The Role of Cryptography and AI in Defending against Malware Attacks in health care infrastructure

Dr. Srividya B V

Lincoln Global Postdoctoral Research (LGPR), Lincoln University College, Malaysia
Upendra Kumar,

Lincoln Global Postdoctoral Research (LGPR), Lincoln University College, Malaysia
CA: Srividya B V, pdf.Srividya@lincoln.edu.my

Abstract: This article presents an AI- driven adaptive cryptographic framework, where the encryption-decryption algorithms are dynamically selected based on the severity index of the malware attack. The severity index is computed based on the weighted average of malware and behavioral anomaly. The severity index is used by a light weight decision model to choose a secured cryptographic algorithm automatically. In this work, based on severity index, either AES-256 or hybrid cryptosystem comprising of ECC & AES or digital signature-supported Edwards Curve based Digital Signature algorithm integrated with ECC is chosen. The parameters considered are the key generation time, time for encryption and decryption, along with the communication overhead for various payload sizes and different severity levels, Depending on severity of threat, performance of the cryptographic system is tested and results are indicated using bar charts and graphs. The experimental analysis exhibits a significant reduction in computational and communication overhead when a low-risk is encountered while stronger security mechanisms are efficient for high-risk transmissions. This achieves a practical balance between privacy, confidentiality, integrity and efficiency in real-time and resource constrained environments.

Keywords: Malware detection, Severity Index, Cryptography, Key generation

Introduction

This article focuses on obtaining a secured environment when the health care infrastructure is infected by malware. A compromised system is isolated from the network, upon detection of behavioural anomaly, so that it prevents any unauthorized access, and spreading of malware laterally through the network. Subsequently the malware executable is safely concealed using a strong algorithm for preventing any further access. Using adaptive cryptographic techniques, the memory regions of each system in the network is encrypted. An appropriate choice of cryptographic algorithm based on severity of the attack is carried out by a light weight AI-based scheme. The chosen algorithm balances the security strength, computation time and communication overhead. In compromised situations, the proposed techniques maintain integrity and data security by enabling secured cyber analysis.

The proposed decision model dynamically chooses an appropriate cryptographic algorithm according to the severity of threat. This AI component functions as a contextual classifier, mapping a suitable encryption method to a severity index which in turn is derived from risk-related characteristics, behavioural anomaly and attack probability.

The model learns optimum threshold criteria that balance security strength and computing overhead rather than depending on a single static cryptographic algorithm. This makes it possible to use efficient

symmetric encryption (AES-256) to protect low-risk data, while stronger hybrid or public-key-based cryptographic techniques (ECC + AES, EdDSA + ECC) are triggered in medium- and high-risk scenarios. The technique is purposely lightweight to allow real-time adaptation in resource-constrained and latency-sensitive situations.

Related work

This section highlights the importance of integrating Artificial Intelligence and Cryptography for various real time applications.

Table 1. Comparison of existing cryptographic techniques used when malware is detected

Sl. No.	Title	Approach	Benefits
1	AI-Driven Cybersecurity in IoT: Adaptive Malware Detection and Lightweight Encryption via TRIM-SEC Framework[1]	Light weight Elliptic Curve Cryptography	Key generation with minimum computation
2	Cryptographic Techniques in Artificial Intelligence Security: A Bibliometric Review[2]	Survey on AI Security	Integration of Cryptography and AI to obtain Secured Privacy preserving AI systems
3	Prediction of android ransom ware with deep learning model using hybrid cryptography[3]	Hybrid Homomorphic Elliptic curve with blow fish is employed.	High Accuracy is obtained. Key generation and Computation time is significantly reduced.
4	Enhancing IoT security with a DNA-based lightweight cryptography system[4]	The authors have combined DNA sequences with ECC	Generates better security and reduces the strain on the system
5	A lightweight trusted framework for secure data exchange and threat mitigation in IoT-enabled healthcare environments[5]	Light weight ECC based Encryption protocol	The data is preserved confidentially with integrity and authentication.

From the survey, it is concluded that there is a rising demand for the development of adaptive encryption policies, which broadens the applicability to smart city, health care and IoT scenarios.

Key Contribution:

This work focuses on detection of malware in a health care infrastructure. Upon detection of a malicious malware and high risk, the infected system is securely isolated. The other systems in the network are protected by hiding the malware executable. The real-time memories of these systems are encrypted. Thus a severity-index based policy model is proposed to map the cryptographic strength, enabling context-aware security enforcement. This work introduces an intelligent decision-making framework that dynamically selects suitable cryptographic algorithms among AES, Hybrid ECC+AES, EdDSA based on real-time malware severity and system risk, there by optimizing the trade-off between security strength and computational overhead.

Method, Experiments and Results

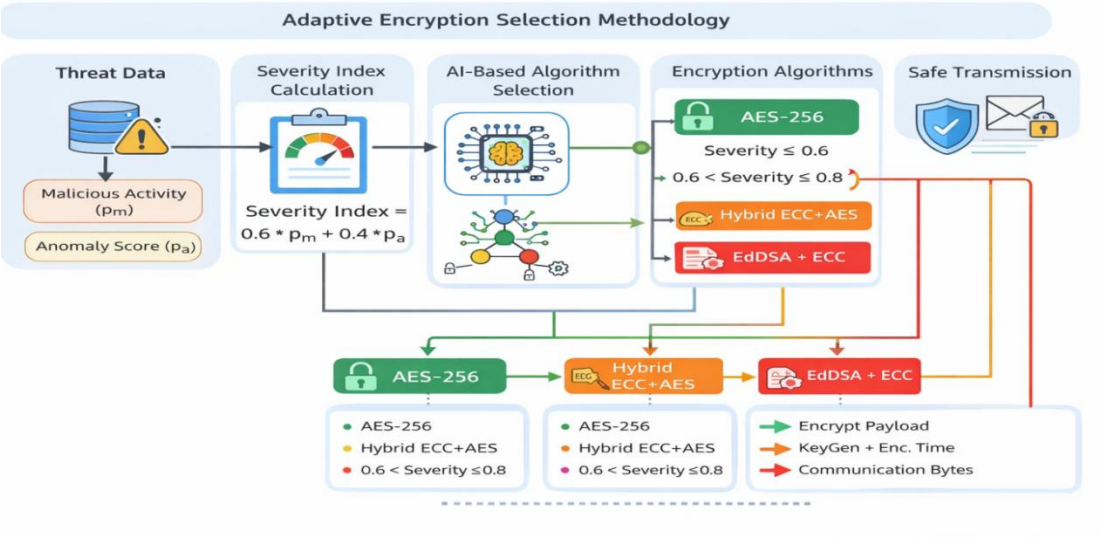

Figure 1: Adaptive Encryption Selection

In this article, a secured approach is used to detect malware and behavioral anomaly for the sensor network in health care infrastructure. Isolation of the infected system, concealing the malware executables using an appropriate stenographic technique, using AI-driven adaptive cryptographic techniques with dynamic key management strategy for memory is the highlight of this work. Figure 1 depicts an adaptive encryption system for defending against malware attacks.

When a malicious malware is detected, severity of threat is determined. If threat is low or medium, the relevant data is automatically encrypted using a suitable algorithm. Isolation of the system from the network, memory analysis is carried out immediately, if the threat is either high or critical. A severity index is computed based on the observed threat level, system privilege misuse, memory tampering, and execution behavior.

The malware detection system determines the Severity Index $SI = \alpha P_m + \beta P_a$, where Pm is the probability of malware being malicious and Pa is the probability of anomaly behavior. The Severity Index is fed as an input to the decision tree classifier, which is trained using Gini impurity criterion $CA = f(SI)$. Thus an appropriate Cryptographic Algorithm is selected based on the learned function of Severity. This classifier partitions the severity space into multiple security regions. Based on the learning thresholds, an encryption algorithm is dynamically selected. This adaptive approach offers layered security, guarantees protection of compromised systems in network while maintaining efficiency and integrity.

In health care there are computing systems, Internet of Medical Things driven by sensors, Cloud servers for maintaining patient information. The health care infrastructure demands continuous service. Hence it is essential to maintain the health care facilities with utmost care.

Figure 2a depicts the average overhead versus Severity levels. It can be seen that when severity index is above 0.8, digital signature scheme integrated with ECC is used. Maximum overhead time taken is around 2.5msec.

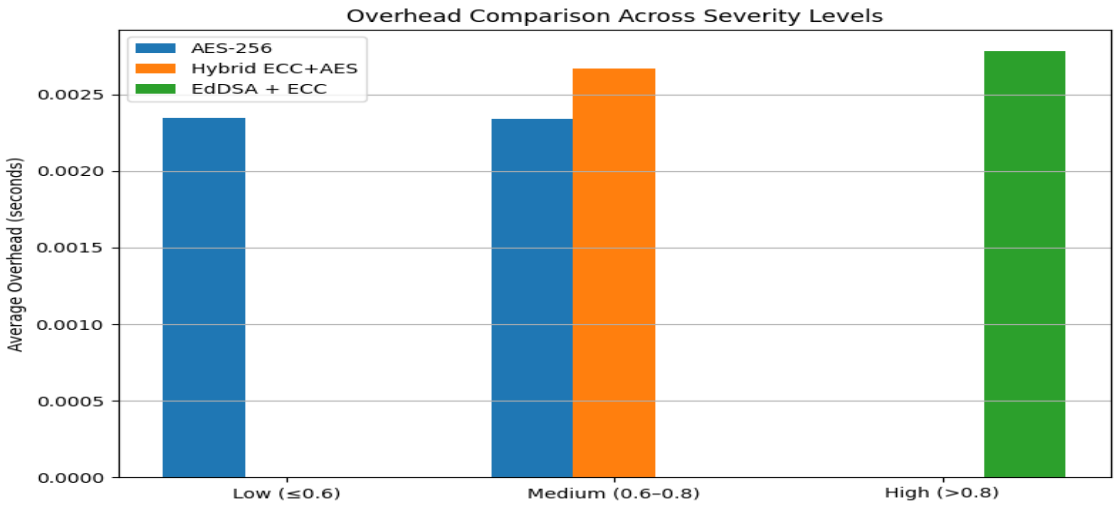

Figure 2a. Average Overhead vs Severity Levels

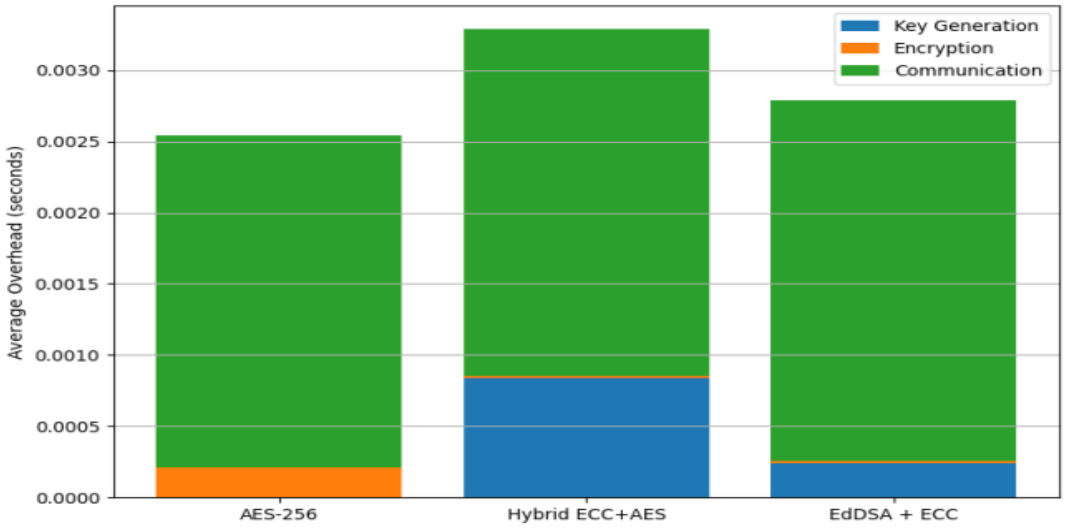

Figure 2b: Overhead for various Cryptographic techniques

Figure 2b depicts the average overhead time for parameters such as key generation, encryption and communication. It can be seen that the key generation time and communication time is more for hybrid ECC and AES cryptosystem as shared key needs to be generated for AES and public key-private key pair needs to be generated for ECC. For the proposed scheme, AES takes more time to encrypt compared to its counterparts.

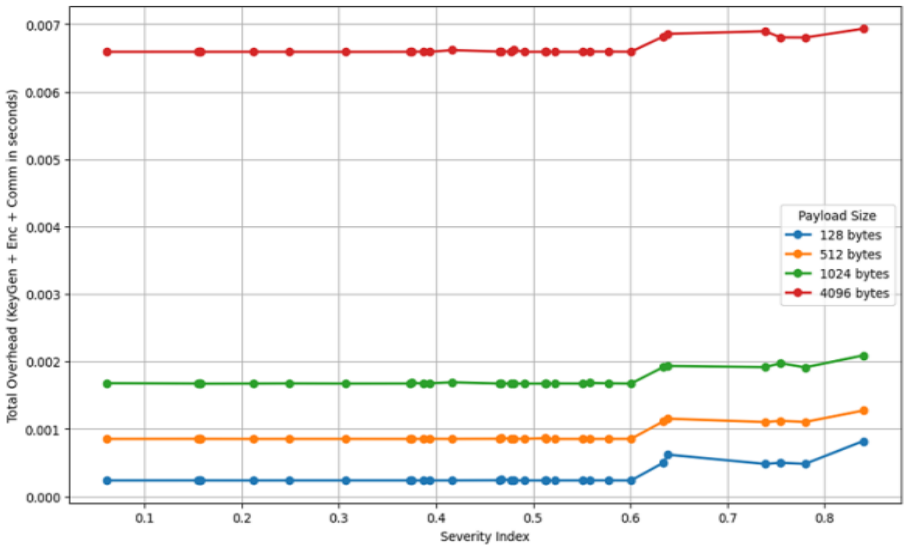

Figure 2c: Adaptive Encryption overhead Vs Security Index;

Figure 2c shows the adaptive encryption overhead for different payload versus severity Index. From the graph, it can be concluded that the overhead almost remains the same for a specific value of payload, even if severity index is increasing.

Discussions:

This work demonstrates the effective balance between security and performance when malware is detected in health care services, as the proposed method is to choose a cryptographic algorithm dynamically by using a light weight AI-based approach. The severity of threat is computed based on the malicious malware, its lateral movement in the network and behavioural anomaly.

AES-256, a shared key cryptosystem is chosen for lowest severity conditions(less than 60%), with dynamic key management techniques. This method results in the lowest overhead, minimal key generation techniques and reduced communication costs.

When the severity level is medium (between 60% to 80%), a hybrid encryption system comprising of ECC and AES is chosen to encrypt the data. This approach increases the overhead as it involves generation of shared key, private-public key pair, stronger security, computation and communication overhead.

As the severity level is high (greater than 80%), digital signature followed by ECC is used. This approach provides highest security ensuring stronger protection under high risk malware attack conditions also by isolating the compromised node.

Overall, the results validate the dynamic selection of the encryption algorithm with key management technique.

Conclusion

Upon detection of malware in an ever demanding un-interrupted health care service, the malware is made inaccessible by hiding the executables. Cryptographic algorithms are chosen dynamically by using an adaptive key management technique. Thus with the help of Machine learning and Artificial Intelligence, the system provides an enhanced service comprising threat detection, automated response and strong cyber security framework.

References

1. Barnaby Fortescue, Edmund Hawksmoor, Alistair Wetherington, Frederick Marlowe, Kevin Pekepok, “Neural Encrypted State Transduction for Ransomware Classification: A Novel Approach Using Cryptographic Flow Residuals”, Cryptography and security, August 2025; arXiv:2502.05341
2. Hamed Taherdoost, Tuan-Vinh, Khadija Slimani, “Cryptographic Techniques in Artificial Intelligence Security: A Bibliometric Review”, Cryptography, MDPI, https://doi.org/10.3390/cryptography9010017
3. K R Kalphana , S Aanjankumar , M Surya , M S Ramadevi , K R Ramela , T Anitha , N Nagaprasad , Ramaswamy Krishnaraj, “Prediction of android ransomware with deep learning model using hybrid cryptography”, Sci Rep. 2024; DOI: 10.1038/s41598-024-70544-x
4. Sehrish Aqeel, Adnan Shahid Khan, Irshad Ahmed Abbasi , Fahad Algarni , Daniel Grzonka, “ Enhancing IoT security with a DNA-based lightweight cryptography system”, Sci Rep. 2025; DOI: 10.1038/s41598-025-96292-0
5. Pramit Kumar Samant , Vinay Pathak , Wakar Ahmad , Abdulatif Alabdultif , “A lightweight trusted framework for secure data exchange and threat mitigation in IoT-enabled healthcare environments” , Sci Rep.2025; doi: 10.1038/s41598-025-22797-3.