South Asian Journal of Engineering and Technology Research Article

Open Access Full Text Article 142(2024) 7-10 DOI: 10.26524/sajet.2024.3

# A Covert Timing Channels Data Encryption Sceme In Cloud Simulation

**S. Shangavi[1], Dr. T. Suresh Kumar[2]**

[1]PG Scholar[1], Department of Computer Science and Engineering, Nandha College of Technology, Erode-638052.

[2]Associate Professor[2], Department of Computer Science and Engineering, Nandha College of Technology, Erode-638052.

**Corresponding author**.
**Correspondence:** S. Shangavi
**E-mail**: shangu7482@gmail.com

**Article info**
Received 29th December 2023
Received in revised form
22 February 2023
Accepted 26 April 2024

**Keywords**
Traffic flows, image, CTC

https://sajet.in/index.php/journal/article/view/264

## Abstract

Covert Timing Channels (CTC) have become an impending network security problem as the sophistication and use of data exfiltration carried out by cyber-attacks has increased. Inter-arrival periods are used by these channels to steal sensitive data from targeted networks. Machine learning approaches are increasingly being used to detect CTCs, which use statistical-based measures to distinguish malicious (covert) traffic flows from genuine (overt) traffic flows. Given the attempts of cyber-attacks to elude detection and the expanding column of CTCs, covert channels detection must increase in both performance and precision in order to detect and prevent CTCs, as well as reduce the quality of service degradation caused by the detection process. We provide a new image-based method for fully autonomous vehicles in this research. Our strategy is based on the fact that covert channels provide communications that can be transformed into colored visuals. Our approach is based on this observation and is meant to detect and find the malicious part (i.e., a sequence of packets) within a traffic flow automatically. Our technique lowers the drop in service quality caused by blocking complete traffic flows in which hidden channels are found by finding the covert components within traffic flows. To detect covert traffic, we first convert traffic flows into colored images and then extract image-based attributes. We use these attributes to train a classifier on a huge dataset of covert and overt traffic. We use these attributes to train a classifier on a huge dataset of covert and overt traffic. This method achieves remarkable results, with a detection accuracy of 95.83 percent for cautious CTCs and a covert traffic accuracy of 97.83 percent for 8-bit covert messages, much above the capabilities of commonly used statistical-based solutions.

**Introduction**

Covert channels are useful for smuggling sensitive information out of targeted networks. This method of exfiltration is particularly effective since it makes use of existing system resources that were not designed to send sensitive data for communication purposes. By doing so, typical detection mechanisms such as firewalls and intrusion detection systems are unable to identify the transport of covert data.

## I. EXISTING SYSTEM

In the current system, securing through numerous metrics is not possible. It is not possible to encrypt the image and secure the message at the same time. We go over the many CTC detection and prevention methods that have been proposed in the literature. We investigated two types of study for the design and evaluation of our suggested approach: statistical-based CTC detection and machine learning-based CTC detection. The sequence connection has a bad link.

**DRAWBACKS**

Simple tests are ineffective at detecting complex and resilient CTC algorithms. It makes no attempt to overlap (imitate) the time-delays experienced by overt traffic. The packet time-delay configuration was configured to equal the overt traffic's twofold mean inter-arrival time. When contrasted to overt traffic, it frequently generates traffic anomalies.

## II. PROPOSED SYSTEM

The proposed methodology is ELIPTICAL CURVE CRYPTOGRAPHY with COVERT TIMING CHANNELS. Because of their capacity to effectively identify covert timing channels, machine learning algorithms have been applied in numerous CTC detection systems. In general, these approaches use a labelled set of overt and covert data flows to train and develop machine learning models using various metrics (or features). a new method for detecting hidden timing channels that is both automated and accurate I got around it and was able to secure the image encryption. Elliptical curve cryptography with covert timing channels is the most efficient and time-saving method.

**ADVANTAGES**

The delay of transmission times of packets plays a key role in evading detection by cyber defendership enables to utilize the popular image processing techniques to extract more robust image-based features for further processing. It aims at providing a comprehensive analysis of various classifiers and accuracy measures to provide the flexibility to select the classifier. It provides the ability to drop only the malicious part of traffic flows while allowing the rest of the traffic flow to pass through.

## III. LIST OF MODULES

- Index generation
- Bug Fixing
- Digital Image Correction
- Hidden Data

**A. Index generation**

The textured image is loaded in the index value generation, and the value is assigned to a specific spot based on the texture of the image pixels. This can be used to store and encrypt data as well as retrieve information.

**B. Bug Fixing**

A patch is a series of modifications to a computer programme or its supporting data that are intended to update, correct, or improve it. This involves addressing security flaws and other defects, and such updates are sometimes referred to as bugfixes or bug fixes. When the source code for compiled and image object applications is unavailable, patching allows them to be modified.

**C. Digital Image Correction**

The method of algorithmically creating a large digital image from a tiny digital sample image by exploiting its structural features is known as texture synthesis. It is a subject of computer graphics study and is applied in a variety of applications, including steganography.

**D. Hidden Data**

The hidden data will simply be the remaining produced by dividing the new pixel by the appropriate factor. This is a method in which the data is buried in the difference between neighbouring pixels, so that simply extracting a few bits will never reveal the secret data.

## IV. PERFORMANCE EVALUATION

Our evaluation aims to assess (a) the effectiveness of our approach in detecting covert timing channels under various cyber-attack defence evasion configurations; (b) the ability of our approach to pinpoint the covert part (set of packets) of the traffic sub-flow; and (c) compare and contrast different machine learning classifiers in detecting CTCs based on their accuracy and interpretability.

## V. CONCLUSION

Snap Catch is a revolutionary technique for detecting hidden timing channels that is both automated and accurate. Snap Catch is a covert traffic detection tool that uses image processing and machine learning algorithms. First, utilizing a unique method that captures the concrete aspects of network traffic and portrays them in colourful images, the system translates traffic inter-arrival times into coloured images.

## VI. REFERENCES

1. S. Al-Eidi, O. Darwish, and Y. Chen. Covert timing channel analysis either as cyber-attacks or confidential applications. Sensors, 20(8):2417, 2020.
2. O. Darwish, A. Al-Fuqaha, G. B. Brahim, I. Jenhani, and A. Vasilakos. Using hierarchical statistical analysis and deep neural networks to detect covert timing channels. Applied Soft Computing, 82:105546, 2019.
3. Z. Cui, F. Xue, X. Cai, Y. Cao, G.-g. Wang, and J. Chen. Detection of malicious code variants based on deep learning. IEEE Transactions on Industrial Informatics, 14(7):3187–3196, 2018.
4. O. Darwish, A. Al-Fuqaha, G. B. Brahim, I. Jenhani, and M. Anan. Towards a streaming approach to the mitigation of covert timing channels. In 2018 14th International Wireless

Communications & Mobile Computing Conference (IWCMC), pages 255–260. IEEE, 2018.

5. V.S. Sureshkumar "Optimized Multicloud Multitask Scheduler for Cloud Storage and Service by Genetic Algorithm and Rank Selection Method" ,International Journal of Advanced Science Engineering and Technology , pp:2-7, Issue 4, volume 3,2014.
6. K. Biswas, D. Ghosal, and S. Nagaraja. A survey of timing channels and countermeasures. ACM Computing Surveys (CSUR), 50(1):1–39, 2017.
7. S. S. Sarikan and A. M. Ozbayoglu. Anomaly detection in vehicle traffic with image processing and machine learning. Procedia Computer Science, 140:64–69, 2018.
8. L. Chappell. Wireshark 101: Essential skills for network analysiswireshark solution series. Laura Chappell University, USA, 2017.
9. V.S. Sureshkumar, A.Chandrasekar, "Fuzzy-GA Optimized Multi-Cloud Multi-Task Scheduler For Cloud Storage And Service Applications", International Journal of Scientific & Engineering Research , Volume 4, Issue3, March-2013
10. V.S.Suresh kumar , E.Prabhakar, Dr.S.Nandagopal "Liklihood weighted bagging ensemble approach to analyze public sentiment about covid -19 pandemic", International journal for mechanical engineering ,pp:1-7,Issue-3,Volume-6,2021
11. V.S.Sureshkumar,R.V.Kamal,A.Moulieeshwaran,P.sabarish,A.Vikas" A Novel Quality based computation offloading Framework for edge cloud supported-Internet of Things", International Research Journal of Modernization in Engineering Technology and Science,PP:10673-10680,Issue-4,Volume-6,2024.
12. Machine Learning Threatens 5G Security was published by J. Suomalainen et al., in the year of 2020.
13. R.Ebinson,A.GuhanShanmugam,S.C Mouneswaran,P.Abinathan,V.S.Suresh kumar"Energy–Efficient Task Offloading Based on Differential Evolution in edge Computing System with Energy Harvesting",South Asian Journal of Engineering And Technology,pp:1-12,Volume-13,issue-1,2023
14. V.S. Sureshkumar, D. Joseph Paul, N.Arunagiri, T.Bhuvaneshwaran , S,Gopalakrishnan "*Optimal Performance And Security Of Data Through FS- Drops Methodology*" ,International Journal of Innovative Research In Engineering Science and Technology , pp:1-7, Issue 3, volume5,2017
15. E.prabhakar, V.S.Suresh kumar, Dr.S.Nandagopal "*Mining better advertisement tool for government schemes using machine learning",International Journal of psychosocial Rehabilitation,pp:1122-1135,Issue 4, Volume23,2019*