JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Crypto System Verification Security Levels Using Machine Learning

Ms. K. Jyotsna (M.C.A). Rajeev Gandhi Memorial college Of Engineering and Technology, Nandyal

*** Mr. V. V. Nagendra Kumar, M. Tech, (Ph.D). Rajeev Gandhi Memorial college Of Engineering and Technology, Nandyal**

ABSTRACT

Recent developments in multimedia technology have made the security of digital data a vital concern. To address the shortcomings of the current security mechanisms, researchers frequently concentrate their efforts on altering the existing protocols. However, during the past few decades, a number of proposed encryption algorithms have been shown to be insecure, posing a major security risk to sensitive data.

It is crucial to use the best encryption method to defend against such attacks, but which algorithm is best in a certain situation will depend on the type of data being secured. However, evaluating various cryptosystems one at a time to determine the optimal one can consume a significant amount of processing time. We provide a security level detection for quick and precise selection of relevant encryption techniques.

A Support Vector Machine (SVM) into an algorithmic solution for image encryption. As part of this effort, we also produce a dataset employing common encryption security criteria, such as entropy, contrast, homogeneity, peak signal to noise ratio, mean square error, energy, and correlation. These variables are used as features that have been derived from various cipher pictures.

Based on their level of security, dataset labels are categorized into three groups: strong, acceptable, and weak. We evaluated accuracy to assess the performance of our suggested model, and the results show that this SVM-supported system is effective.

Keywords: - Support vector machine (SVM), security analysis, image encryption, cryptosystem.

1. INTRODUCTION

1.1 Introduction

Due to the exponential growth in multimedia data transmissions across insecure channels (most notably the Internet), security has become a prominent study area. To shield data from snoopers and unauthorized users, several researchers have turned to creating novel encryption techniques. When encrypting digital photos, diffusion and confusion (sometimes referred to as scrambling) are two essential components.

According to a hypothesis put forth by Claud Shannon, a cryptosystem with confusion and diffusion techniques can be regarded as secure. On digital photos, the scrambling process can be applied directly to the pixels or to the rows and columns, whereas diffusion modifies the original pixel values. In other words, the replacement process replaces each distinct pixel value with the value of the S-unique box. The privacy of the data cannot be fully protected by transmission in an encrypted manner.

Despite being encrypted for transmission, the information can still be viewed by unauthorized users due to the encryption algorithms lax security. The robustness of the image is significantly impacted by the

security level of the encryption algorithm used to encrypt it.

The plain image will be completely encrypted using a very powerful encryption technique, making it resistant to attacks on its availability, integrity, and secrecy. When selecting an encryption technique, temporal complexity is another important factor to take into account in addition to security. The type of application must be considered when selecting a cryptosystem because different forms of data have different security priorities. Encrypted. We present a support vector machine (SVM)-based security level detection approach for picture encryption schemes since the image encryption algorithm is crucial.

2. Literature Survey

• **[1] Automated detection and classification of cryptographic algorithms in binary programs through machine learning by Diane Duros Hosfelt.,** Internet threats, especially malware, frequently use cryptographic methods to mask their activities and potentially take over a victim's system (as in the case of ransomware). The proliferation of malware and other dangers is too rapid for the traditional time-consuming binary analysis techniques to be effective.

Automating cryptographic algorithm detection and categorization allows us to expedite program analysis and more effectively fight malware. This thesis presents various approaches for machine learning-based automatic discovery and classification of cryptographic algorithms in built binary programs. The findings in this work suggest that machine learning may be used to discover and identify cryptographic primitives in compiled code, while more research is required to thoroughly verify these methods on real-world binary programmers. These methods are presently being employed in small, single-purpose programs to find and classify cryptographic algorithms, and more research is being advocated in order to apply them to actual scenarios.

Summary this thesis investigated how to extract information from compiled code and train machine learning models to identify and categorize cryptographic methods. Utilizing four distinct learning algorithms, three various model types were assessed on four different feature sets. Despite the fact that decision tree models were found to perform best on these data, it is possible that an SVM with a linear kernel will generalize to real-world data more effectively. Given a relatively small sample size, cross-validation findings show that algorithm classification and detection will be over 95% accurate.

[2] Applications in Security and Evasions in Machine Learning: A Survey by Ramani Sagar 1,*, Rutvij Jhaveri 2 and Carlos Borrego 3: Machine learning (ML) has recently emerged as a key component in producing security and privacy across a range of applications. Serious problems including real-time attack detection, data leaking vulnerability assessments, and many more are addressed with ML. In a variety of areas, including real-time decision-making, huge data processing, shortened learning cycle times, cost-efficiency, and error-free processing, ML comprehensively supports the demanding requirements of the current security and privacy scenario.

As a result, in this work, we examine the cutting-edge techniques that make better use of machine learning (ML) to address current security-related real-world needs. We look at various security applications from the point of view of ML models and evaluate the accuracy outcomes across various conceivable aspects.

An outline for an interdisciplinary research field is provided by the analysis of ML algorithms in security applications. Attackers can circumvent the ML models by engaging in adversarial attacks, even with the deployment of modern, sophisticated technology and techniques. As a result, it becomes necessary to evaluate the ML models' susceptibility to adversarial attacks at the time of development.

To further support this notion, we also examine the many adversarial attacks that can be made against ML models. We have modeled the threat model and protection tactics against adversarial attack techniques to provide accurate representation of security features. Additionally, we addressed the model point at which potential attacks may occur and illustrated the adversarial attacks depending on the attackers' understanding of the model. be committed. Finally, we also research various adversarial attack characteristics.

3. OVERVIEW OF THESYSTEM

3.1 Existing System

Acquiring precisely balanced and closely linked datasets is nearly hard under the current system. Even if there are vast amounts of data available, it is still a difficult task to extract the pertinent facts. To get around all of this, we extract usable data using machine learning packages from the scikit-learn library.

3.1.1 Disadvantages of Existing System

- Less feature compatibility
- Low accuracy.
- Hight Complexity.
- Highly Inefficient.

3.2 Proposed System

In recent years, a plethora of encryption algorithms, including chaotic and transformation-based methods, have been introduced. Some of the currently used encryption methods have been shown to be insecure and to offer insufficient security based on statistical analysis of their results. One method to assess the security of an encryption algorithm is to examine the statistics of its security parameters.

Traditional approaches typically involve making these comparisons one at a time, which takes a lot of time. We developed a machine learning model that combines SVM to aid us in quickly selecting an appropriate encryption method.

3.2.1 Advantages of Proposed System:

- It increases the accuracy.
- It reduces the time complexity.
- It automates the process of detecting the security levels of encryption algorithms

3.3 Methodology

3.3.1 User:

The user model is a structure that is used to capture certain characteristics about an individual user.

- **Data gathering:**

Needs to gather the information or data from the open source, this will be use in the train the models.

- **Pre-processing:**

Data need to be pre-processed according the models it helps to increase the accuracy of the model and better information about the data.

- **Feature Engineering:**

In this step features are selected based on the priority of the column data, by this we can reduce the time investing on many columns.

- **Model Building**

To get the final result model building for the dataset is an important step. Based on the dataset we build the model for classification and regression.

- **View Results**

User view's the generated results from the model.

3.3.2 System

The system model is a Process oriented representation that emphasizes the influences, or flow, of information between models.

- **Model Checking**

System checks model accuracy and it takes of the necessary for the model building

- **Generate Results**

System takes the input data from the users and produces the output.

3.4 Algorithms and Methods:

Support-vector device 1 Support-vector machines are supervised learning models that analyze data using machine learning techniques for classification and regression. SVMs are one of the most trustworthy prediction methods because they are based on statistical learning frameworks. Given a set of training examples, each labelled as belonging to one of two categories, an SVM training algorithm builds a model that assigns new examples to one of two categories, making it a non-probabilistic binary linear classifier.

SVM enlarges the gap between the two categories as much as feasible by mapping training examples to points in space. Then, new examples are projected into that same space and classified according to which side of the gap they fall on. In a higher- or infinite-dimensional

space, a support-vector machine constructs a hyper plane or group of hyper planes that can be used for classification, regression, or other tasks like outlier detection. Since the higher the margin, the lower the classifier's generalization error, it makes sense that the hyper plane with the largest distance from the closest training data point of any class (referred to as the functional margin) achieves a respectable separation.

The sets to discriminate are frequently not linearly separable in that space, even when the beginning problem is described in a finite-dimensional space. In order to facilitate separation, it was proposed [5] to convert the initial finite-dimensional space into a considerably higher-dimensional area. The mappings that SVM algorithms employ include

4 ARCHITECTURE

s

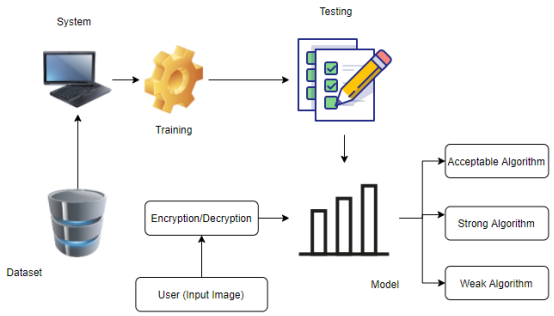
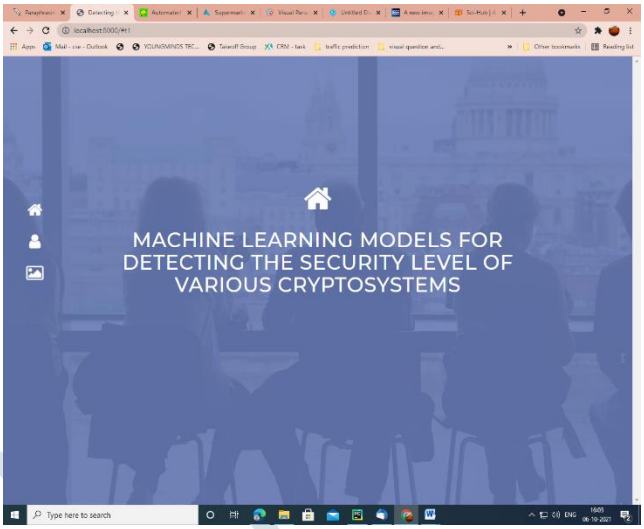


Fig 1: Frame work of proposed method

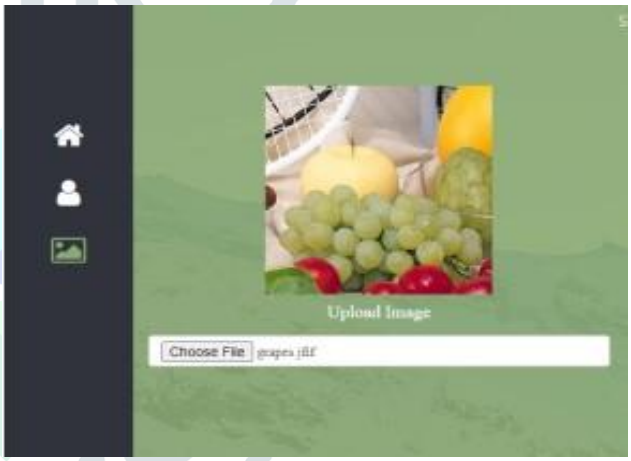
Architecture diagram show that the dataset connected to system. The system starts testing the data by using different types of models like Acceptable, Strong, and Week algorithms. By testing these models we can produce the results.

5. RESULTS SCREEN SHOTS

Home Page:

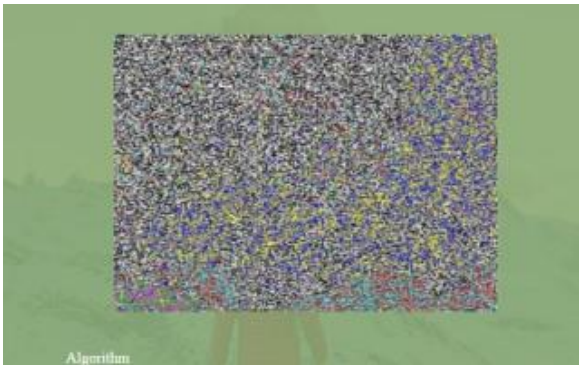


Upload image:



Choose options:

Predict Result:



6. CONCLUSION

In this post, we built and suggested a model that can rapidly and accurately determine the security level of various encryption systems. We started by building a dataset and adding characteristics that represented the security parameters shared by different encryption techniques. We have separated the values of all attributes into three intervals—strong, acceptable, and weak—that represent the resulting security levels in order to generate a dataset. The various encryption techniques are then evaluated on our suggested model to determine the level of security that each one delivers. By calculating the statistical values of each, we can manually determine the security level of these encryption techniques. This process takes a long time to complete using conventional testing techniques, however using our suggested model, testing can be completed in a matter of seconds. Finally, we evaluated the performance of our proposed model using various tests and discovered that it generates 94% accurate predictions at a significantly faster rate than other models currently in use.

7. FUTURE ENHANCEMENT

As for future works, In the future work, the use of deep learning techniques to detect the security level of cryptosystems will be investigated.

8. REFERENCES

[1] WHO Pneumonia. World Health Organization. (2019), https://www.who.int/news-room/fact-sheets/detail/pneumonia

[2] Neuman M., Lee E., Bixby S., Diperna S., Hellinger J., Markowitz R., et al. Variability in the interpretation of chest radiographs for the diagnosis of pneumonia in children. Journal of Hospital Medicine. 7, 294–298 (2012) https://doi.org/10.1002/jhm.955 PMID: 22009855

[3] Williams G., Macaskill P., Kerr M., Fitzgerald D., Isaacs D., Codarini M., et al. Variability and accuracy in interpretation of consolidation on chest radiography for diagnosing pneumonia in children under 5 years of age. Pediatric Pulmonology. 48, 1195–1200 (2013) https://doi.org/10.1002/ppul.22806 PMID: 23997040

[4] Kermany D., Zhang K. & Goldbaum M. Labeled Optical Coherence Tomography (OCT) and Chest X-ray Images for Classification. (Mendeley, 2018)

[5] Lal S., Rehman S., Shah J., Meraj T., Rauf H., Damasˇevičius R., et al. Adversarial Attack and Defence through Adversarial Training and Feature Fusion for Diabetic Retinopathy Recognition. w

[6] Rauf H., Lali M., Khan M., Kadry S., Alolaiyan H., Razaq A., et al. Time series forecasting of COVID-19 transmission in Asia Pacific countries using deep neural networks. Personal and Ubiquitous Computing. pp. 1–18 (2021) https://doi.org/10.1007/s00779-020-01494-0 PMID: 33456433

[7] Deng J., Dong W., Socher R., Li L., Li K. & Fei-Fei, L. Imagenet: A large-scale hierarchical image database. 2009 IEEE Conference on Computer Vision and Pattern Recognition. pp. 248-255 (2009)

[8] Dalhoumi S., Dray G., Montmain J., Derosière, G. & Perrey S. An adaptive accuracy-weighted ensemble for inter-subjects classification in brain-computer interfacing. 2015 7th International IEEE/EMBS Conference on Neural Engineering (NER). pp. 126-129 (2015)

[9] Albahli S., Rauf H., Algosaibi A. & Balas V. AI-driven deep CNN approach for multi-label pathology classification using chest X-Rays. PeerJ Computer Science. 7 pp. e495 (2021) https://doi.org/10.7717/peerj-cs.495 PMID: 33977135.