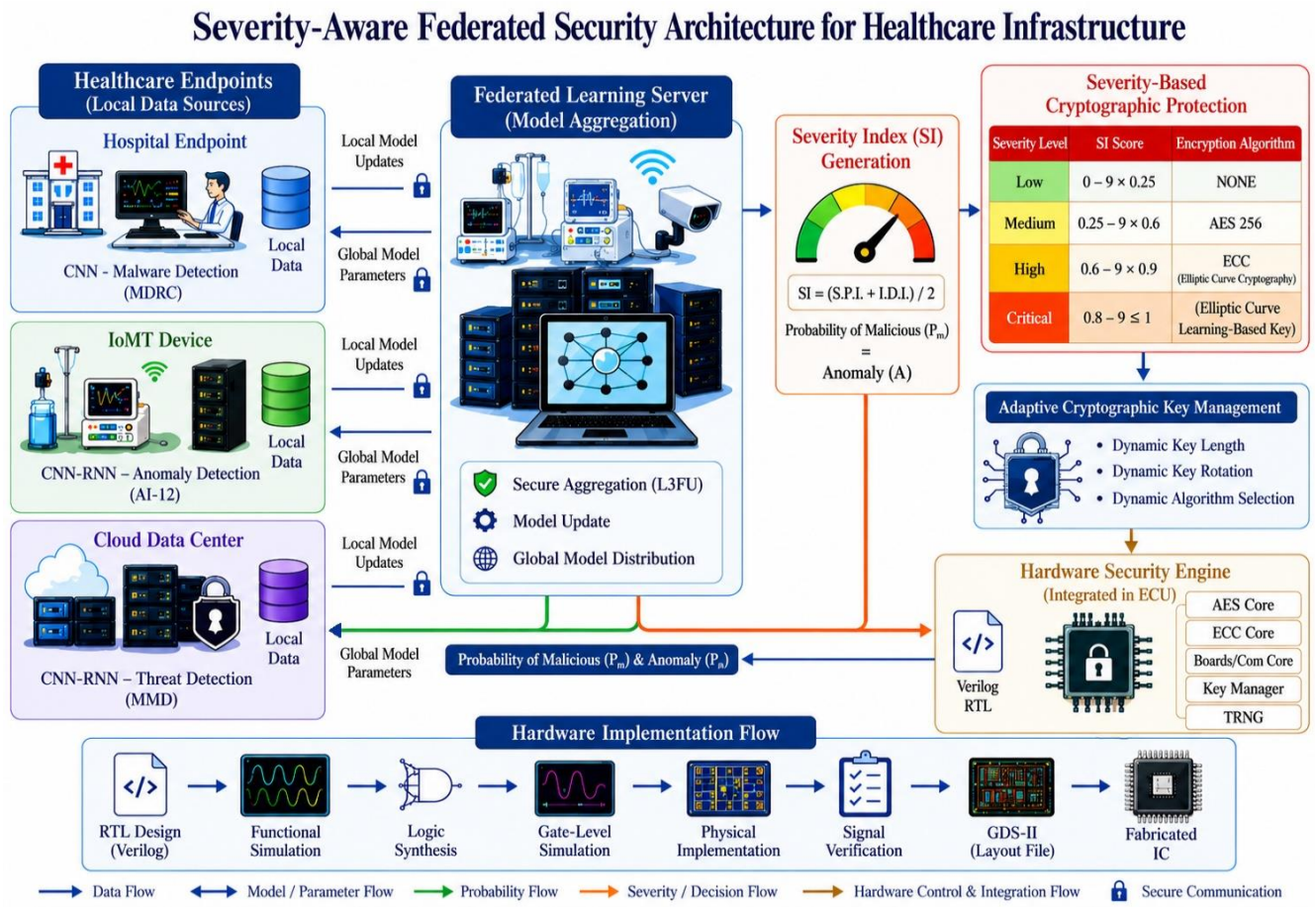


Fig. 1 Severity aware federated security architecture for healthcare infrastructure

The LLM analyses the non-IID heterogeneous data from the IoT of medical Things for any possible malware and estimates the malware probability and anomaly probability. These probabilistic outcomes provide a context-aware intelligent security decision.

In Federated learning, the clients independently train their models without sharing any raw data, thereby preserving privacy. The global model aggregates the local updates and provides probabilistic inputs for further threat evaluation.

Severity index is a weighted sum of Malware probability and anomaly probability. This value is categorised into severity levels for hardware processing. Based on the severity index, AES, ECC or Edwards curve Digital Signature is selected. This ensures a balance between security strength and hardware efficiency.The architecture of the hardware security engine is responsible for computing severity, select appropriate encryption modes and execute the suitable cryptographic operations. It comprises of control logic and key management units. The control logic uses a Finite State Machine (FSM) approach to dynamically switch between the various encryption modes based on the severity level. Easy integration and scalability are the core aspects of this modular design.

This design follows a standard flow from RTL simulation, synthesis and physical design. The system is evaluated based on area, delay, power, throughput and security strength, the efficiency of the severity-driven adaptive hardware security.

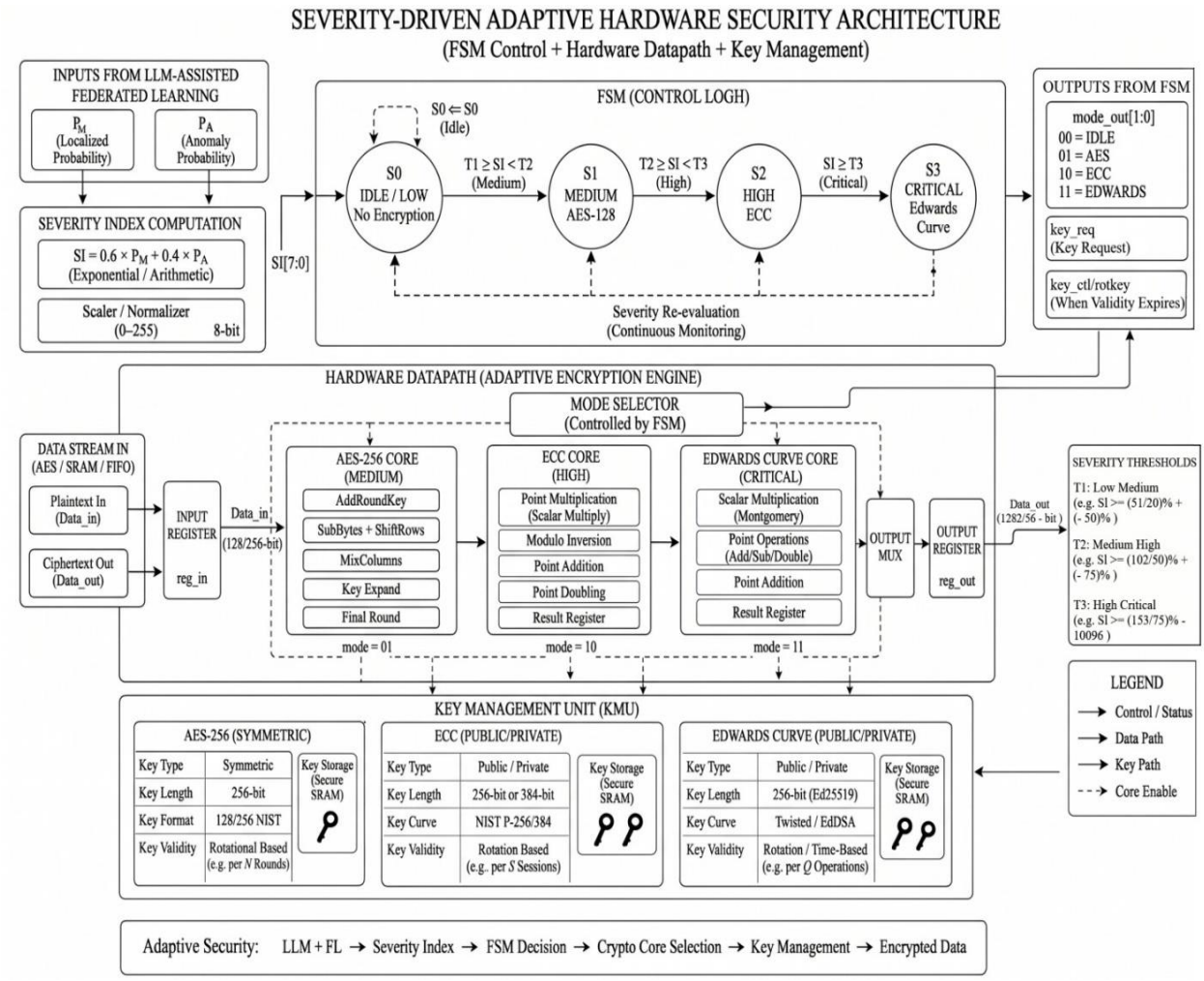


Fig. 2 Hardware security architecture

Figure 2 depicts hardware architecture for severity driven adaptive security system. It integrates LLM assisted Federated learning with real-time cryptographic control. Severity index is computed using the weighted average of malware and anomaly probability.

This is further processed by the FSM to select an appropriate encryption model. Based on the severity level, the hardware data path dynamically activates the cryptographic cores. A key management unit, integrated with every cryptographic core, supplies the required key with different type, varying length and validity periods for each algorithm. This architecture ensures efficient, scalable data protection in the healthcare infrastructure.

To demonstrate the effectiveness of this design, the following section presents the simulation results, synthesis and hardware analysis. The results highlight the efficiency of dynamically choosing a strong encryption algorithm, which impacts area, delay and power.

4. Results and Discussion

This section elaborates the implementation details of the various encryption systems, such as Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), Edwards Curve-based cryptography and the Adaptive Cryptographic system, operating on 128-bit data. The functional verification, in terms of simulation results, performance parameters such as area, gate count, power analysis, timing analysis, and frequency of operation, are tabulated.

4.1. Functional Verification

From Table 1, it can be observed that the Finite State Machine (FSM) model selects an appropriate cryptographic system based on the Severity Index (SI) to keep the system secured. When the system is affected by malware, depending on severity of threat, the system files are encrypted suitably, and the malware executable is encrypted and concealed to avoid further access. System which exhibits anomalous behaviour is isolated from the network, and strong security algorithms are implemented on it.

Table 1. Functional verification of severity driven adaptive system

Test case	Pm	Pa	Severity Index	FSM state	Encryption selected
TC1	0.2	0.3	0.24	IDLE	None
TC2	0.4	0.5	0.44	MEDIUM	AES-256
TC3	0.7	0.6	0.66	HIGH	ECC
TC4	0.9	0.8	0.86	CRITICAL	Edwards Curve-based Cryptography

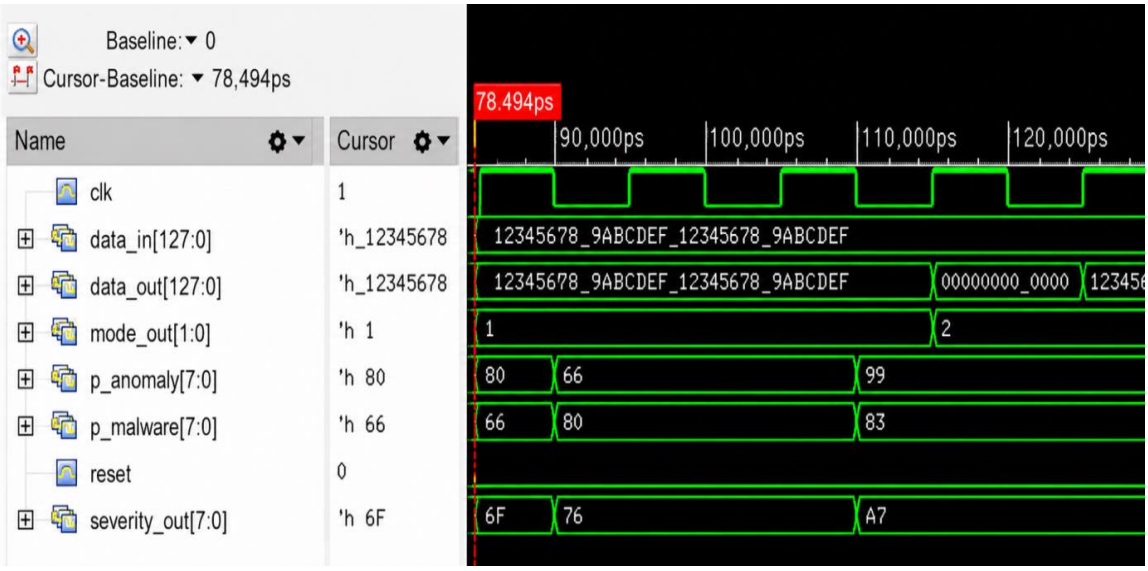


Fig. 3 Simulation results

Figure 3 depicts the simulation results for different cases of probability of malware and probability of anomaly behaviour.

Probability of malware is (66)h= (102) d=102/256=0.398
Probability of anomaly behaviour is (80)h= (128) d=128/256=0.5.
Severity index is computed as SI=0.6*Pm+0.4*Pa=0.44.

Here, mode 1 is selected. In mode-1, AES encryption algorithm is executed. It can be observed that the data_in and data_out(after decryption) are the same.

Probability of malware is, (B3)h= (179) d=179/256=0.69
Probability of anomaly behaviour is (99) h= (153) d=153/256=0.6.
Severity index is computed as SI=0.6*Pm+0.4*Pa=0.66.

Here, mode 2 is selected. In mode-2, ECC encryption algorithm is executed. It can be observed that the data_in and data_out(after decryption) are the same.

From Table 2, it can be observed that area occupied by the control logic of adaptive system is optimal, as it involves designing the FSM, severity index computation, key management and adaptive selection logic.

Table 2. Synthesis results of cryptographic cores

Algorithm	Area	Gate Count
AES-256	28344.255um^2	670
ECC	1818799.0 um^2	92016
Edwards Curve	84573.721um^2	4620
Adaptive System	53541.736 um^2	1586

Table 3 is the performance of the implemented adaptive security system, demonstrating an area-power efficient design. This FSM-based adaptive encryption system has faster switching between states, ensuring a dynamic security reconfiguration.

Table 3. Performance of the hardware security system

Metric	Value
Total Area	53541.736 um^2
Total Power	1.05923e-02W
Maximum frequency	107.48Mhz
Critical path delay	9.304ns

4.2. Timing Analysis

The critical path delay and the maximum operating frequency are determined for the various encryption models. AES provides the best performance, with the lowest critical delay and the highest frequency. ECC is the slowest because of its complex arithmetic. Edwards curve and the proposed adaptive system performance is identical.

Table 4. Timing performance of encryption modes

Parameter	Critical Path delay	Fmax(MHz)
AES-256	6.373ns	156.9MHz
ECC	9.962ns	100.38MHz
Edwards Curve	9.296ns	107.57MHz
Adaptive System	9.304ns	107.48Mhz

4.3. Power Analysis

The total power, dynamic power and leakage power is determined for the adaptive cryptographic system and each encryption module. The results are tabulated in Tables 5 and 6.

Table 5 depicts the power consumed by the cryptographic model for various severity levels. AES has very low power consumption compared to ECC, as it involves several complex calculations. More intense is the calculations, more security is offered.

From Table 6, it can be observed that the adaptive crypto system offers the lowest leakage power among the cryptographic modules.

Table 5. Power consumption vs severity level

Severity level	Active Encryptor module	Power(W)
Low	None	-
Medium	AES-256	2.99817e-03
High	ECC	1.83602e-01
Critical	Edwards Curve Digital Signature and Cryptosystem	6.19048e-03

Table 6. Power consumption comparison

Parameter	Dynamic Power(W)	Leakage Power(W)
AES-256	2.53750e-03	9.26684e-06
ECC	1.02464e-01	8.87086e-05
Edwards Curve	4.24196e-03	2.28261e-06
Adaptive System	8.82770e-03	1.60109e-06

4.4. Area-Delay-Power Trade Off

Designs with larger area consume more dynamic power. Strategies adopted to reduce delay may increase power. Higher operating frequency increases switching activity. AES and the adaptive system have an improved Area-Delay product as well as a Power-Delay product.

4.5. Throughput and Latency

The results are tabulated for a block size of 128 bits. The results obtained in Tables 7 and 8 demonstrate a trade-off between security complexity, latency and data throughput. Algorithms with increased computational complexity have a higher latency, and its throughput is also affected.

Table 7. Throughput and latency

Severity Level	Parameter	Latency(in cycles)	Throughput
Low	None	14	859.8 Mbps
Medium	AES-256	25	1434.5 Mbps
High	ECC	30	514.0 Mbps
Critical	Edwards Curve	16	458.9 Mbps

Table 8. Delay and throughput comparison

Parameter	Delay	Latency(Cycles)
AES-256	6.373ns	14
ECC	9.962ns	25
Edwards Curve	9.296ns	30
Adaptive System	9.304ns	16

Table 9 gives the performance of the adaptive cryptosystem. The adaptive cryptographic system introduces a mode switching time of 20-30 ns due to FSM-based runtime selection of encryption algorithms according to the severity index. Although the adaptive control logic increases area (20543.846 μm^2) and introduces 15-25% power overhead with a 10-18% latency increase, it enables flexible and security-aware operation compared to fixed cryptographic architectures.

Table 9. Performance of the adaptive cryptosystem

Parameter	Value	Description
Mode switching time	20-30ns	Time required for the FSM to switch between the various encryption modes, based on severity index
Control logic area	20543.846um^2	Area occupied by FSM, severity index computation, key management, and adaptive selection logic
Power overhead	15-25%	power consumed due to adaptive cryptographic switching and multiple hardware security modules
Performance impact	10-18% latency has increased	Additional latency introduced by runtime severity analysis and encryption mode switching compared to fixed cryptographic systems.

The adaptive cryptosystem uses FSM based architecture. Based on the severity index obtained from LLM, the adaptive cryptosystem operates in 4 different modes as shown in Figure 1. Time taken to switch between the various cryptographic algorithms is tabulated in Table 10.

Table 10. FSM switching performance

Transition	Switching time	Delay
AES-> ECC	20ns	AES delay is 2.3times higher than ECC
ECC->Edwards Curve	30ns	ECC gives a delay of 2.82 times higher than Edwards
Edwards curve-> AES	20ns	Edwards Curve gives 6.5 times lower delay compared to AES

4.6. Key Management Evaluation

The key management unit generates keys for AES, ECC and Edward's curve-based cryptographic algorithms. It asserts validity of the key based on number of times the key is used.

This unit is also responsible for selecting the right key based on the mode of selection in an adaptive crypto-system. This unit occupies a total cell area of 365.904um^2, with a cell count of 8. The leakage power is 1.11801e-08Watts, with an internal power of 2.44042e-05Watts and total power of 2.71447e-05Watts. The critical path delay is 0.385ns.

5. Conclusion

From the results, it is evident that the higher the security, the more complex is the algorithm. Area and delay increases. Compact architectures improve the power and timing efficiency. The adaptive system achieves the balance between area and delay. This algorithm can be further optimized to reduce the hardware, while still preserving the performance, though AES remains the most efficient cryptographic system.

References

[1] Valerian Rey et al., "Federated Learning for Malware Detection in IoT Devices," *Computer Networks*, vol. 204, pp. 1-14, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Himanshi Babbar, Shalli Rani, and Wadii Boulila, "NGMD: Next Generation Malware Detection in Federated Server with Deep Neural Network Model for Autonomous Networks," *Scientific Reports*, vol. 14, no. 1, pp. 1-15, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] D. Karthik et al., "Federated Learning based Malware Detection System," *2025 International Conference on Knowledge Engineering and Communication Systems (ICKECS)*, Chickballapur, India, pp. 1-7, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[4] Ripal Ranpara et al., "Scalable Architecture for Autonomous Malware Detection and Defense in Software-Defined Networks using Federated Learning Approaches," *Scientific Reports*, vol. 15, no. 1, pp. 1-16, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[5] Qiang Yang et al., "Federated Machine Learning: Concept and Applications," *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 2, pp. 1-19, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[6] Brendan McMahan et al., "Communication Efficient Learning of Deep Networks from Decentralized Data," *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, PMLR*, vol. 54, pp. 1273-1282, 2017. [Google Scholar] [Publisher Link]

[7] Peter Kairouz, and H. Brendan McMahan, "Advances and Open Problems in Federated Learning," *Foundations and Trends in Machine Learning*, vol. 14, no. 1-2, pp. 1-210, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Sawsan Abdulrahman et al., "A Survey on Federated Learning: The Journey from Centralized to Distributed On-Site Learning and Beyond," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5476-5497, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Tom Brown et al., "Language Models are Few-Shot Learners," *Advances in Neural Information Processing Systems*, vol. 33, pp. 1877-1901, 2020. [Google Scholar] [Publisher Link]

[10] Yue Zhao et al., "Federated Learning with Non-IID Data," *arXiv preprint*, pp. 1-12, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[11] Zhaoxiong Yang, Shuihai Hu, and Kai Chen, "FPGA-based Hardware Accelerator of Homomorphic Encryption for Efficient Federated Learning," *arXiv preprint*, pp. 1-7, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Rares Ifrim, Dumitrel Loghin, and Decebal Popescu, "A Systematic Review of Fast, Scalable, and Efficient Hardware Implementations of Elliptic Curve Cryptography for Blockchain," *ACM Transactions on Reconfigurable Technology and Systems*, vol. 17, no. 4, pp. 1-33, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] Shubhashri Joshi et al., "Scalability and Performance Analysis of 2048-Bit RSA Algorithm across Advanced CMOS Technology Nodes," *2025 International Conference on Applications of Machine Intelligence and Data Analytics (ICAMIDA)*, Aurangabad, India, pp. 1-5, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[14] Deepa M et al., "An Efficient Implementation of AES Algorithm for Cryptography using CADENCE," *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, pp. 1478-1484, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Amit Shohal, and Jasbir Kaur, "Efficient RTL to GDS II Flow for Finite State Machine Integration: A Physical Design Approach," *2024 IEEE 5th India Council International Subsections Conference (INDISCON)*, Chandigarh, India, pp. 1-5, 2024. [CrossRef] [Google Scholar] [Publisher Link]