International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

IJIEMR Transactions, online available on 31st Mar 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 03

10.48047/IJIEMR/V12/ISSUE 03/89

Title **SECURITY LEVELS OF VARIOUS ENCRYPTION ALGORITHMS DETECTION USING ML**

Volume 12, ISSUE 03, Pages: 612-615

Paper Authors

K.Sireesha, D.Ratna Kumari, Revathi Konakala, Reethika Kolusu

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Security Levels of Various Encryption Algorithms Detection Using ML

K.Sireesha[1], D.Ratna Kumari[2], Revathi Konakala[3], Reethika Kolusu[4]
[1]Assistant Professor of Computer Science Engineering Dept,ALIET
[2,3,4]UnderGraduate students of Computer Science and Engineering Depart, ALIET
sireeshakcs@aliet.ac.in , ratnakumari5095@gmail.com, revathisrinivas2910@gmail.com, reethikakolusu@gmail.com

Abstract

The security of digital data has become increasingly important as a result of recent advancements in multimedia technology. Researchers frequently focus their efforts on changing the current protocols to solve the flaws of the present security measures. Yet, during the past few decades, several proposed encryption algorithms have been insecure, posing a huge 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 particular situation will depend on the kind of data that has to be secured. However, evaluating various cryptosystems one at a time to determine the optimal choice can consume a significant amount of processing time. We suggest a security-level identification method for picture encryption techniques that uses a support vector machine for quick and precise selection of the correct encryption algorithms (SVM).We also create a dataset using a variety of encryption security criteria, including entropy, contrast, homogeneity, peak signal-to-noise ratio, mean square error, energy, and correlation.. We use these variables as features that are taken from various cipher pictures.

Introduction

Due to the exponential increase in multimedia data transmissions through unsecured networks, security has become a prominent study area (most notably the Internet). To protect data from unwanted users, several academics have turned to creating new encryption techniques. While encrypting digital photos, diffusion, and misunderstanding are two essential components (also known as scrambling). According to a hypothesis put forth by Claud Shannon, a cryptosystem with confusion and diffusion techniques can be regarded as secure. With digital photos, the scrambling process can be applied directly to the pixels or 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. Transmission in an encrypted method cannot completely safeguard the privacy of the data. Due to the weak security of the encryption algorithm, even though the data is encrypted for transmission, it can still be accessed by unauthorized users. The security level of the encryption algorithm that is used to encrypt the image has a major impact on its robustness.

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 that needs to be encrypted affects the cryptosystem that should be used since different forms of data have different security priorities. Because the picture encryption algorithm is crucial, we suggest a security-level detection method for image encryption algorithms that incorporates a support vector machine (SVM).

Literature Survey

1. "A Comparative Analysis of Symmetric Key Encryption Techniques" by D. K.

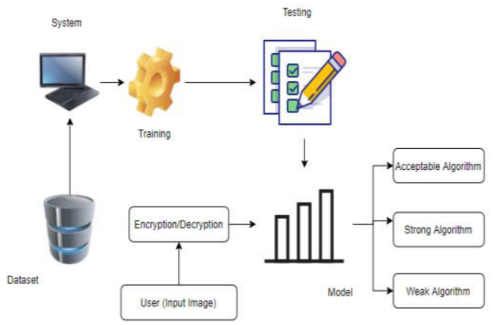
Kushwaha, V. K. Srivastava, and N. Sharma.

In this study they tried to evaluate the performance of DES, 3DES and AES symmetric encryption algorithms under MANET environment. On the other hand, they applied a secure key management solution using the DHKE protocol. And finally they offered the ability to choose the encryption type by the user based on the required security level

Automated detection and classification of cryptographic algorithms in binary programs through machine learning by Diane Duros Hosfelt Threats from the internet, particularly malicious software (i.e., malware) often use cryptographic algorithms to disguise their actions and even to take control of a victim's system (as in the case of ransom ware). Malware and other threats proliferate too quickly for the time-consuming traditional methods of binary analysis to be effective. By automating detection and classification of cryptographic algorithms, we can speed program analysis and more efficiently combat malware. This thesis will offer different ways for automatically discovering and classifying cryptographic algorithms in compiled binary programmes using machine learning. While more research is needed to fully test these methods on real-world binary programmes, the findings in this paper imply that machine learning may be used to detect and identify cryptographic primitives in compiled code with success. These techniques are now being used to discover and categorise cryptographic algorithms in small single- purpose programmes, and more work is being suggested to apply them to real-world situations.

Proposed system

A slew of encryption algorithms, including chaos and transformation-based algorithms, have been presented in recent years. By examining the statistical findings of existing encryption algorithms, it has been discovered that some of them are unsecure and do not provide adequate protection. Analyzing the statistics of an encryption algorithms security parameters is one technique to determine its security level. Traditional methods of accomplishing this usually include making these comparisons one by one, which takes a long time. We created a machine learning model that combines SVM to help us choose a suitable encryption technique more rapidly.



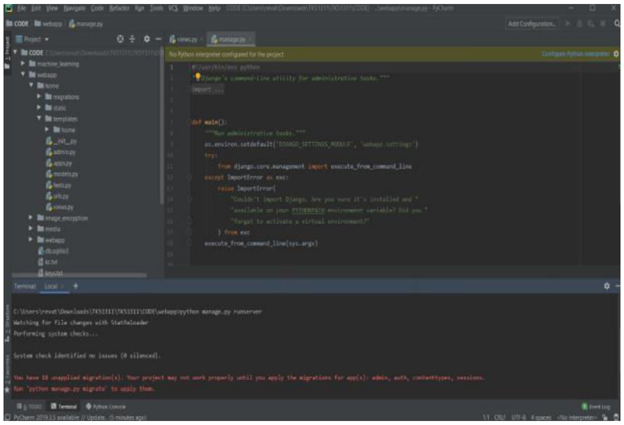
Methodology

Support-vector machines are supervised learning models that analyse data for classification and regression using machine learning methods. One of the most trustworthy prediction techniques is the use of SVMs, which are based on statistical learning frameworks.

Given a set of training examples, each of which is marked as belonging to one of two categories, an SVM training method develops a model that, when presented with additional instances, assigns them to one of two categories, resulting in 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. Next, based on which side of the gap they fall, new examples are projected to fit into one of the categories by being mapped into that same space. 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.

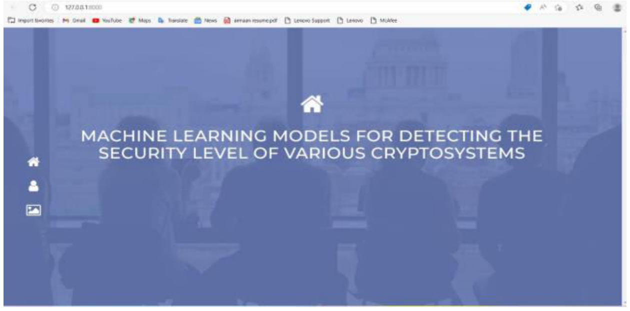
The mappings used by SVM schemes are designed to ensure that dot products of pairs of input data vectors can be computed easily in terms of the variables in the original space, by defining them in terms of a kernel function.

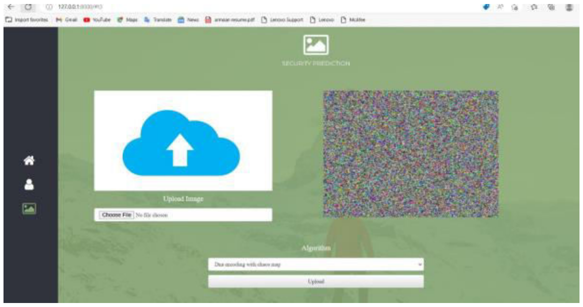
RESULTS AND DISCUSSION

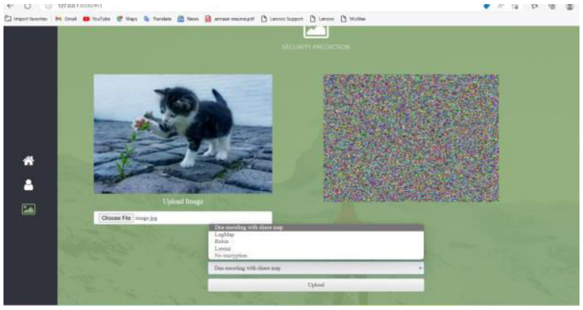

File Edit View Navigate Code Refactor Run Tools VCS Window Help
CODE webapp manage.py
Add Configuration...
Project
views.py manage.py
No Python interpreter configured for the project
Configure Python interpreter
CODE
machine_learning
webapp
home
migrations
static
templates
home
__init__.py
admin.py
apps.py
models.py
tests.py
urls.py
views.py
image_encryption
media
webapp
db.sqlite3
kc.txt
key.txt
Terminal Local
TODO Terminal Python Console
Event Log
PyCharm 2019.3.5 available // Update... (5 minutes ago)
1:1 CRLF UTF-8 4 spaces <No interpreter>

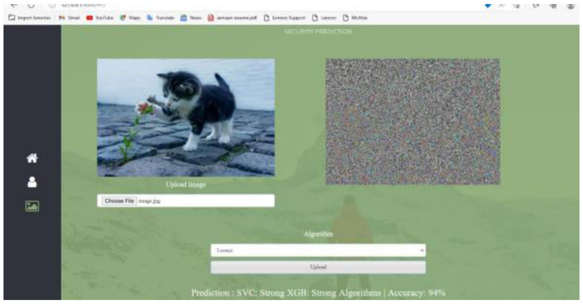
```
#!/usr/bin/env python
"""Django's command-line utility for administrative tasks."""
import ...


def main():
    """Run administrative tasks."""
    os.environ.setdefault('DJANGO_SETTINGS_MODULE', 'webapp.settings')
    try:
        from django.core.management import execute_from_command_line
    except ImportError as exc:
        raise ImportError(
            "Couldn't import Django. Are you sure it's installed and "
            "available on your PYTHONPATH environment variable? Did you "
            "forget to activate a virtual environment?"
        ) from exc
    execute_from_command_line(sys.argv)
```

```
C:\Users\revat\Downloads\TK51111\TK51111\CODE\webapp>python manage.py runserver
Watching for file changes with StatReloader
Performing system checks...

System check identified no issues (0 silenced).

You have 18 unapplied migration(s). Your project may not work properly until you apply the migrations for app(s): admin, auth, contenttypes, sessions.
Run 'python manage.py migrate' to apply them.
```









Prediction : SVC: Strong XGB: Strong Algorithms | Accuracy: 94%

Conclusion

In this article, we have developed and proposed a model that can detect the security level of various encryption schemes quickly and accurately. We began by creating a dataset and incorporating the security parameters common to various encryption schemes as features. To prepare a dataset, we have divided the values of all features into three intervals—strong, acceptable, and weak—that describe the resulting security levels. Next, the different encryption schemes are tested on our proposed model in order to detect the level of security each one offers. We can also detect the security level of these encryption schemes manually by determining the statistical values of each one. With traditional testing methods, this process takes a great deal of time to accomplish but with our proposed model, testing can be achieved within a few seconds. To conclude, we also tested our proposed model using different experiments to evaluate its performance, and we found that it produces 94% correct predictions at much faster speeds than other models currently available

FUTURE SCOPE

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

References

1. I. Hussain, A. Anees, A. H. Alkhaldi, M. Aslam, N. Siddiqui, and R. Ahmed, "Image encryption based on Chebyshev chaotic map and S8 S-boxes,
2. A. Anees, I. Hussain, A. Algarni, and M. Aslam, "A robust watermarking scheme for online multimedia copyright protection using new chaotic map,"
3. A. Shafique and J. Ahmed, "Dynamic substitution based encryption algorithm for highly correlated data, "
4. F. Ahmed, A. Anees, V. U. Abbas, and M. Y. Siyal, "A noisy channel tolerant image encryption scheme,"
5. M. A. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, "A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation,"
6. C.E.Shannon, "Communication in the presence of noise,"
7. S.Heron,"Advanced encryption standard (AES),"