International Research Journal of Education and Technology

Peer Reviewed Journal
ISSN 2581-7795

A Highly Advanced Data Encryption Scheme in Cloud Simulation

Devarajsamy S[1], Athavan P A[2], Manoj Kumar P[3], Naveen Kumar M[4], PrakashR[5]

[1]Assistant Professor, [2,3,4,5]UG Students - Final Year, Department of Information Technology, Nandha College of Technology, Perundurai – 638052, Tamilnadu, India

Abstract

With the quick development of information exfiltration completed by digital assaults, Covert Timing Channels (CTC) have turned into a fast approaching organization security hazard that keeps on filling in both refinement and use. These sorts of channels use between appearance times to take delicate information from the designated networks. CTC recognition depends progressively on AI strategies, which use factual based measurements to isolate vindictive (secretive) traffic streams from the genuine (plain) ones. In any case, given the endeavors of digital assaults to dodge identification and the developing segment of CTC, incognito channels discovery needs to work on in both execution and accuracy to distinguish and forestall CTCs and relieve the decrease of the nature of administration brought about by the recognition cycle. In this paper, we present an inventive picture based answer for completely robotized CTC location and restriction.Our methodology depends on the perception that the secretive channels create traffic that can be changed over to shaded pictures. Utilizing this perception, our answer is intended to naturally recognize and find the malignant part (i.e., set of parcels) inside a traffic stream. By finding the incognito parts inside traffic streams, our methodology decreases the drop of the nature of administration brought about by hindering the whole traffic streams in which secret channels are distinguished. We first proselyte traffic streams into shaded pictures, and afterward we extricate picture based highlights for discovery undercover traffic. We train a classifier utilizing these elements on a huge informational index of undercover and clear traffic. This methodology shows an amazing exhibition accomplishing a recognition precision of 95.83% for wary CTCs and a secret traffic exactness of 97.83% for 8 cycle clandestine messages, which is far past what the famous measurable based arrangements can accomplish.

Introduction

Secretive channels give powerful strategies to exfiltrate touchy information from the designated networks. This kind of exfiltration is especially successful in light of the fact that it utilizes existing framework assets, which were not initially intended to send touchy information with the end goal of correspondence. By doing this, the exchange of the secret information becomes imperceptible by conventional location techniques, for example, firewalls and interruption discovery frameworks. Because of the capacity to send information without being identified, clandestine channels have turned into a genuine danger to the expert space just as the overall local area of web clients. Notwithstanding the way that undercover channels can be utilized to release private data, they can be used by vindictive gatherings to convey and trade data to organize destroying Distributed Denial of Service (DDoS) assaults.

Secret Channel

In PC security, a secret channel is a sort of assault that makes a capacity to move data objects between processes that shouldn't be permitted to convey by the PC security strategy. The term, begun in 1973 by Butler Lampson, is characterized as channels "not planned for data move by any means, for example, the help program's impact on framework load," to recognize it from authentic channels that are exposed to get to controls by COMPUSEC.

Recognition

As a rule, identification is the activity of getting to data without explicit collaboration from with the sender.In the historical backdrop of radio interchanges, the expression "finder" was first utilized for a gadget that recognized the basic presence or nonappearance of a radio transmission, since all correspondences were in Morse code. The term is as yet being used today to portray a part that extricates a specific sign from each of the electromagnetic waves present. Recognition is typically founded on the recurrence of the transporter signal, as in the natural frequencies of radio telecom, however it might likewise include separating a weak transmission from commotion, as in radio space science, or recreating a secret transmission, as in steganography.In optoelectronics, "identification" signifies changing a got optical contribution over to an electrical result. For instance, the light sign got through an optical fiber is changed over to an electrical sign in an identifier, for example, a photodiode.In steganography, endeavors to distinguish stowed away signals in presumed transporter material is alluded to as steganalysis. Steganalysis has a fascinating distinction from most different kinds of recognition, in that it can frequently just decide the likelihood that a secret message exists; this is as opposed to the identification of signs which are essentially encoded, as the ciphertext can regularly be related to conviction, regardless of whether it can't be decoded.In the military, recognition alludes to the exceptional discipline of observation with the expect to perceive the presence of an article in an area or ambiance.Finally, the craft of discovery, otherwise called following hints, is crafted by an analyst in endeavoring to remake an arrangement of occasions by recognizing the significant data in a circumstance.

Entropy

Entropy is a logical idea, just as a quantifiable actual property that is most ordinarily connected with a condition of turmoil, arbitrariness, or vulnerability. The term and the idea are utilized in assorted fields, from traditional thermodynamics, where it was first perceived, to the infinitesimal portrayal of nature in measurable physical science, and to the standards of data hypothesis. It has found far-running applications in science and physical science, in organic frameworks and their connection to life, in cosmology, financial matters, humanism, climate science, environmental change, and data frameworks remembering the transmission of data for telecom.The thermodynamic idea was alluded to by Scottish researcher and architect MacquornRankine in 1850 with the names thermodynamic capacity and hotness potential.In 1865, German physicist Rudolph Clausius, one of the main authors of the field of thermodynamics, characterized it as the remainder of a tiny measure of hotness to the momentary temperature. He at first depicted it as change content, in German Verwandlungsinhalt, and later authored the term entropy from a Greek word for change. Alluding to minute constitution and construction, in 1862, Clausius deciphered the idea as which means disaggregation.

Entropy predicts that specific cycles are irreversible or unthinkable, beside the prerequisite of not disregarding the protection of energy, the last option being communicated in the primary law of thermodynamics. Entropy is integral to the second law of thermodynamics, which expresses that the entropy of separated frameworks left to unconstrained advancement can't diminish with time, as they generally show up at a condition of thermodynamic harmony, where the entropy is most noteworthy.Austrian physicist Ludwig Boltzmann clarified entropy as the proportion of the quantity of conceivable infinitesimal plans or conditions of individual particles and atoms of a framework that conform to the perceptible state of the framework. He along these lines presented the idea of measurable problem and likelihood circulations into anotherfield of thermodynamics, called factual mechanics, and tracked down the connection between the infinitesimal collaborations, which vacillate about a normal arrangement, to the perceptibly noticeable conduct, in type of a basic logarithmic law, with a proportionality consistent, the Boltzmann steady, that has become one of the characterizing general constants for the cutting edge International System of Units (SI).In 1948, Bell Labs researcher Claude Shannon created comparable factual ideas of estimating infinitesimal vulnerability and variety to the issue of irregular misfortunes of data in media transmission signals. Upon John von Neumann's idea, Shannon named this element of missing data in undifferentiated from way to its utilization in measurable mechanics as entropy, and brought forth the field of data hypothesis. This portrayal has since been distinguished as the all-inclusivemeaning of the idea of entropy.

Computerized Image Processing

Advanced picture handling is the utilization of a computerized PC to deal with computerized pictures through a calculation. As a subcategory or field of advanced sign handling, computerized picture handling enjoys numerous upper hands over simple picture handling. It permits a lot more extensive scope of calculations to be applied to the information and can stay away from issues, for example, the development of commotion and bending during handling. Since pictures are characterized north of two aspects (maybe more) advanced picture handling might be demonstrated as multidimensional frameworks. The age and advancement of computerized picture handling are fundamentally impacted by three variables: first, the advancement of PCs; second, the improvement of math (particularly the creation and improvement of discrete arithmetic hypothesis); third, the interest for a wide scope of uses in climate, agribusiness, military, industry and clinical science has expanded.

AI

AI (ML) is the investigation of PC calculations that work on naturally through experience and by the utilization of information. It is viewed as a piece of man-made consciousness. AI calculations fabricate a model dependent on example information, known as "preparing information", to settle on expectations or choices without being expressly modified to do as such. AI calculations are utilized in a wide assortment of utilizations, for example, in medication, email separating, and PC vision, where it is troublesome or impossible to foster regular calculations to play out the required errands.A subset of AI is firmly identified with computational measurements, which centers around making expectations utilizing PCs; however not all AI is factual learning. The investigation of numerical advancement conveys strategies, hypothesis and application areas to the field of AI. Information mining is a connected field of study, zeroing in on exploratory information examination through solo learning. In its application across business issues, AI is likewise alluded to as prescient examination.

Computerized Reasoning

As a logical undertaking, AI outgrew the journey for man-made brainpower. In the beginning of AI as a scholastic discipline, a few scientists were keen on having machines gain from information. They endeavored to move toward the issue with different representative strategies, just as what was then named "neural organizations"; these were for the most part perceptrons and different models that were subsequently observed to be reexaminations of the summed up straight models of statistics.Probabilistic thinking was likewise utilized, particularly in mechanized clinical finding.Notwithstanding, an expanding accentuation on the intelligent, information based methodology caused a break among AI and AI. Probabilistic frameworks were tormented by hypothetical and commonsense issues of information procurement and portrayal. By 1980, master frameworks had come to overwhelm AI, and measurements were undesirable. Work on emblematic/information based learning proceeded inside AI, prompting inductive rationale programming, however the more measurable line of exploration was presently outside the field of AI legitimate, in design acknowledgment and data recovery. Neural organizations research had been deserted by AI and software engineering around a similar time. This line, as well, was proceeded outside the AI/CS field, as "connectionism", by analysts from different disciplines including Hopfield, Rumelhart and Hinton. Their fundamental achievement came during the 1980s with the reevaluation of backpropagation.AI (ML), redesigned as a different field, begun to thrive during the 1990s. The field changed its objective from accomplishing man-made consciousness to handling resolvable issues of a commonsense sort. It moved concentrate away from the emblematic methodologies it had acquired from AI.

Related Works

Getting through the different measurements is unimaginable in the current framework encrypting the picture and getting the message as a similar time is preposterous. We talk about CTC location and anticipation approaches existing in the writing. The exploration works that we have considered for the plan and assessment of our proposed approach can be assembled into two principle classes: measurable based CTC discovery, and AI based CTC identification Poor association in the arrangement association.

CTC recognition strategies are for the most part centered on the investigation of organization traffic. Most of CTC recognition strategies notice network traffic conduct and concentrate measurable properties of undercover and plain traffic and contrast those properties with perceive inconsistencies and identify clandestine correspondence .Similarly, in a parallel CTC was distinguished utilizing unmistakable traffic and secret traffic histogram. They examined a straightforward measurable strategy for distinguishing CTCs. This technique expects that a surge of organization traffic generally fits an ordinary circulation; a stream with a bimodal or multi-modular appropriation would propose the presence of a secretive planning channel. Consequently, the technique was among quick to zero in on anomalies looking like organization traffic dispersion. In their methodology, the choice tree was prepared utilizing different measurable elements removed from traffic streams. The model's adequacy in identifying the example of between appearance seasons of CTC parcels was then tried utilizing a bunch of both obvious and incognito traffic. The assessment consequences of this work showed that the model was compelling in recognizing CTCs.

Shorouq Al-Eidi, et.al hasproposed the covert planning channels are a significant option for sending data in the realm of the Internet of Things (IoT). In clandestine planning diverts information are encoded in between appearance times between back to back bundles dependent on changing the transmission season of real traffic. Commonly, the change of time happens by deferring the sent parcels on the sender side. A vital perspective in incognito planning channels is to observe the limit of parcel defer that can precisely recognize secretive traffic from genuine traffic. In light of that we can survey the degree of risky of safety dangers or the nature of moved delicate data subtly. In this paper, we concentrate on the between appearance time conduct of clandestine planning directs in two distinctive organization setups dependent on factual measurements, furthermore we explore the parcel postponing limit esteem. Our trials show that the limit is around equivalent to or more noteworthy than twofold the mean of authentic between appearance times. For this situation secret planning channels become discernible as solid oddities.This review utilized secret planning channels by altering the hour of genuine traffic and infuse the traffic that holds clandestine data inside the real traffic. The between appearance seasons of real traffic and secret traffic were examined in two diverse organization setups to investigate the conduct for the two deals with the two arrangements and see how the organization conditions impacted on the chomp rate transmission of the incognito planning channels and the exactness of recognizing clandestine traffic from genuine traffic. Our outcomes observed that the secret traffic didn't for the most part show outrageous qualities when the limit of parcel defers that used to conceal the undercover information not exactly or equivalent the quarter of the mean of the between appearance seasons of real traffic. Thusly, more incognito traffic are counted near the real traffic, making the time scope of secretive traffic covers with the time scope of authentic traffic and the differentiation between them hard. Notwithstanding, there is no cross-over between the time scopes of secretive traffic and the time scope of genuine traffic when the limit of parcel defers that utilized around equivalent to or more prominent than the twofold the mean between appearance seasons of authentic traffic, making the recognizing them more straightforward. In light of these perceptions, it is valuable to find these limit that can assist with recognizing the incognito from authentic traffic [1].

Omar Darwish, et al. proposed the covert planning channels give a component to spill information across various substances. Controlling the circumstance between bundle appearances is a notable illustration of such methodology. The time based property makes the recognition of the secret messages inconceivable by conventional security ensuring instruments like intermediaries and firewalls. This paper presents another conventional various leveled based model to recognize secret planning channels. The location interaction comprises of the examination of a bunch of factual measurements at continuous progressive levels of the between appearance times streams. The factual measurements considered are: mean, middle, standard deviation, entropy, Root of Average Mean Error (RAME). A genuinely factual measurements timing channel dataset of secret and plain channel occurrences is made. The produced dataset is set to be either level where the factual measurements are determined on all progressions of information or hierarchal (5 degrees of order were thought of) where the factual measurements are processed on sub pieces of the stream also. Following this technique, 5 unique datasets were created, and used to prepare/test a profound neural organization based model. Execution results about exactness and model preparing time showed that the various leveled approach outflanks the level one by 4 to 10 percent (as far as precision) and had the option to accomplish short model preparing time (as far as seconds).In our future work, we at first propose further expanding our model by broadening the current dataset with more issue space, measurable, and data hypothesis related elements. For the area related highlights, we will think about two expansive classes of elements: Hardware related (like CPU, switches, network speed, and so on); and Software related (kind of uses, sort of organization traffic, and so on) For the Statistical highlights, we will consider a subset of the measurements utilized in [2017] that incorporate mode, auto-connection coefficient, and so on With respect to data hypothesis related elements, we will consider extra measures, for example, Gini list to gauge the disparity (i.e., scattering) among between appearance times and Kullback-Leiber dissimilarity to remember data for how unique between appearance time disseminations act. Then, at that point, we will consider various sorts of convention epitomes, for example, UDP and crude attachments which don't initiate a great deal of buffering delays as the TCP convention does. At last, we will explore and execute new alleviation strategies as countermeasures against the distinguished incognito planning channels. We are likewise considering expanding our dataset by considering extra non-measurable highlights fully intent on further developing the clandestine planning channel recognition rate [2].

Zhihua Cui et al haveproposed.In this paper with the advancement of the Internet, malevolent code assaults have expanded dramatically, with pernicious code variations positioning as a critical danger to Internet security. The capacity to recognize variations of vindictive code is basic for insurance against security breaks, information robbery, and different risks. Current techniques for perceiving vindictive code have shown helpless discovery precision and low location speeds. This paper proposed a clever strategy that pre-owned profound figuring out how to work on the recognition of malware variations. In earlier exploration, profound learning showed fantastic execution in picture acknowledgment. To carry out our proposed recognition strategy, we changed over the vindictive code into grayscale pictures. Then, at that point, the pictures were recognized and ordered utilizing a convolutional neural organization (CNN) that could extricate the highlights of the malware pictures naturally. Furthermore, we used a bat calculation to address the information awkwardness among various malware families. To test our methodology, we led a progression of trials on malware picture information from Vision Research Lab. The test results showed that our model accomplished great exactness and speed as contrasted and other malware recognition models.This paper proposed a clever technique to work on the recognition of malware variations through the use of profound learning. To start with, this technique changed the vindictive code into gray scale pictures [3].

Omar Darwish et.al has proposed Leaking information utilizing clandestine planning channels is considered as a basic danger in network correspondence. These sort of channels utilize the time between appearance parcels to pass data between various cycles, making it an extremely basic to plan procedures to wipe out and alleviate such channels; thus, guaranteeing a safer correspondence climate. This paper proposes another web based streaming way to deal with the relief of undercover planning channels. The new methodology disposes of undercover planning channels while lightly affecting the general Quality of Service (QoS). A classificationbased technique was utilized to test the exhibition of the proposed relief model. Clandestine planning channels are considered as quite possibly the most challengeable dangers for spilling datum. The significance of concentrating on such sort of channels ascended widely and quickly due to the limits of customary procedures (like intermediaries and firewalls) in recognizing these oddities and in the end reveals such dangers [4].

Selim S. Sarikan et al. has proposedanomaly identification is a significant piece of an Intelligent Transportation System. In this review, picture handling and AI procedures are utilized to distinguish irregularities in vehicle developments. These peculiarities remember standing and going for turn around bearing. Pictures are caught utilizing CCTV cameras from front and back side of the vehicle. This capacity makes the outcomes strong to the varieties in functional and natural conditions. Various back to back outlines are gained for movement discovery. Elements, for example, edges and tag corner areas are separated for following purposes. Bearing of the traffic stream is acquired from the prepared classifier. K-closest neighbor is picked as the classifier model. The proposed strategy is assessed on a public parkway and promising identification results are accomplished. Abnormality discovery is such a significant issues that numerous Intelligent Transportation Systems (ITS) are looking with it. Distinguishing peculiarities in vehicles heading of development is a subset of this intricate issue. Vehicles moving off course represent a significant danger for different drivers. Without question, if peculiarities in vehicles bearing of development are distinguished precisely continuously; hazard of mishaps can be diminished fundamentally. As the urban areas and transportation framework advance around more brilliant and more astute partners, observation frameworks become a fundamental issue.In this review, a vehicle stream identification way to deal with recognizestraffic oddities are introduced [5].

Proposed Methodology

Ellipticalcurve cryptography with covert timing channels are utilized as the proposed technique Machine learning calculations have been utilized in numerous CTC location approaches in view of their capacity to successfully recognize secretive planning channels. As a rule, these methodologies utilize different measurements (or elements) to prepare and develop AI models utilizing a marked arrangement of obvious and incognito traffic streams. a clever procedure for computerize and exact identification of secret planning channels. Defeated exhaustive it and got to the picture encryption. Circular bend cryptography with undercover planning channels is exceptionally effective and the less tedious. Elliptic-bend cryptography (ECC) is a way to deal with public key cryptography dependent on the logarithmic construction of elliptic bends over limited fields. ECC permits more modest keys contrasted with non-EC cryptography (in light of plain Galois fields) to give same. In PC security, an incognito channel is a sort of assault that makes a capacity to move data objects between processes that shouldn't be permitted to convey by the PC security strategy Security.

Peer Reviewed Journal
ISSN 2581-7795

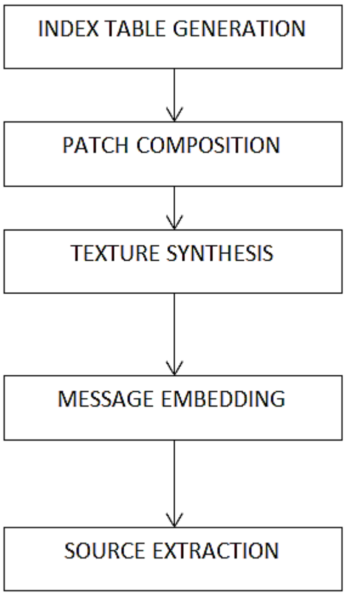

Figure 1System Flow Diagram

Index Table Generation

In the file esteem age the finished picture is stacked and the worth is given with the specific spot as indicated by the surface of the picture pixels.This can be utilized to store the message and scramble the information and recover the data.

Texture Synthesis

A fix is a bunch of changes to a PC program or its supporting information intended to refresh, fix, or further develop it. This incorporates fixing security weaknesses and different bugs, with such fixes normally being called bug fixes or bug fixes.Fixing makes conceivable the alteration of aggregated and picture object programs when the source code is inaccessible.

This requests a careful comprehension of the inward functions of the article code by the individual making the fix, which is troublesome without close investigation of the source code.

Patch Composition

Surface Synthesis is the course of algorithmically developing an enormous computerized picture from a little advanced example picture by exploiting its underlying substance.It is an object of exploration in PC designs and is utilized in many fields, among setgnography.

Message Embedding

The information stowed away will essentially be equivalent to the rest of by partitioning the new pixel by likewise.This is a technique where the information is concealed in the contrast between the nearby pixels, so simple extraction of few pieces won't ever give the information stowed away.

Machine Learning Model Construction

Our methodology's last advance is to develop an AI model to group the produced pictures into one or the other clandestine or obvious. For this assignment, we train a bunch of models utilizing thefollowing AI calculations: Support Vector Machine (SVM), Choice Tree (DT) and Gullible Bayes (NB).We prepared every characterization model utilizing the highlights removed from each picture. Then, at that point, we assessed the models utilizing the hold-out approval strategy. In light of the hold-out approval strategy, we split our dataset into 75% for preparing and 25% for testing (approval).

Performance Evaluation

Our assessment tries to gauge the presentation of our methodology in the accompanying terms: (a) the adequacy of our way to deal with identify clandestine planning channels under varioussafeguard avoidance arrangements of digital assaults; (b) the capacity of our way to deal with pinpoint the secret part (set of bundles) of the traffic sub-stream; and (c) investigate uniqueAI classifiers dependent on their precision and decipher capacity in distinguishing CTCs. In AI and data recovery, there are different measurements to gauge the various parts of precision. For instance, review is exactness measure that objectives the culmination of recognition (i.e., the small part of the absolute CTCs that were recognized). Then again, accuracy estimates the quality (or precision) of recognized CTCs. Various variables might be viewed as while taking on the precision measure(s). Focusing on the review measure demonstrates a wary recognition approach: inclining towards the fulfillment of distinguished CTCs rather than accuracy (bogus up-sides). This technique limits missed CTCs to the detriment of erroneously arranging obvious traffic as incognito. A few circumstances might require focusing on accuracy as opposed to reviewing: inclining towards keeping bogus cautions low to the detriment of missing a few CTCs. Our assessment targets giving a thorough examination of different classifiers and exactness measures to give the adaptability to choose the classifier whose precision determinations that are generally pertinent to clients (partners). Thusly, we utilize the most famous exactness measures in AI and data recovery spaces. We list these actions and clarify every one next. Genuine Positive (TP) is the quantity of fragments (pictures) that are effectively delegated CTCs. Genuine Negative (TN) is the quantity of fragments that are effectively delegated non-CTC (obvious) channels. Bogus Positive (FP) is the numberof sections that are erroneously named CTC channels. Bogus Negative (FN) is the quantity of sections that are erroneously named non-CTC channels while, truth be told, they are CTCs.

Experimental Setup

To approve the exactness and productivity of our proposed approach, we present our exploratory outcomes and contrast them and three famous benchmark CTC discovery draws near. These identification approaches are the consistency test entropy test, and remedied restrictive entropy furthermore, to gauge and think about our methodology's viability in recognizing various kinds of secret channels, we consider various designs of undercover channels that reach from easy to covert CTCs that use progressed guard avoidance procedures.This kind of clandestine channel displays close unmistakable traffic conduct utilizing bundle between appearance times that are to some degree like clear traffic. Due to its similitude to obvious traffic, CCTC is a seriously moving kind of undercover channel to distinguish. Our third arrangement of assessment results shows the exhibition of our methodology for identifying Ultra-Cautious Covert Timing Channels (UCCTC). UCCTC is one of the most developed digital assaults which confines undercover channels from showing practices (parcel between appearance times) that stray from clear traffic. This limitation frequently forfeits the taken data's quality forcibly changing the bundles to happen inside a decreased time period. Nonetheless, this limitation makes this sort of cover channels the most hard to recognize because of the great closeness to obvious traffic conduct produced by non-malevolent applications.Then again, the proposed approach is as yet nonexclusive and should be tuned to hold fast to the association's security mission and requirements. In this segment, we talk about the tuning needed to accomplish the best outcomes utilizing snap Catch. The assessment of snap Catch shows that it accomplishes high precision and inclusion. In any case, our methodology actually presents some bogus up-sides (obvious traffic being dishonestly recognized) and some bogus negatives (vindictive traffic being erroneously missed/permitted). We have tried different things with different AI classifiers and determined their outcomes as far as accuracy and review. Various factors possibly are viewed as while choosing the most proper classifier dependent on the partner guard procedure.

Conclusions

We present Snap Catch, an original strategy for mechanize and precise discovery of clandestine planning stations. Snap Catch is intended to practice picture handling and AI methods for secret traffic location. To begin with, the framework changes over the between appearance seasons of traffic into hued pictures utilizing an inventive instrument that catches the substantial highlights of organization traffic an addresses them in hued pictures. By extricating strong and precise highlights from the shaded pictures, Snap Catch trains different AI classifiers to proficiently identify secretive channels dependent on a tunable protection system that focuses on (or balances) exactness and fulfillment. What's more, we propose a component to pinpoint the secret messages (i.e., set of parcels) inside a traffic stream to permit of dropping just a portion of the traffic stream that contains the clandestine message rather than the whole stream.Our assessment of Snap Catch shows that it beats the adjusted contingent entropy, entropy, and routineness approaches. Further, our methodology shows the least presentation misfortune in distinguishing little undercover messages and the super wary clandestine channels (UCCTC), the most developed kind of secret digital assaults. Snap Catch endlessly beats the gauge approaches in distinguishing the portions inside traffic streams that convey clandestine messages, which altogether decreases the deficiency of the nature of administration brought about by dropping incognito traffic streams. At long last, we give different situations and use cases for tuning Snap Catch to execute a guard methodology that fits the instrument clients' assets and security goals.

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. K. Biswas, D. Ghosal, and S. Nagaraja. A survey of timing channels and countermeasures. ACM Computing Surveys (CSUR), 50(1):1–39, 2017.
6. 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.
7. L. Chappell. Wireshark 101: Essential skills for network analysiswireshark solution series. Laura Chappell University, USA, 2017.
8. .O. Darwish, A. Al-Fuqaha, G. B. Brahim, and M. A. Javed. Using mapreduce and hierarchical entropy analysis to speed-up the detection of covert timing channels.In 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pages 1102–1107.IEEE, 2017.
9. F. Iglesias, V. Bernhardt, R. Annessi, and T. Zseby. Decision tree rule induction for detecting covert timing channels in tcp/ip traffic. In International Cross-Domain Conference for Machine Learning and Knowledge Extraction, pages 105–122. Springer, 2017
10. F. Iglesias and T. Zseby. Are network covert timing channels statistical anomalies? In Proceedings of the 12th International Conference on Availability, Reliability and Security, pages 1–9, 2017