Chapter 6
A Survey of Machine Learning and Cryptography Algorithms

M. Indira
P.K.R. Arts College for Women (Autonomous), Gobichettipalayam, India

K. S. Mohanasundaram
P.K.R. Arts College for Women (Autonomous), Gobichettipalayam, India

M. Saranya
P.K.R. Arts College for Women (Autonomous), Gobichettipalayam, India

ABSTRACT

The intersection of machine learning and encryption has emerged as a key area in technology. A model shift in technology and data security has brought the combination of machine learning and encryption. In order to provide insight on the underlying algorithms and techniques, this survey was taken between the domains. It presents an overview of machine learning and cryptography algorithms. A wide variety of algorithms are examined in the field of machine learning. This survey also clarifies the interaction between machine learning and cryptography, demonstrating how these two fields work together to produce privacy-preserving ML, secure authentication, anomaly detection, and other benefits. A new era of data privacy and security has methods like secure multi-party computation (SMPC) and homomorphic encryption, which allow calculations on encrypted data. An updated overview of machine learning techniques used in cryptography is presented in this survey. The report offers recommendations for future study initiatives and summarizes the work.

INTRODUCTION

The integration of machine learning (ML) with encryption has caused an unprecedented shift in the field of modern technology, opening up previously unheard-of opportunities in the areas of security, privacy, and data-driven insights. Combining the strong principles of cryptography with machine learning's capacity to identify patterns and extract useful information from large datasets creates a potent coalition

DOI: 10.4018/979-8-3693-1642-9.ch006

against new threats and difficulties. The domains of privacy preservation, secure model training, and better adversarial resilience are undergoing significant changes due to this mutually beneficial interaction (Biggio et al., 2023).

In almost every industry conceivable, the modern community has incredible access to cutting-edge hardware and software at a pace that is unparalleled. On the other hand, this has given rise to an entirely new set of security and privacy risks. As a result, it is imperative to address the security and privacy aspects of various cyberthreats, which are growing dramatically faster than before due to undiscovered malware. More than 10 billion of the world's people, according to a special report, depend upon mobile phones or other smart devices for banking, shopping, financing, healthcare, blockchain applications, social media posts, and professional information and updates.

Therefore, there is a good probability that data will be hacked or disclosed when downloading apps on smart devices. In addition, malicious software can be activated via faulty system processes, unapproved network entry, and the collection of private data. Numerous anti-virus programmes, intrusion detection systems, defenders, and the most recent firewalls with security updates are available to address these problems.

Enormous search areas and handling enormous amounts of data are two commonalities between encryption and machine learning (ML). While machine learning (ML) has long been used in cryptography, given the daily cohort of over 5 quintillion bytes of data, ML approaches are now more pertinent than ever. In order to continuously learn from and adapt to the massive quantity of data being provided as input, machine learning (ML) typically automates the creation of analytical models. The relationship between the input and output data produced by cryptosystems can be shown using machine learning techniques.

To generate the private cryptographic key, machine learning techniques like boosting and mutual learning can be applied. Classification techniques like naive Bayesian, Artificial Neural Networks, support vector machine, and AdaBoost can be applied to categorise objects and encrypted traffic into steganograms that are utilised in steganography. In addition to being used in cryptography, the art of building safe systems for encrypting and decrypting private information, machine learning techniques can also be used in cryptanalysis, the art of cracking cryptosystems to carry out specific side-channel attacks.

The ways in which cryptography and machine learning differ and are similar show how one discipline can affect another. Cryptography and machine learning have attracted a lot of interest. Generally speaking, cryptanalysis and machine learning share more similarities than does machine learning and cryptography. This is because their shared goal searching across expansive search spaces is the reason for this. The goal of a cryptanalyst is to decipher the correct key, but the goal of machine learning is to select an appropriate answer from a wide range of potential answers. Over the past few years, applications of various machine learning approaches have drawn increasing attention.

There are other study fields as well, such as machine learning modification to mislead its application to incorrect classification, quantum machine learning, and privacy preservation. The fields of machine learning and cryptography mutual research are not new. The computational complexity of machine learning and its computational components were covered by Kearns in his dissertation. This research cleared the path for further machine learning and cryptography research. Machine learning has several uses in the field of information and network security, in addition to cryptography and cryptanalysis.