

RESEARCH ON ARTIFICIAL INTELLIGENCE APPLICATIONS IN CRYPTOGRAPHY WITH AN ANALYSIS IN VULNERABILITIES DETECTION MANAGEMENT

¹V.Esther Jyothi, ²V.Madhu Latha, ³D.S.B.Bharathi

¹Assistant Professor, Department of Computer Applications, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, India, vejyothi@vrsiddhartha.ac.in

²Assistant Professor, Department of Business Management, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, madhulathav@vrsiddhartha.ac.in

³Professor, PG Department of management studies, The Hindu College-MBA, Machilipatnam

Abstract: The paper examines several recent developments in artificial intelligence-based cryptography. It looks at how Machine Learning can be used to evaluate and encrypt data in particular. Artificial Neural Networks (ANNs) and the concepts of Deep Learning using Deep ANNs are briefly discussed. The aim of this paper is to provide an overview of how AI can be used to encrypt data and perform cryptanalysis on such data and other data types in order to determine an encryption algorithm's cryptographic power.

Keywords: Artificial Intelligence, Machine Learning, Deep Learning, Artificial Neural Networks, Cryptography

I. INTRODUCTION

Artificial intelligence (AI) is a term used to describe a set of methodologies and applications that allow a computer to perform tasks that would normally require human intelligence. AI refers to a digital computer's or a computer-controlled robot's ability to perform tasks normally associated with intelligent beings [1].

This paper aims to provide an overview of such applications with an emphasis on cryptography, as well as citations to more technically based papers that are relevant to the subject. This article concentrates on the use of Artificial Neural Networks to produce non-linear ciphertext that is unique and unclonable.

II. MACHINE LEARNING

Pattern detection is the most common problem that machine learning is used to solve. This is when a large dataset of potentially abnormal patterns in a signal or picture, for example, needs to be broken down into common features and/or segments that can then be identified in a predetermined manner.

The rationale of the decision-making process can be rendered softer by making the threshold conform to the demarcation of such input metrics in terms of their known precision, quantity, and other prior knowledge. The foundations for the development and implementation of Artificial Neural Networks are Fuzzy Logic Systems. An ANN usually improves the precision of pattern classification decisions beyond what can be achieved by traditional data categorization.

III. ARTIFICIAL NEURAL NETWORKS

Artificial Neural Networks function by feeding them a set of metrics that are assumed to be a composite representation of the data, metrics that are computed by transforming the data into a feature vector. The significance of each component of this vector is then calculated using a weight w , and the weighted components are combined to produce a single output value.

The ANN generates an output in reference to a choice process by adjusting the values of these weights. Figure 1 is an illustration of a data transfer method that incorporates several inputs into a single output [1]. By inputting a similar set of weighted feature vectors or modifying the components of the vector that are input, it can be repeated to generate a variety of different outputs.

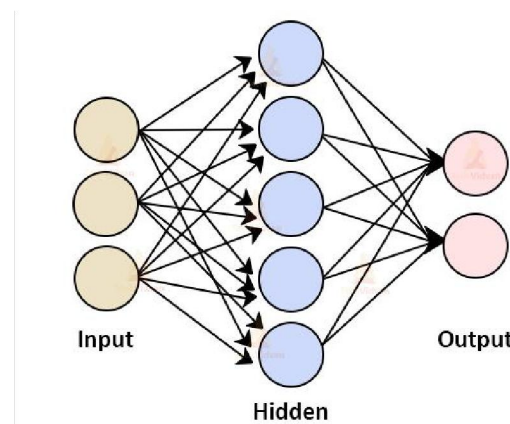


Figure 1: Artificial Neural Network Architecture

The computations involved in moving information from the hidden layer to the output layer are believed to require a numerical value adjustment for all or any of the applied weights. The use of Python programming to build AI systems is becoming more popular. Regardless of the framework, programming language, or toolbox used, the architecture of a network is critical and must be optimised to maximise the use of AI with an ANN for a particular problem. The quality and quantity of the training data are particularly important. This determines the accuracy of the weights, which can be thought of as the network's keys to future operation, along with the network's architecture. The encryption algorithm for generating an output cipher text that can then be used to encrypt plaintext data has an obvious application in cryptography, where the weights are identical to the keys and network architecture.

IV. ARTIFICIAL NEURAL NETWORKS AND DEEP LEARNING

It is common practise to first process the data in order to produce a feature vector containing metrics that are thought to be a fair representation of the data's critical characteristics, such as a digital signal. As shown in Figures 2 and 3, the number of nodes in the input layer becomes relatively small in comparison to the original data, i.e. the length of the digital signal. This is critical when it comes to making the most of the limited computational power available to 'drive' an ANN and generate a fast decision-making method.

The size of the feature vector is determined by the feature vector's size and the elements it contains, which should preferably be much smaller than the original data from which it was built using a variety of signal or image processing algorithms to produce precise metrics. The computing time needed to compute the feature vector in comparison to the time required to train the ANN is an optimality problem that must be considered.

The rise in processing power that has enabled a deep learning paradigm to emerge is primarily driven by companies like Facebook and Google, as well as national security agencies concerned with issues like face recognition and track and trace.

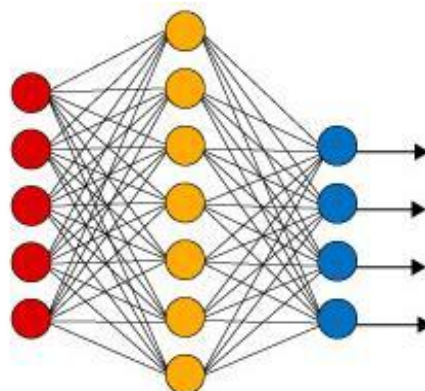


Figure 2: Simple Neural Network

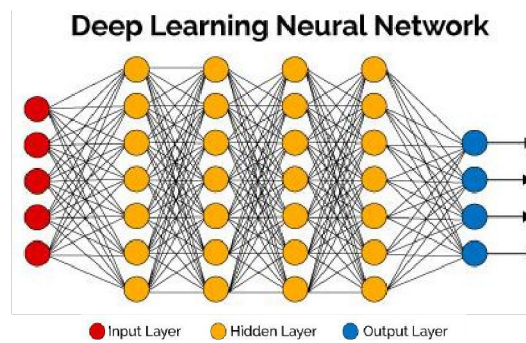


Figure 3: Deep Learning Neural Network

ANNs need real-world data to function in real-world settings, regardless of the processing power available. While the introduction of access to big data has addressed this need, such data may be unavailable or absent from current data fields in certain cases. Deep learning solutions for complex pattern recognition problems are critical for the future growth of many technologies, programming environments, functions, and structures, all of which are rapidly evolving.

V. ARTIFICIAL NEURAL NETWORKS AND CYBER SECURITY

Cyber security refers to a collection of techniques for safeguarding data formation, analysis, preservation, and transmitting over an open network like the Internet. Infection of files by a virus designed to covertly penetrate a single computer or a network of computers is a well-known example of this. To evade detection, computer viruses have become more sophisticated and run in stealth mode. Every day, new viruses are created. To escape detection, many of these viruses simply alter their appearance and signatures, but their operation and method of infecting files and systems remain the same. This opens up the possibility of learning ANNs on a variety of known viruses, assuming that their digital signatures can be detected by inspecting future data streams and new files [1] and [3].

VI. ARTIFICIAL NEURAL NETWORKS AND CRYPTOGRAPHY

One of AI's most important characteristics is its ability to identify trends in large amounts of data. The aim of cryptography is to maximise the diffusion and uncertainty that comes with converting plaintext to cipher text. The encrypted data – the cipher text – could, in theory, be completely pattern-free. The cipher text must be a complex randomised representation of the plaintext, which is generally associated with the use of a one-way function with no inverse solution. This opens up the possibility of using AI in the development of ciphers, their classification and cryptanalysis of encrypted data.

Since cryptography relies on the generation of a random number field (the cipher) to convert plaintext into ciphertext, let's seed a network with a few random numbers and then train it with a real source of noise, allowing the weights to be changed so that the network produces a fairly accurate simulation of the target random data field. The initial random numbers and weights represent the key(s) required to replicate the random number field that can be used to encrypt and then decrypt the data in this case, since the network architecture is known to two interacting entities.

The encryption/ decryption algorithm is similar to the network architecture. In this way, a small number of random elements in the input function vector can be used to generate the cipher's random number field. This is based on the use of Evolutionary Computing, a machine learning technique that can be used to generate a nonlinear equation that, upon iteration, can create a random number field, with the (conventional) key as the initial condition of the iterator.

Cryptographic algorithms are used to ensure data confidentiality, integrity and authenticity with only the sender and receiver of an encrypted message having access to the original data. Today, cryptographic security is determined by the key's resistance to attacks rather than the algorithm's secrecy; that is, the encryption key is unknown but the algorithm's method is well-known. There are many such algorithms with various implementations, some of which are more common than others due to their ease of implementation or efficiency [9]. Despite widespread knowledge of algorithm implementation, cracking the code is neither easy nor fast.

The first step is to figure out the encoding algorithm, and once that's done, the only way to get the original data is to use cryptanalysis to crack the cipher. As a result, even a simple cryptanalysis is a major undertaking. There are, however, smaller and more complex reduced activities that, when combined, which enable the task to be completed successfully: determining the cypher size, retrieving the cipher key, determining the form of encoding used for cyphering, and retrieving the encryption algorithm. This research focuses on classifying cryptograms by data mining to identify algorithms used for encoding plain texts.

Since DES was vulnerable to brute force attacks and other cryptanalysis techniques, the Blowfish algorithm was proposed as an alternative. Since Blowfish was designed to replace DES, some research has focused on comparing the two algorithms. RSA has been used for medical image encoding and decoding as well as a hybrid Bluetooth communication algorithm.

Data mining is a technique that employs a number of algorithms to extract relevant patterns from large datasets that may be useful in decision-making. The classic C4.5 decision tree data mining algorithm and two pruning methods are available to minimise time complexity. The Multilayer perceptron, on the other hand, is a well-known neuron network classifier. It has an input layer, intermediate layers, and an output layer, with a supervised classificatory training step and back propagation as a form of error minimization.

The National Institute of Standards (NIST), Computer Security Resource Center, offers a Cryptographic Algorithms Validation Program [4], which involves checking new PRNGs [5], in addition to any function being evaluated against the checks shown in Figure 4 and Figure 5. These NIST tests are an international standard for evaluating a cipher's cryptographic strength and are necessary when using a cryptographic algorithm.

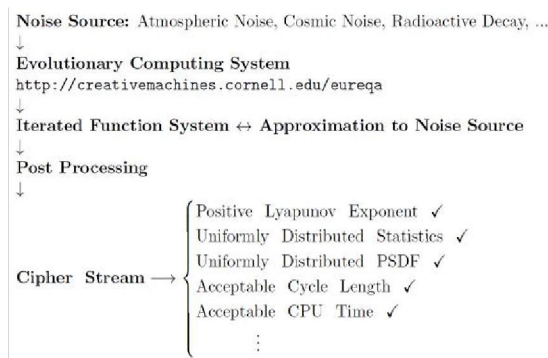


Figure 4: The process for evolving a cipher text using EC

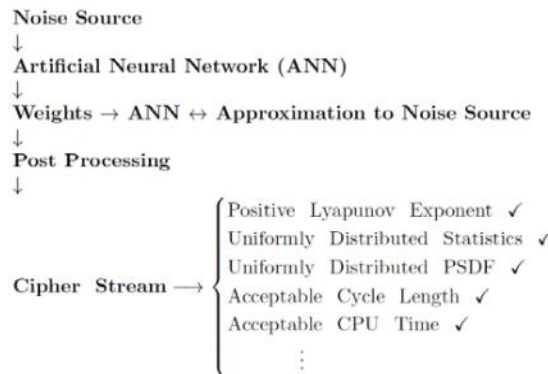


Figure 5: The process for generating a stream cipher using an ANN.

VII. RESULT AND CONCLUSION

Since software quality is so critical in application development, many tools have been developed to ensure that the applications developed are of high quality. Figure 6 shows detailed performance-based comparison of various vulnerability detection methods.

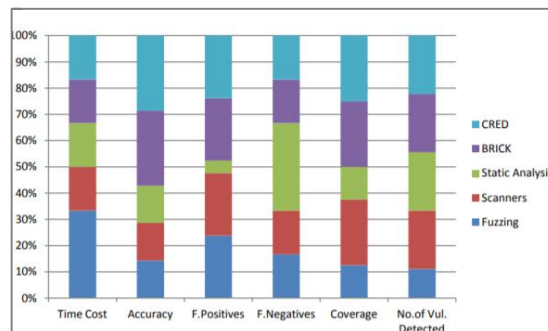


Figure 6: Comparison of vulnerability detection methods

The aim of this paper is to provide a broad overview of how artificial intelligence is being used to develop encryption algorithms and cryptanalysis as well as how ANNs can be equipped to model chaos as a supplement. Using the IoT and a widely used communications device, such as the mobile, AI can be used to produce encrypted data for authentication. Of course, there are many more applications of machine learning in cryptography than those discussed in this article [6], [7]. Figure 7 presents different AI techniques used for vulnerabilities detection with their goal.

Reference	Goal	AI Techniques
(Richardson et al., 2010)	Limits of automated fingerprinting for OS	Decision tree, rule learner, SVM-SMO, instance-based clustering
(Peng et al., 2012)	Score and rank risks of Android apps	Naive Bayes, Probabilistic generative model
(Rasthofer et al., 2014)	Identify sources and sinks from code of any Android API	Linear SVM
(Mokhov et al., 2014)	Identify bad coding practices	NLP, Modular A* Recognition Framework
(Yamaguchi et al., 2015)	Infer vulnerability search patterns in C code	Complete-linkage clustering
(Liu et al., 2015)	Predict future data leak instances from network logs	Random Forest
(Blum et al., 2017)	Improve fuzzing of inputs	Neural network
(Shoshitaishvili et al., 2018)	Discover vulnerabilities in binary code	Symbolic execution and fuzzer

Figure 7: AI Techniques for vulnerabilities detection

Current encryption algorithms, protocols, and standards associated with information and cyber security are expected to change dramatically in the near future as a result of complementary technologies such as advances in DNA computing [8], deep learning, and quantum computing. Furthermore, a much wider global scope of society will be involved in the study, growth, and management of these changes.

VIII. REFERENCES

- [1] Jonathan Blackledge and Napo Mosola; Applications of Artificial Intelligence to Cryptography, Transactions on Machine Learning and Artificial Intelligence, Volume 8 No 3 June, (2020);
- [2] Maghrebi, H., Portigliatti, T., Prouf, E., Breaking Cryptographic Implementations Using Deep Learning Techniques, Security, Privacy, and Applied Cryptography Engineering (SPACE), 6th International Conference, 2016. [Online] Available from: <https://eprint.iacr.org/2016/921.pdf>
- [3] Bezobrazov, S., Blackledge, J. M. and Tobin, P., Cryptography using Artificial Intelligence, The International Joint Conference on Neural Networks (IJCNN2015), Killarney, Ireland, 12-17 July, 2015.
- [4] Blackledge, J. M., Bezobrazov, S. Tobin, P. and Zamora, F., Cryptography using Evolutionary Computing, Proc. IET ISSC2013, Letterkenny, Co Donegal, Ireland, June 20-21, 2013 (Awarded Best Paper Prize for ISSC2013). <https://arrow.tudublin.ie/aaconmuscon/5/>
- [5] NIST, Cryptographic Algorithm Validation Program (CAVP), 2020, [Online] Available at <https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program>
- [6] Open Quantum Safe Project, Software for Prototyping Quantum Resistant Cryptography, 2016. <https://openquantumsafe.org/>
- [7] Stamp, M., Introduction to Machine Learning with Applications in Information Security, Chapman & Hall/CRC Machine Learning & Pattern Recognition, 2018. ISBN-13: 978-1138626782.

- [8] Alan, M. M., Applications of Machine Learning in Cryptography: A Survey, 2019. <https://arxiv.org/pdf/1902.04109.pdf>
- [9] Nandkumar Niture, Machine Learning and Cryptographic Algorithms – Analysis and Design in Ransomware and Vulnerabilities Detection, 2020. EasyChair-Preprint-3207.pdf

IX. AUTHORS PROFILE



She has 15
Professor,
Siddhartha

Dr. V. Esther Jyothi was awarded Ph.D from Rayalaseema University and M.Tech from JNTUK, Kakinada. She has 14 years of teaching experience. At present, she is working as Assistant Professor, Department of Computer Applications, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada. Her area of interest include Machine Learning and Network Security.



University, Machilipatnam, MBA
M.Com from Andhra University,
experience. At present she is
College-MBA, Machilipatnam.

Dr. V. Madhu Latha was awarded Ph.D. from Krishna University, Machilipatnam and MBA from Acharya Nagarjuna University, Guntur. years of teaching experience. At present, she is working as Assistant Department of Business Management, Velagapudi Ramakrishna Engineering College, Vijayawada.



Dr. D.S.B. Bharathi was awarded Ph.D from Krishna from Acharya Nagarjuna University, Guntur, and Visakhapatnam. She has 17 years of teaching working as professor and principal for The Hindu