Professor Weinstein

HNRS 302

5 April 2024

Selective Literature Review

Introduction

In today's increasingly digital world, protecting our sensitive information and data has become one of the most urgent concerns in the world of cybersecurity. From government records and medical data to cloud storage and financial systems, encryption is the foundation of defense. Widely used algorithms consist of Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES); these algorithms have provided us with robust protection for decades. Often seen as the most crucial cryptographic advancement in decades. However, recent advancements in quantum computing, interconnected devices (IoT/Internet of Things), and sophisticated cyber-attacks are beginning to truly expose the limitations of these traditional encryption models we use today. As a result of this, our static algorithms are struggling to meet the demands of our future landscape.

In response, experts in the field of digital security turned to a recent innovation known as Artificial Intelligence (AI), which is a set of technologies that enable computers to perform advanced functions. Specifically, in the field of AI, Machine Learning, or ML, is a potential solution to these challenges. ML is known as a system that can autonomously learn on its own, which it can do so using extremely large sets of data. Unlike static encryption methods, ML-based systems offer us adaptability, contextual learning, and the ability to recognize patterns within unfathomable amounts of data. These features allow encryption to not only respond to threats, but it allow us the ability to anticipate them, potentially changing the way we defend our systems. Within high-risk environments with little to no margin for error, such as healthcare, IoT,

and finance, ML has the potential to optimize encryption in real-time, increase scale protection according to a system's needs, and enhance randomness in key generation - key components of an adaptive cryptographic defense.

Despite growing interest in ML utilization as a tool for enhancing cryptographic security, the current body of research on ML-enhanced encryption remains fragmented. Some studies only seem to focus on performance metrics, while others examine isolated use cases within a specific sector, creating a large gap in progress for sufficient research and advancements. Very few studies offer us a comprehensive synthesis of how ML contributes across the major functional areas of encryption: key generation, performance optimization, and threat detection. This lack of sophisticated and integrated insight makes it extremely difficult for cybersecurity researchers, engineers, and policymakers to correctly evaluate ML's true impact on modern encryption and see the promise it truly has to offer.

To address this gap, the literature review synthesizes six peer-reviewed studies that explore ML's role. These sources will be organized into three areas of interest: Utilizing Machine Learning to Enhance Encryption Key Generation, Improving Speed and Scalability for Large-Scale Applications, and Enabling Real-Time Threat Detection. This review provides a synthesized view of current research on this promising topic. In doing so, it identifies emerging opportunities in the field of digital security, possible limitations that can recur, and the significance of ML for the future of encryption and cryptography in specific, and simply the entire landscape of data security.

Literature Review

Utilizing Machine Learning to Enhance Encryption Key Generation

Traditional cryptographic key generation methods used in RSA and AES often rely on static algorithms for success. These algorithms cannot adapt to a constantly shifting threat landscape or a diverse operational environment. ML introduces features of adaptability, contextual awareness, and performance-based iteration to the process of key generation. Okdem and Okdem (2023) illustrate a model in which environmental sensor data derived from IoT devices are used as a base, or a "seed," for ML algorithms to successfully generate dynamic cryptographic keys. These keys reflect real-world dynamics and offer higher outputs of randomness, which reduces predictability from outsiders and vulnerability from attacks. While Okdem and Okdem focus on responding to external stimuli, Chaudhary et al. (2022) highlight the true significance of performance-based self-improvement.

These two strategies converge on the value of continuous evaluation in key generation, a fundamental factor in its success and evasive skills from a threat. Rather than relying on fixed sources of entropy, both systems adapt over time, which is done by either sensing a changing environment or learning from an internal simulation within a system. Furthermore, these models are validated by Sayed (2024), whose empirical form of study conducts a comparative analysis. Comparing ML-generated keys against traditional methods. Sayed finds that the keys that utilize the use of ML consistently demonstrate a higher entropy score than keys that use traditional methods. In addition, higher levels of unpredictability and resistance to brute-force attacks by ML-based generated keys were also a key finding of the study. This experimental evidence provides true credibility to the conceptual frameworks offered by Okdem and Chaudhary, showing that ML's theoretical strength translates into proven and measurable security gains.

The integration of these sources within one another reveals that ML enhances key generation successfully, not through a single outlet/mechanism, but by combining content

awareness (Okdem & Okdem), performance optimization (Chaudhary et al.), and empirical verification (Sayed). Together, these sources construct a holistic outlook of intelligence key generation systems, which can adapt to both their performance feedback and their operational context within a system. Thus, this suggests that ML can allow for the development of encryption keys that are not only more randomized to avoid attacks, but also more resilient to current and zero-day threats.

Improving Encryption Speed/Scalability for Large-Scale Applications

Large-scale systems such as financial networks and healthcare infrastructures require encryption systems to maintain high performance while securing vast amounts of sensitive data, emphasizing two major traits of cybersecurity: Integrity and Confidentiality. ML offers promising solutions by optimizing effort, in which the systems choose how and when encryption is applied, allowing systems to safely balance speed and security dynamically, providing a great solution when resources need to be used efficiently. Kour et al. (2024) propose an ML model that uses a Support Vector Machine (SVM) to classify plaintext into a scale of tiers ranked by importance. More important data is assigned heavier encryption and more resources, while less critical information receives a form of lightweight protection. This ML-based strategy reduces overall processing time (speed), while maintaining security in the areas that matter most. Similarly, this approach is echoed by Chinbat et al. (2024), applying a similar logic with IoT healthcare devices. Their study draws attention to the fact that ML enables encryption systems to remain effective even on devices with low processing power, such as wearable health monitors. This is successfully done by the use of ML, allowing for a selective encryption of vital data while reducing computation load somewhere else. While Kour et al. focus on content-aware

prioritization, Chinbat et al. bring in the downfall device-level systems hold, showing how ML can enable adaptable security with resource-aware features even in a hardware-constrained environment.

Asmar, Muath, and Tuqan (2024) build upon both of these models by introducing a component that is based on the concept of time. Their research based in the financial sector demonstrates how ML algorithms can successfully receive a large set of data and successfully patterns of traffic, such as high-volume periods of transactions between two or more parties/ In addition, their research also finds that ML algorithms can reallocate encryption resources accordingly, based on financial events based on real-time. This time-aware prioritization, a key characteristic of ML, enables systems to remain efficient during times of high-stress conditions, a factor not addressed by either Kour or Chinbat et al.. The triad of the three sources presents a compelling strategy that applies multi-dimensionally. Kour provides content-based encryption differentiation, Chinbat applies that same strategy to hardware-constrained healthcare environments, and Asmar, Mauth, and Tuqan introduce the strategy of time-aware elasticity for peak performance.

Together, these sources indicate that ML contributes to encryption scalability by enabling systems to intelligently decide where, how, and when to apply their resources, rather than universally boosting processing speed altogether. In the case of encryption speed and scalability, ML serves as a decision-making filter, granting encryption systems to operate smarter, not harder, valuing power, resources, and most importantly, time. This advancement could potentially fit the puzzle piece of our future, where high-throughput, modern environments depend on resources that are commonly scalable, not defined.

Real-Time Threat Detection and Adaptive Cryptographic Defenses

Now, encryption is simply no longer just a method of securing data, whether in transit or at rest. It must also serve as a dynamic trait of defense in digital security, protecting users against incoming and evolving threats, such as zero-day attacks. ML has to potential to play a critical role in transforming encryption systems into automated security agents, which can detect, learn, and respond to malicious factors in real time. Chaudhary et al. (2022) shed light on embedding ML classifiers within encryption algorithms themselves, to detect weird or abnormal behavior, known as anomalies, during the transmission of data. These classifiers recognize deviations from normal behavior and interrupt the flow of data when a potential threat is suspected or properly identified. To do so, the machine is fed a vast amount of data. This real-time capability of ML-based encryption systems prevents malicious payloads from a foreign threat from successfully reaching their destination, preventing the chance for an attack. Okdem and Okdem (2023) offer a complementary perspective by focusing on intrusion detection systems integrated with ML, which operate at the perimeter—identifying unauthorized access attempts before decryption begins. While Chaudhary targets anomalies during active transmission, Okdem emphasizes early-stage defense, thereby creating a multi-layered strategy.

To expand, Sayed (2024) presents encryption systems that evolve based on previous attack patterns. With research suggesting that ML allows cryptographic protocols to "learn," like a human, from breaches and attempted attacks, improving the system's resilience proactively. Collectively, Okdem and Okdem (2023) focuses on early-stage threat detection along with Sayed's emphasis on systems that learn from past attacks, whether successful or not, show how ML can strengthen encryption at the initial point of entry and over time, successfully combining the advantage of immediate defense with the power of conservative long-term adaptation.

In the same scope of the research from Sayed (2024), Asmar, Muath, and Tuqan (2024) further signify the value of adaptive models with integrated ML through their research of failed decryption attempts regarding digital banking systems. Their findings suggest that ML can detect trends across multiple attacks and reconfigure encryption protocols, and preemptively block potential vulnerabilities, successfully detecting any chase of threat. Together, the two sources collectively highlight the benefit ML can potentially offer in the real world in regards to threat detection, and the essential human-like features it has in digital security, while Sayed emphasizes ML's ability for continuous evolution after attacks, Asmar, Muath, and Tuqan focuses on ML's ability to successfully detect threats to shape future defenses before new attacks occur.

It becomes clear that ML has the potential to change how encryption functions within the entire landscape of digital security. Rather than solely relying on fixed rules, a strategy we currently use, ML-driven systems combine real-time detection (Chaudhary), preventative blocking (Okdem & Okdem), post-breach adaptation (Sayed), and predictive defense modeling (Asmar, Muath, and Tuqan). The collective outcome consists of a security system so layered that it doesn't just respond to attacks, it actively prepares for them with respect to time. In doing so, ML flaunts its potential to the world from being able to act as a static gatekeeper, to a dynamic learning system capable of self-improvement and resilience without the need for manual input.

Conclusion

The research question that guides this study - *How can machine learning enhance encryption algorithms to improve cryptographic performance and security for protecting sensitive data?*-emerges from a growing body of literature on cryptographic innovation, AI, and cybersecurity resilience. The scholarship reviewed above demonstrates that ML offers a

compelling tool for enhancing encryption systems by enabling adaptability, real-time decision making, and intelligence recognition of patterns within large sets of data. While existing studies explore the use of ML in specific cryptographic tasks and instances, such as key generation, lightweight encryption regarding IoT, and intrusion detection systems, less attention has been paid to how these contributions intersect with each other across the broader landscape of encryption systems. This important gap in the literature prompts the current investigation, with the objective being not only to dive deeper into a variety of real-world, individual use cases, but to examine how ML fundamentally reshapes the world of encryption from static protection to another form of dynamic, intelligent defense, almost changing what encryption is entirely.

This research builds on established accredited work in the landscape of AI and cybersecurity by connecting advances in ML to enduring challenges in the real-world of encryption: speed, scalability, and real-time adaptability. However, this research strays away from prior research by integrating many factors of cryptographic function, offering a layered approach rather than just a single use case, bringing together scholarship that addresses performance, key generation, and adaptive threat detection and mitigation under one holistic view. Investigating ML's role in transforming encryption holistically may reveal how intelligent systems can scale across a variety of industries while improving overall system resilience. This ability to be applied to a broad set of frameworks rather than just a single sector could be the single most important stepping stone into the future of encryption. With the proposal in question and analyzing the current scholarship to properly address it, this research seeks to contribute to a larger conversation about the future of data protection. It presents a serious question and time-demanding inquiry on how ML might not just support, but entirely redefine encryption, laying a foundation for next-generation cybersecurity frameworks.

References

Asmar, Muath, and Alia Tuqan. “Integrating machine learning for sustaining cybersecurity in Digital Banks.” Heliyon, vol. 10, no. 17, Sept. 2024, https://doi.org/10.1016/j.heliyon.2024.e37571.

Brakerski, Zvika, et al. “Quantum Attacks on Classical Encryption and the Need for Post-Quantum Cryptography.” Communications of the ACM, vol. 65, no. 3, 2022, pp. 78–85. https://doi.org/10.1145/3494123.

Chaudhary, Shubham, M. Raj, A. Saini, and R. Singh. “Machine Learning and Applied Cryptography.” International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 6, no. 1, 2022, https://www.researchgate.net/publication/358180724.

Chinbat, Tserendorj, et al. “Machine learning cryptography methods for IOT in Healthcare.” BMC Medical Informatics and Decision Making, vol. 24, no. 1, 4 June 2024, https://doi.org/10.1186/s12911-024-02548-6.

Kour, Ravi, A. Tiwari, R. Sharma, and M. Singh. “A Fusion of Machine Learning and Cryptography for Fast Data Encryption through the Encoding of High and Moderate Plaintext Information Blocks.” Multimedia Tools and Applications, vol. 83, no. 4, 2024, pp. 10765–10791. https://doi.org/10.1007/s11042-024-18959-6.

Okdem, Selcuk, and Sema Okdem. “Applications of ML-Based Cryptography in IoT Security Systems.” Applied Sciences, vol. 13, no. 2, 2023, p. 1111. https://www.mdpi.com/2076-3417/13/2/1111.

Sayed, Md Abu. “A Comparative Study of Machine Learning-Based and Traditional Cryptographic Methods for Personal Data Encryption.” Journal of Information Security and Applications, vol. 76, 2024, p. 103837. https://www.researchgate.net/publication/386989160.

Tucker, Carolyn C., and C. Edward Chow. “Ethical Considerations in the Use of AI for Cybersecurity.” Journal of Information Ethics, vol. 31, no. 2, 2022, pp. 75–89. https://doi.org/10.3172/JIE.31.2.75.

World Economic Forum. “Cybersecurity and AI: The Perfect Pairing or a Double-Edged Sword?” World Economic Forum, 21 Sept. 2023, https://www.weforum.org/agenda/2023/09/cybersecurity-ai-risks-opportunities/.