International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 SJIF 2023: 8.176 ISSN: 2582-3930

Detecting the Security Level of Various Cryptosystems Using Machine Learning Models

H.K Shashikala[1], Nallani Ashok kumar[2], K Jayanth[3]

[234]7 B.Tech 4th Year, CSE, Jain University, Bengaluru 562112, Karnataka, India.
[1]Associate Professor, CSE, Jain University, Bengaluru, 562112, Karnataka, India.

Abstract

Recent advances in multimedia technology have increased the need for digital data security. Researchers typically focus on changing current practices to address system security vulnerabilities. However, the security of critical data is seriously compromised by a number of proposed encryption algorithms that have proven weak over time. Using the right encryption technique is essential, but the type of data you want to protect will determine which algorithm is best for your particular situation. However, comparing different cryptosystem solutions individually can be a time-consuming process. Our technique uses support vector machines (SVMs) to assess the security level of image encryption. Choose the right encryption method quickly and securely. This effort also produces a dataset containing standard cryptographic security metrics such as entropy, contrast, uniformity, peak signal-to-noise ratio, mean squared error, energy, and correlation. These features were assembled from a series of scrambled images. Record labels are divided into three classes based on the level of security they offer.

Their accuracies were calculated to assess the performance of acceptable, well-performing, and bad recommendation models, and the results showed how effective his SVM-based system was.

Key Words: security analytics, image encoding, support vector machines (SVM), and cryptosystems

I. INTRODUCTION

The exponential growth of multimedia data transmission over insecure channels, especially the Internet, has made security an important research topic. Many experts have worked on developing new encryption techniques to protect data from hackers and rogue users. Two elements, he said, are essential to the scrambling of a digital image: scattering (also called scrambling) and confusion. According to Claude Shannon's theory, cryptosystems that use scrambling and spreading techniques are considered secure. A digital image can be scrambled directly on pixels or scrambled on rows and columns, but diffusion modifies the original pixel values. In other words, during the replacement process, individual pixel values are replaced with S-eigen box values. However, to protect your privacy, your data will only be sent in encrypted form. Due to the low security level of the encryption process, the data can be read by unauthorized persons even after it is available in encrypted form. Image durability is greatly affected by the security level of the cryptographic algorithms used for encryption. Simple photos are fully encrypted using strong encryption technology to prevent attacks on availability, confidentiality and integrity. Security and time complexity should also be considered when choosing an encryption method. Different types of data have different security priorities, so the type of application you are encrypting determines which encryption method to use. This section introduces a method for evaluating the security of an image encryption system

II. LITERATURE REVIEW

[1] Automatic Detection and Classification of Cryptographic Algorithms in Binaries Using Machine Learning, written by Diane Duros Hosfelt.

In this study, we looked into how to identify and categories cryptographic methods in compiled code using feature extraction and machine learning models. Using four different feature sets and four different learning techniques, we assessed three various model types. Although decision tree models have been found to perform best on this data, his SVM with linear kernel outperforms decision tree models in terms of generalization to real-world data. I can. The system correctly classifies and detects >95% of relatively small and homogeneous samples, according to cross-validation results.

[2] Workarounds for machine learning and security applications developed by Ramani Sagar 1, Rutvij Jhaveri 2, and Carlos Borrego 3.

Because machine learning in security applications depends so heavily on the quality of the data, emerging cyberthreats could harm the infrastructure that stores vital data. The difficulty of detecting opponent samples by gathering and forecasting enemy samples is faced

when using machine learning-based techniques in security applications. This leads us to the conclusion that both designers and attackers will use the new model as a research tool. The security of machine learning-based decision-making systems in hostile contexts opens the door to new study areas as security incidents develop quickly. Malicious users occasionally simply boost the false negative rate while lowering the false positive rate accordingly, maintaining a consistent total mistake rate and enabling the attack to go undetected. This makes it possible for attackers to launch complex attacks. To accurately identify attacks on ML-based systems, this sort of issue needs to be looked at. Regardless of the privacy sector, significant improvements in current privacy protection techniques suffer from subpar performance since machine learning algorithms use complex operations with several parameters. As a result, we ought to think of really effective strategies for protecting privacy in a hostile setting. This finding revealed a pertinent trade-off between machine learning classifiers' accuracy and scalability. For instance, informal security application judgements regarding when to employ which strategy. However, this does not guarantee that the classifier's accuracy will finally attain precise accuracy, especially in the case of weak labels. Therefore, adding people or using transfer learning to make more changes is worthwhile. in this manner The essential question is which machine learning algorithms are secure in this way that can balance three aspects: performance cost, security optimization, and performance generalization. Decisions are made through experimentation. should be planned and constructed.

[3] Federated Machine Learning for Secure and Privacy-Preserving Medical Imaging Marcus R. Makowski, Daniel Rückert, Rickmer F. Braren, and Georgios A. Kaissis
Artificial intelligence (AI)-based methods have the potential to completely change the medical sector. As an example, medical image processing has seen the effective application of computer vision techniques, traditional machine learning, and more recently deep neural networks. There have been many published large curated picture corpora; picture Net is likely the most well-known. More oncology-related studies and applications, as well as potent pre-trained algorithms that facilitate transfer learning, have resulted from this. cancer identification, genomic characterization, cancer subtyping, stage prediction, outcome risk assessment, and recurrence risk calculation are applications in non-oncological disciplines.

[4] Ransomware and Vulnerabilities Detection Using Machine Learning and Cryptographic Algorithms.
In order to develop new models to defeat encryption and avoid paying ransom fees, this white paper proposes a machine learning approach for novel ransomware detection and random number decryption strategies. The study also suggested categorizing the infected files so that the system could distinguish between them using the model it trains. The primary issue is structurally broken down into three smaller issues: identifying ransomware issues, developing machine learning-based encryption techniques, and creating decryption keys for ransom issues. 8 Apr 19, 2020 Ransomware and Vulnerability Detection Using Machine Learning and Cryptographic Algorithms My continued work will revolve towards producing outcomes and accuracy for the research-related algorithms I'm working on.

[5] Using Deep Learning and Machine Learning Algorithms to Predict DDoS Attacks B. RamaSubba Reddy, A. Suresh Babu, and Saritha.
This article provides a comprehensive assessment of the research on machine learning and deep learning methods for Dodos attack detection and prediction. 34 articles are chosen for this study's investigation following a laborious sifting process. Due to computational complexity, it turns out that the majority of current research uses answers and algorithmic patterns based on statistical algorithms. Additionally, there aren't many publications that cover DDoS forecasting. The integration of several DDoS attacks and countermeasure methods is reviewed in this paper. This makes it simple for researchers of the next generation to solve knowledge gaps in the use of machine learning algorithms to automate DDoS attack prediction in various dispersed networks.

III. PROPOSED MODEL

Numerous new cryptographic algorithms, including chaos- and transform-based ones, have been developed recently. We found that several of the existing encryption methods were unsecure and did not offer enough security when we looked at the statistical outcomes of such techniques. One method for figuring out the security level of a cryptographic algorithm is to analyze the statistics of its security parameters. Performing these comparisons one at a time is common for traditional approaches to accomplish this, which takes time. In order to make the process of selecting the best encryption method for you faster, we created a machine learning model that combines SVMs.

Advantages:

- The accuracy has increased.
- Reduce the complexity of time.

- Automate the procedure for determining a cryptographic algorithm's level of security.

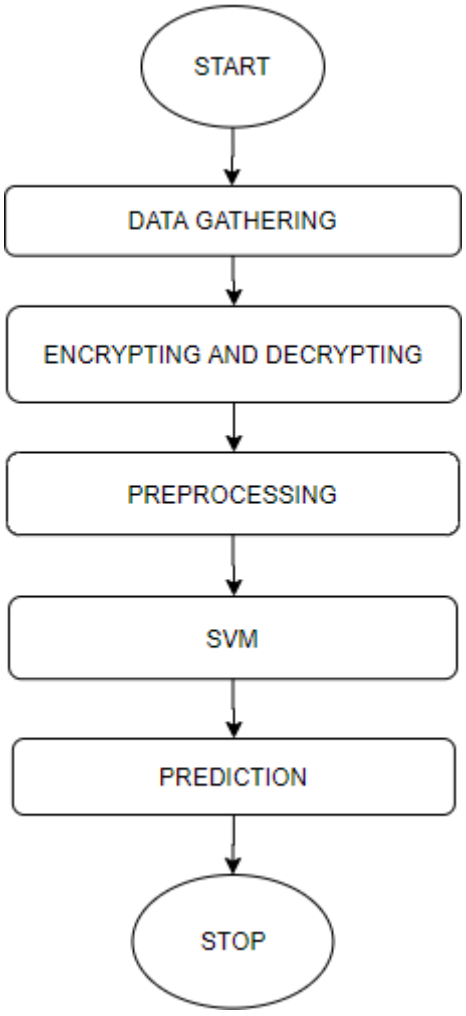

Fig: Block Diagram

IV. METHODOLOGY AND ALGORITHMS:

1. Support-vector machine

Pillar Vector Machine, a supervised learning model, uses a learning approach to examine data for machine learning classification and regression analysis. SVM is based on statistical learning framework and he is one of the most reliable forecasting methods. The SVM training method creates a model that classifies fresh samples into one of two groups and a non-probabilistic binary based collection of training samples. Each sample is labelled as belonging to one of two categories. Create a linear classifier. By assigning training patterns to positions in space, SVM maximizes the distance between her two categories. New samples are projected to fit in the same space depending on which side of the gap they are on specific category. Technically, an assisted vector machine creates one or more hyperplanes in a high- or infinite-dimensional space that can be used for further tasks such as classification, regression, and outlier identification. It is logical that the feature edge or hyperplane in each class furthest from the nearest training data point provides effective separation. This is because the generalization error of the classifier decreases as the margin size increases. The original problem is represented in a finite-dimensional space, but the component sets in this space are typically not linearly separable. This led to the proposal to move the first finite-dimensional space to the next domain. It has a much higher number of dimensions and is probably easier to separate. SVM schema mapping aims to define the SVM schema in terms of kernel functionality. You can quickly compute the dot product of pairs of two input data vectors with respect to the variables in the original space.

2. DNA encoding

In DNA computing, molecular biology, biochemistry, and DNA are replacing traditional silicon-based computing technologies. An interdisciplinary subject called bimolecular computing, also known as DNA computing, is exploding in popularity. Rapid advances in DNA computing have enabled researchers to create multiple biological and algebraic operations based on his DNA sequence [13]. A single strand of DNA is made up of four nucleotides: A, C, G, and T. A and T, C and G complement each other. Modern computer theory uses binaries to represent all information. However, DNA code theory uses DNA sequences to represent information. Thus, 2-bit binary values are used to represent the four bases in a DNA sequence in binary form base. Binary theory says that 0 and 1 are complementary, so we know that 00 and 11 and 01 and 10 are also complementary. There are four different ways to encode the four bases, represented by the numbers 00, 01, 10, and 11. = 24. Since DNA bases complement each other, only 8 of the 24 possible code combinations satisfy the principle of complementary base pairing.

3. Logistic Map

A common classic example of how complex and chaotic behavior can arise from very simple nonlinear dynamical equations is the logistic map, or second order polynomial map (or iteration relation). Biologist Robert May, in his 1976 paper [1], popularized this map by using it as a discrete-time demographic model comparable to Pierre-François's Verst's logistic equation. According to this nonlinear difference equation, the population is still small, but reproduction increases it in proportion to the current population. Hunger (density-dependent mortality) where the growth

rate is reduced by the assumed 'carrying capacity' of the environment minus the current population. However, as a population model. The main problem with logistic maps is that certain initial conditions and parameter values can lead to negative population numbers, such as when r > 4. The previous Ricker model also exhibits chaotic dynamics, but does not suffer from this problem.

4. Rubik's Cube Image Encryption

This program uses the Rubik's Cube idea to rearrange the pixels of an image. Using the XOR operator on the odd row and column images containing the key disrupts the connection between the original image and the encrypted image. The same inverted key is applied to even rows and columns of the image. Experimental tests were performed using detailed numerical analysis to demonstrate the resilience of the proposed method against different types of attacks, such as statistical attacks and differential attacks (visual tests). Performance evaluation tests also show high security of the proposed image encryption technique. It provides fast encryption and decryption and is suitable for real-time encryption and transmission applications over the Internet.

5. Lorenz Image Encryption

The Lorentz equation is simply a model for heat-induced fluid flow in an environment. This paradigm was originally developed by E.N. introduced and explained. Lorenz 1963 [11–13]. The “butterfly effect” is a typical chaotic system and is associated with attractors because he, like a butterfly, has two wings [12,14]. Therefore, it has been extensively studied in the fields of chaotic control, synchronization phenomena, dynamical system modeling and chaos theory. The chaotic Lorentz equation is a 3D dynamic system characterized by x, y, and z. The system of equations behaves chaotically compared to the original system parameters. Compared to 1D or 2D systems, the chaotic behavior of Lorentz systems is much more complex. Encrypt the image using the Lorentz equation.

V. RESULTS AND DISCUSSION

Fig: This page describes the concept behind this project.

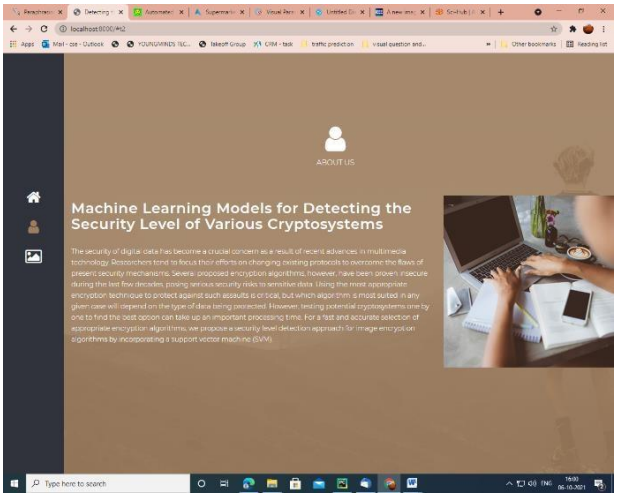

Fig: This Page describes the accuracy of models

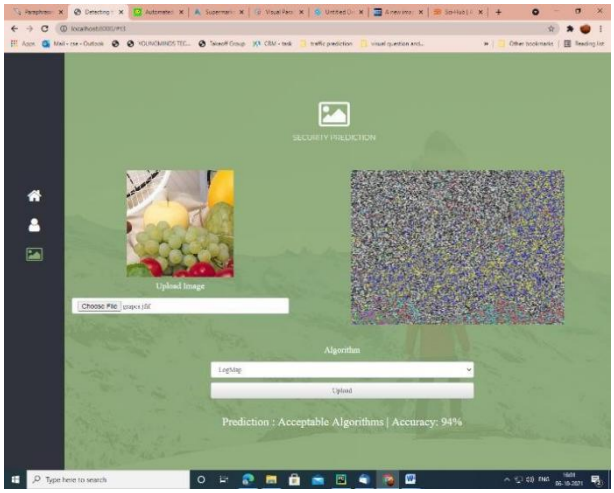

Fig: Accuracy with Svm : 94%

VI. CONCLUSION

In this paper, we built and suggested a model for detecting the security level of various encryption techniques. Create a data collection first, and include security characteristics that are shared by all encryption algorithms. We separated the value of each feature into three intervals (strong, acceptable, and weak) and then explained the resulting safety levels in order to build the dataset. The level of security offered by each encryption system is then tested on the suggested model. By figuring out their various statistics, you may also manually determine the security level of these encryption techniques. This process takes a long time using conventional testing techniques, however using the suggested model, tests can be run quickly. Finally, we examined the suggested model in a number of tests to assess its performance and discovered that it was 94% faster and more accurate than other models that were at the time.

VII. FUTURE SCOPE

Future studies will look into how to rate the security of deep learning-based cryptosystems.

REFERENCES

1.I. Hussain A. Aneesa. H. Alkhaldi, M. Islam, N. Siddiqui and R. Ahmed, "Image Encryption Based on Chaotic Chebyshev Maps and S8-S Boxes",

2. A Anees, I. Hussain, A. Agarin, M. Aslam, “A Robust Watermarking Scheme for Online Multimedia Rights Protection Using New Chaos Maps,”

3. A Shafiq and J. Ahmed, "Dynamic Permutation-Based Encryption Algorithm for Strongly Correlated Data",

4. F. Ahmed, A. Anees, V.U. Abbas and M.Y. Siyal, "Noise Channel Tolerant Image Encoding Scheme"

5M. A.B. Farah, R. Guesmi, A. Kachori, M. Samet, "A new chaos-based optical image encoding using fractional Fourier transform and DNA sequence manipulation",

6. C. E. Shannon, "Communication in the Presence of Noise",

7. S. Heron, “Advanced Encryption Standard (AES)”

8. H. Liu, A. Kadir, X. Sun, “A Chaos-Based Fast Color Image Encryption Scheme Using True Random Keys from Ambient Noise”,

9. Y.-L. Lee and W.-H. Cai, "New secure image transmission technology via secret fragments Visualization of mosaic images by almost reversible color conversion"

10. A. Annie’s, A.M. Siddiqui, F. Ahmed, "Chaotic Permutation of Strong Autocorrelation Data in Cryptographic Algorithms",

11. L. Liu, Y. Lei, D. Wang, "A Fast Chaotic Image Encoding Scheme Using Joint Permutation Spreading Operations".

12. M. Khalili and D. Asatryan, “Color Space Effects for Extended Discrete Wavelet Transform-Based Digital Image Watermarking Using Arnold Transform Maps,”

13. L. Zhang, J. Wu, and N. Zhou, "Image Encoding with Discrete Fractional Cosine Transformation and Chaos",