ISSN: 2182-2069 / E-ISSN: 2182-2077

Study on Identification of Trojan Horse Infections for Securing Financial Cloud

Yoghesh Dharangutti[1*], Dr. Sumitra Padmanabhan[2], R. Hannah Jessie Rani[3], Manish Nagpal[4], Divya Paikaray[5], and Shreya Ghosal[6]

[1*]Assistant Professor, Symbiosis Centre for Advanced Legal Studies and Research (SCALSAR); Symbiosis Law School, Pune (SLS-P), Symbiosis International (Deemed University, India. yogesh.d@symlaw.ac.in, https://orcid.org/0000-0002-3437-6626

[2]Associate Professor, Department of uGDX, ATLAS SkillTech University, Mumbai, Maharashtra, India. sumitra.padmanabhan@atlasuniversity.edu.in, https://orcid.org/0000-0003-4846-080X

[3]Assistant Professor, Department of Electrical and Electronics Engineering, Faculty of Engineering and Technology, Jain (Deemed-to-be University), Bangalore, Karnataka, India. jr.hannah@jainuniversity.ac.in, https://orcid.org/0000-0002-5449-104X

[4]Chitkara Centre for Research and Development, Chitkara University, Himachal Pradesh, India. manish.nagpal.orp@chitkara.edu.in, https://orcid.org/0009-0000-9823-5251

[5]Assistant Professor, Department of Computer Science & IT, ARKA Jain University, Jamshedpur, Jharkhand, India. divya.p@arkajainuniversity.ac.in, https://orcid.org/0000-0001-7886-1538

[6]Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. shreya.ghosal.orp@chitkara.edu.in, https://orcid.org/0009-0002-8724-7315

Received: April 21, 2025; Revised: June 04, 2025; Accepted: July 24, 2025; Published: August 30, 2025

Abstract

An internet-wide computer network is made up of several machines that are connected, whether the network is built using traditional infrastructure or cloud computing technology. All of these goods, services and programs come together in one technical framework, together with a large amount of database storage, creating a valuable resource variety. Internet services that enable consumers to make use of the vast possibilities provided by cloud technology facilitate access to these products. Cloud computing's many benefits include low cost, easy-to-use self-service accessibility, built-in flexibility, smooth scalability, and efficient use of virtualised resources, which are driving creativity and effectiveness in contemporary technology paradigms. However, there are several security vulnerabilities in the cloud computing (CC) setup. Trojan horses (TH) are among the most frequent security issues in the context of computing in the cloud. The TH can compromise services offered by cloud computing and harm virtual machines, apps and resources in the cloud infrastructure. TH assaults could be hazardous, intricate and hard to identify. We begin by assembling an extensive dataset with TH Infections for Securing Financial Cloud data. We proposed the Adaptive Butterfly-optimised Hierarchical Random Forest (ABO-HRF) technique for accurately estimating TH detection. The suggested approach improves the accuracy (89.56%), precision (88.32%), recall (82.54%), and F1 score (84.68%) compared with the current methods.

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 3 (August), pp. 189-199. DOI: *10.58346/JISIS.2025.I3.013*

*Corresponding author: Assistant Professor, Symbiosis Centre for Advanced Legal Studies and Research (SCALSAR); Symbiosis Law School, Pune (SLS-P), Symbiosis International (Deemed University, India.

Keywords: Cloud Computing (CC), Dynamic Analysis (DA), Detection, Trojan Horse (TH), Machine Learning (ML), Security, Adaptive Butterfly-optimised Hierarchical Random Forest (ABO-HRF).

1 Introduction

A revolution in information Technology (IT), cloud computing (CC) leverages distant computers and the World Wide Web (WWW) to offer a shared pool of apps and processing facilities to meet its customers' needs (Grimes, 2019). This type of technology began in the latter part of the 2000s as the final phase of the creation of IT infrastructure, signalling a new paradigm in processing where users can use software and computational power over networking or the web (Rao et al., 2020). Additionally, a new paradigm for storing and delivering services over the Internet has emerged: cloud computing. Users can utilise cloud services from anywhere in the world via the Internet, which allows them to obtain pertinent data for their activities without interfering with the work of others or assigned assets (Liao et al., 2018). Companies can simultaneously run their software on several linked machines. Additionally, CC eliminates the requirement for users to install programs on their computers by allowing them to access resources and applications via internet access, regardless of the point in time, from any location. The appeal of CC has grown recently, and organisations and the IT sector worldwide are becoming more and more interested in it (Davis, 2020). Cloud technology encompasses a wide range of computer systems that are accessible over a network, often the Internet, including servers, apps, email, and storage for files, big assets, databases and applications. Despite all of these wonderful capabilities and advantages, CC is vulnerable to numerous security flaws and threats. The main worry with online computing is security breaches. Because of this, these assaults cause worry for users as well as suppliers of services (SudalaiMuthu, 2022). There are many other types of potential assaults, including phishing, malware insertion, denial-of-service, authorisation, and attackers-in-the-middle attacks. The CC infrastructure is thought to be very vulnerable to malware attacks. Trojan horses have recently gained more notoriety and danger, particularly in the context of CC and systems for computers (Abualhaj and Al-Khatib, 2024). A malicious application that could be loaded into cloud-based networks and do harm is known as a Cloud Trojan injection attack (Gunalan et al., 2023). These harmful programs can be sent to the clouds, performed in genuine situations, and integrated into lawful commands. Furthermore, installing a malicious service or application on the cloud platform is the aim of a cloud Trojan injection attack, (Balaji et al., 2023) according to Costales et al., (2020). The assault may modify cloud-based programmes or prevent them from operating as intended. The hacker attempts to utilise his harmful usage, client support, or device installations to penetrate the internet backbone (Xue et al., 2020). This study looks at the consequences of Trojan horse assaults in CC environments. TH detection could be precisely estimated using the Adaptive Butterfly-optimised Hierarchical Random Forest (ABO-HRF) approach.

Contributions of this Study

- This paper sheds light on the trends and tactics of TH assaults directed at the banking industry through experimentation and instances.
- This report provides useful suggestions for financial institutions to strengthen their safety measures based on their obstacles and conclusions.
- Financial institutions can apply the study's findings to make sure their security procedures comply with legal as well as business requirements.

The first section is determined by the following: The second part gives a related work of the research, the third section details the suggested approach, the fourth part explores the results, and the final section draws a conclusion.

2 Related Works

Srinivas et al., (2019) discussed cybersecurity risks, attacks, and countermeasures. Several standardisation issues in cybersecurity are covered. It also talks about the national policy for cybersecurity, which aims to secure cyberspace, as well as several government laws that safeguard cybersecurity. Despotović et al., (2023) examined financial technology-related cybercrime. The appearance of Fintech and the growing use of diverse digital and movable technology have resulted in extensive modifications to the expense system. Guha et al., (2023) examined hardware vulnerabilities, such as hardware TH might cause a dramatic increase in power consumption during runtime, while maintaining system performance, honesty, and secrecy. Labafniya et al., (2020) examined how hardware vulnerabilities, such as hardware trojan horses (HTH), might increase the dissipation of power abruptly during runtime, while maintaining system availability, integrity and secrecy. Prakash et al., (2023) examined a number of security issues related to cloud computing, examined some of the key topics in cloud safety research, suggested methods for securing the constantly changing cloud environment and provided a practical solution to the issues that cloud producers and buyers encounter. Makura et al., (2020) investigated the potential to change the harmful code invasion level of the cloud to a DFR technique that makes use of reasoning capture and data protection. Dai & Yao, (2019) examined an ML algorithm-based classification technique and suggested the User-Event Threat Matrix Model as a way to identify the affected users. It can identify people who are probably to get the virus while offering them special attention. Parmar & Gajjar, (2023) used an ML approach to meticulously investigate, assess and measure the performance of six distinct Trojan detection classifiers to completely comprehend their dependability, effectiveness, and precision in identifying malicious activities within the economic cloud (Supriya & Dhanalakshmi, 2024). In 2024, Rani et al., (2024) looked into a range of preventative and detection methods. The characteristics, advantages and disadvantages of each technique are used to evaluate how effective it is. More accurate results are produced by deep learning and machine learning algorithms for both recognised and unknown attack patterns. El-Sofany & Abou El-Seoud, (2019) evaluated the model's efficiency and performance, the analysis assessments are shown. The experimental findings showed great promise in defending mobile-based computing systems from denial-of-service assaults. Khalid et al., (2020) outlined an architectural paradigm for a Cloudlet-based system monitoring system. The study focuses on gathering data for a dynamic, (Sindhu, 2023) distributed and real-time capacity allocation that is tailored to the new urban paradigm and intended for mobile complex systems. Zhang, (2018) recommended implementing artificial intelligence in computer network security applications to safeguard computer safety. A TH detection model based on artificial intelligence was created and put to the test. Rosli et al., (2019) presented a clustering detection (eElankavi et al., 2017) method that analyses the characteristics of the malicious software to discover malware activity in data registry infestations using the K-Means clustering methodology. Methods of clustering that use unsupervised ML methods are essential for categorising comparable malware features based on behavioural analyses. (Assegid & Ketema, 2023).

3 Methodology

Describe the framework, networking setups and security features like firewalls, intrusion detection systems and access restrictions that make up the architecture of the financial cloud environment that was

used for the study. Highlighting the sensitivity of the information and the legal constraints surrounding which describe the different kinds of financial applications and data that are handled or stored in a cloud environment.

3.1. Data Collection

To collect benign examples and cloud TH, one can utilise Virus Total and VirusShare.com. Virus share stands as one of the biggest publicly accessible virus archives on the WWW. Alternatively, forensic investigators, disaster emergency personnel and security experts can obtain potentially harmful computer code through the Virus Total website, which is an archive for infection variants. Samples from Virus Total and virushare.com have been collected and gathered, including benign and TH samples. Many popular anti-virus programs, including Avira, Comodo, Bit Defender, F-Secure, Avast, Kaspersky Lab and AVG, were able to identify those samples. Afterwards, machine learning methods will be applied to this dataset to do additional spyware research (Sethi et al., 2019).

3.2. Adaptive Butterfly-Optimised Hierarchical Random Forest (ABO-HRF)

ABO-HRF, or Adaptive Butterfly Optimised Hierarchical Random Forest, is an approach to machine learning that blends components from several approaches to enhance random forest models' overall precision and performance, particularly while managing imbalanced data sets.

3.2.1. Hierarchical Random Forest (HRF)

Multiple investigations have demonstrated the random forest algorithm's superior accuracy in classification, noise, including outlier acceptance, and lack of overfitting tendency. The HRF technique presented in this research uses an adaptive parameter selection procedure to optimise the choice tree node splitting mechanism, hence increasing the algorithm's rate of classification. The distinct properties will result in multiple decision trees when alternative node-splitting strategies are chosen for a single dataset. It is determined that random forest categorisation has a variable level of accuracy. A novel splitting procedure is suggested, which is used for the selection and division of node attributes, once the decision tree is chosen. First, the optimal feature for dividing nodes into parts is chosen, and the node dividing process is divided into a linear mixture. The optimisation of node split is taken into consideration in the two methods, as Spark mllib's random forest method has been incorporated with ID3 and CART. The data concerning the gain and the Gini index are obtained when the sample set D is divided using characteristics and displayed in the node splitting formula.

$$gain(s,b) = Ent(C) - \sum_{u=1}^{U} \frac{|C^u|}{C} Ent(C^u) \quad (1)$$

$$Gini(C,b) = \sum_{u=1}^{U} \frac{|C^u|}{C} Gini(C^u) \quad (2)$$

When C^u denotes that every sample in the $C$with an amount of v a on the property and contained in the $|C^u|$ branched node.

$$Gini(C) = \sum_{l=1 l' \neq l}^{|z|} \sum O^l O^l = 1 - \sum_{l=1}^{|z|} Ol^2 \quad (3)$$

$$G = \min_{\alpha,\beta \epsilon Q} E\{C,b\} = \alpha Gini(C,b) - \beta Gain(C,b) \quad (4)$$

The combination node splitting formula and the adaptive variable choice method are as follows, because the idea of node splitting ought to be focused on the increased cleanliness of a data set following division.

$$t.s\begin{cases}\alpha+\beta=1\\0\le\alpha,\beta\le 1\end{cases} \quad (5)$$

Here, α,βstands for the characteristic's splitter weight factor. To find the best combination of variables, the adaptive selection of parameters method is used. This indicates that to maximise the categorisation impact, ID3 and CART are considered to be the best choices for node partitioning criteria. The accuracy rate and categorisation rate of errors are utilised in the study to gauge success. Formula 6 defines sample D's categorisation rate of errors.

$$F(e;C)=\frac{1}{n}\sum_{j=1}^{n}\mathrm{II}\big(e\big(w_j\big)\neq z_j\big) \quad (6)$$

Formula 7 defines the accuracy rate.

$$acc(e;C)\frac{1}{n}\sum_{j=1}^{n}\mathrm{II}\left(e\big(w_j\big)\neq z_j\right)=1- \quad (7)$$

The remaining part compares and validates the experimental results.

3.2.2. Adaptive Butterfly Optimization (ABO)

We provide a better Adaptive butterfly optimisation method that makes use of chaotic maps to address the algorithm's early problems with convergence, as well as issues with being trapped in local optima. In the field of optimisation, a vast array of chaotic maps is employed. The 10 chaotic maps that have been utilised the most often in the literature, however, were chosen and used in this investigation. Unpredictable maps get their term from the Greek word chaos, which describes the state of the cosmos before order, when everything was dissonant, chaotic, and empty. The expression mapping in this context refers to matching or associating with certain parameters through algorithmic behaviour that can be best defined as chaotic. Consequently, chaotic maps are those that depict the intricate and dynamic behaviour of systems that are not linear. Recently, fractal maps have gained a lot of recognition in the optimisation community for their fluid behaviour, which enables optimisation techniques to more thoroughly and actively explore the area of search. It only exhibits predictable behaviour at first; after that, it acts erratically. Chebyshev map: Equation (8) provides an equation for the Chebyshev maps.

$$w_{l+1}=cos\big(kcos^{-1}(w_l)\big) \quad (8)$$

Circle map: Equation (9) provides an equation for the Circular map.

$$w_{l+1}=w_l+0.2-(0.5-2\pi)sin(2\pi w_l)mod(1) \quad (9)$$

Gauss map: Equation (10) displays the Gauss map equation.

$$w_{l+1}=\begin{cases}0 & w_l=0\\ \frac{1}{w_l mod(1)} & değilse\end{cases} \quad (10)$$

Iterative map: Equation (11) provides an equation that describes the iterative map.

$$w_{l+1}=sin\left(\frac{0.7\pi}{w_l}\right) \quad (11)$$

Logistic map: Equation (12) displays the formula for the Logistic map.

$$w_{l+1}=4w_l(1-w_l) \quad (12)$$

Piecewise map: Equation (13) provides an equation for the individual maps.

$$w_{l+1}=\begin{cases}\frac{w_l}{O} & 0\le w_l\le O\\ \frac{w_l-O}{0.5-O} & O\le w_l\le O.5\\ \frac{1-O-w_l}{0.5-O} & 0.5\le w_l\le 1-O\\ \frac{1-w_l}{O}1-O\le w_l\le 1\end{cases} \quad (13)$$

Sine map: Equation (14) provides an equation for the Gaussian map.

$$w_{l+1} = \frac{\alpha}{4} sin(\pi w_l) \quad (14)$$

Singer map: Equation (15) provides the Singer map equation.

$$w_{l+1} = O\left(7.86w_l - 23.31\, w_l^2 + 28.75\, w_l^3 + 13.302875\, w_l^4\right) \quad (15)$$

Where the actual values of the control variable, P, range from 0.9 to 1.08. Sinusoidal map: Equation (16) provides a formula for the Sinusoidal shape map.

$$w_{l+1} = sin(\pi w_l) \quad (16)$$

Tent map: Equation (17) provides the formula for the Tent map.

$$w_{l+1} = \begin{cases} \frac{w_l}{0.7} w_l < 0.7 \\ \frac{10}{3}(1 - w_l) w_l < 0.7 \end{cases} \quad (17)$$

The fundamental component of the BOA creates equilibrium among the equations indicated in Eqs. The value of the parameter p is found in equations (16)–(17). The BOA method was seen to have the following parameter, p, set at 0.8.

4 Results

We used Keras and Python 3.8 to construct the recommended deep-learning models. Furthermore, our PC machine was configured with "TensorFlow and the CuDNN library based on the GPU" to facilitate the usage of parallel processing. A PC server with an Intel Compassion i7-7700 HQ CPU @ 2.80 GHz processor, 16 GB of RAM, and a 6 GB Nvidia GeForce 1060 graphics license was used for the research. The existing methods of Support Vector Classifier (SVC) (Kimmell et al., (2021), K-nearest neighbour (KNN) (Kimmell et al., (2021), Gradient Boosted Classifiers (GBC) (Kimmell et al., 2021). Performance metrics comprise guess, Precision, Recall, and F1-Score.

Accuracy: Accuracy is measured by comparing the actual labels in the input data with the expected labels. The prediction is considered accurate if the predicted and actual labels coincide. It stands for a portion of all correctly classified data cases. Table 1 and Figure 1 display our proposed solution's accuracy comparison with alternative approaches. When compared to the existing methodologies, the suggested ABO-HRF achieved a greater accuracy of 89.56%. The existing methodologies, including SVC (Kimmell et al., 2021), achieving an accuracy of 87.56%, KNN (Kimmell et al., 2021) demonstrating a performance of 72.34%, and GBC (Kimmell et al., 2021) achieving an accuracy of 81.47%. The table shows the overall performance of existing and proposed methods.

Table 1: Comparison of Existing and Proposed Methods

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
SVC (Kimmell et al., (2021))	87.56	86.2	80.91	83.47
KNN (Kimmell et al., (2021))	72.34	66.6	57.67	61.81
GBC (Kimmell et al., (2021))	81.47	75.22	77.87	76.57
ABO-HRF [Proposed]	89.56	88.32	82.54	84.68

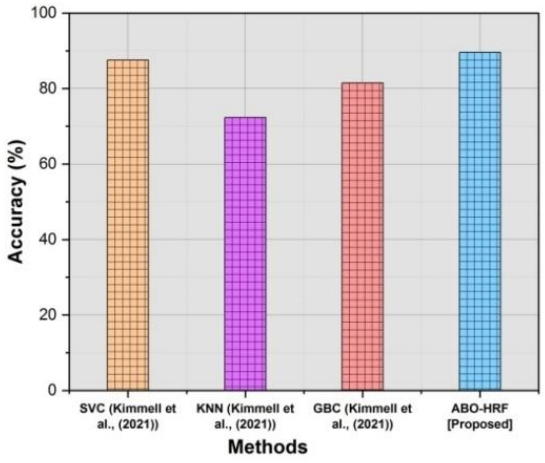

Figure 1: Analysis of Accuracy

Precision: Precision is a frequently used outcome variable, especially in classification tasks. The number of real positive predictions, also known as good guesses, is determined by a model based on the overall number of optimistic forecasts generated by the example. The accuracy comparisons in Figure 2 demonstrate how much better our proposed technique works than more traditional approaches. In contrast to the prevailing methodologies, the newly introduced ABO-HRF demonstrated an enhanced precision of 88.32%. Among the current approaches, SVC (Kimmell et al., 2021) attained an accuracy of 86.2%, KNN (Kimmell et al., 2021) showcased a performance of 66.6%, and GBC (Kimmell et al., 2021) achieved an accuracy of 75.22%.

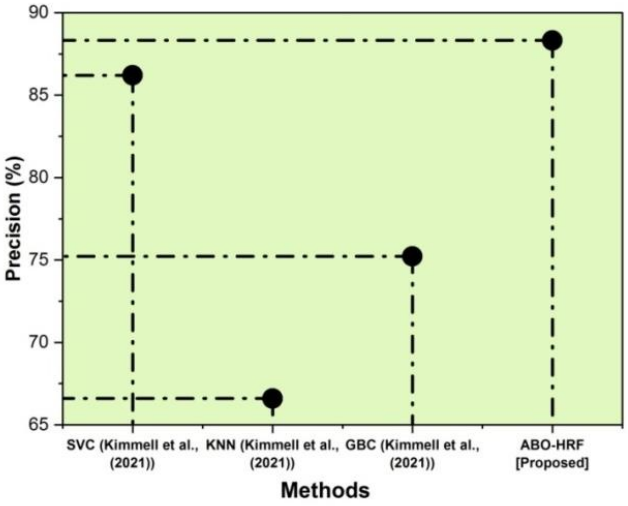

Figure 2: Analysis of Precision

Recall: Recall is a crucial performance measure in deep learning, particularly for classification problems. It is also frequently referred to sensitive or real positive rate. Among all actual occurrences of optimists in the data collection, it calculates the percentage of precise positive expectations. Our suggested technique beats other existing Strategies, as shown by the recall data displayed in Figure 3. In contrast to the prevailing methodologies, the proposed ABO-HRF exhibited a notably higher recall rate

of 82.54%. Among the prevalent techniques, SVC (Kimmell et al., 2021) attained an accuracy of 80.91%, KNN (Kimmell et al., 2021) showcased a performance level of 57.67%, and GBC (Kimmell et al., 2021) achieved an accuracy of 77.87%.

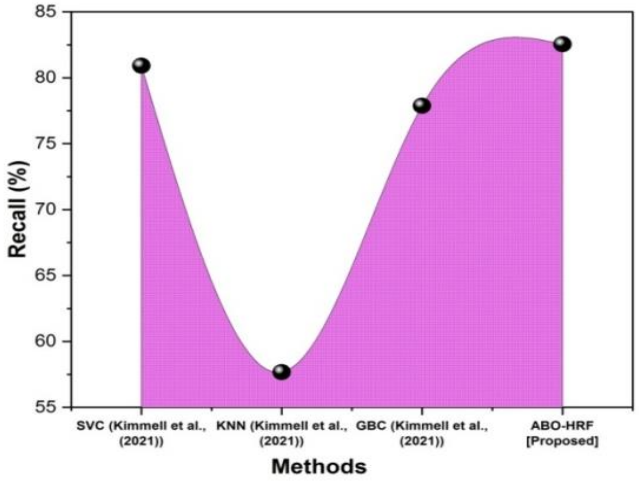

Figure 3: Analysis of Recall

F1 Score: The F1 score is an achievement metric that is extensively used, particularly for jobs involving categorisation. A single number that adds the two measurements while maintaining their respective positions is produced by the accurate harmonic average of recall. We compare the F1-scores in Figure 4 to demonstrate that our suggested approach outperformed other methods in use. Comparing the recommended ABO-HRF to the existing methods, it received an improved rating of 84.68%. These are the present-day methods: SVC (Kimmell et al., 2021) with 83.47% accuracy, KNN (Kimmell et al., 2021) with 61.81% efficiency, and GBC (Kimmell et al., 2021) with 76.57% performance.

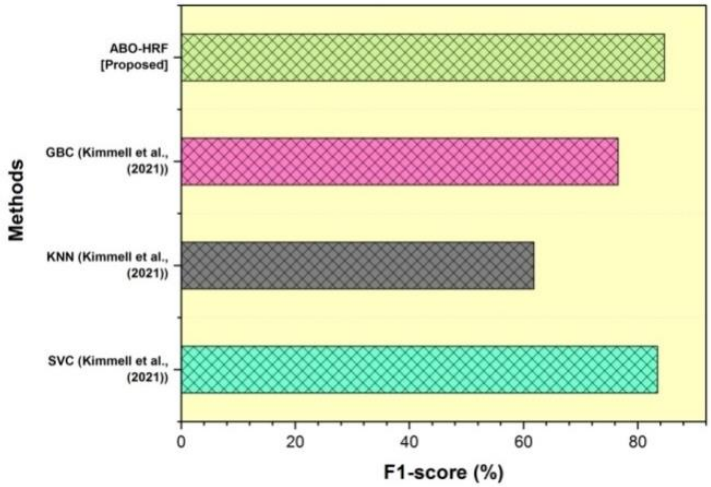

Figure 4: Analysis of F1 Score

5 Conclusion

The study highlights the necessity of detecting TH infections in cloud financial systems and putting suitable safeguards in place to protect confidentiality, accuracy of data and system security. When it

comes to identifying malicious activity, each of the methods of surveillance covered in this study behaviour analysis, detection using signatures, anomaly detection and so forth, has a distinct advantage. The ability to use ML approaches to lower false positives and raise detection accuracy strengthens the overall safety posture of financial cloud systems. Salient characteristics are identified. Many machine learning classifiers are evaluated for accuracy using the cloud TH dataset and Weka software. An 84.68% F1score, 82.54% recalls, 88.32% precision, and 89.56% accuracy could be obtained with the recommended approach. To increase the precision of TH detection in the CC environment study is required. Trojan horses are often designed with specific software bugs or operating systems in mind. Their effectiveness declines across varieties or systems. Future horse Trojans may employ more sophisticated evasion techniques to sidestep security precautions. Among these compounds is the flexible code, which becomes more difficult to identify since it changes with each infection.

References

[1] Abualhaj, M. M., & Al-Khatib, S. N. (2024). Using decision tree classifier to detect Trojan Horse based on memory data. *TELKOMNIKA (Telecommunication Computing Electronics and Control), 22*(2), 393-400. http://doi.org/10.12928/telkomnika.v22i2.25753

[2] Assegid, W., & Ketema, G. (2023). Harnessing AI for Early Cancer Detection through Imaging and Genetics. *Clinical Journal for Medicine, Health and Pharmacy, 1*(1), 1-15.

[3] Balaji, R., Deepakkumar, A., Prabhu, G., Thinakaran, P., & Gowtham, S. (2023). Enhancing Network Security by using SDN Algorithm in Cloud Computing. *International Academic Journal of Science and Engineering, 10*(1), 14–19.

[4] Costales, R., Mao, C., Norwitz, R., Kim, B., & Yang, J. (2020). Live trojan attacks on deep neural networks. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops* (pp. 796-797).

[5] Dai, X., & Yao, L. (2019, August). A classification method and implementation of Trojan and BotNet infected user based on threat matrix model. In *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)* (pp. 1231-1236). IEEE. https://doi.org/10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00229

[6] Davis, S. L. (2020). The trojan horse: Digital health, human rights, and global health governance. *Health and Human Rights, 22*(2), 41-47.

[7] Despotović, A., Parmaković, A., & Miljković, M. (2023). Cybercrime and cyber security in fintech. In *Digital transformation of the financial industry: approaches and applications* (pp. 255-272). Cham: Springer International Publishing. https://doi.org/10.1016/S2212-5671(15)01440-9

[8] Elankavi, R., Kalaiprasath, R., & Udayakumar, R. (2017). A fast clustering algorithm for high-dimensional data. *International Journal of Civil Engineering and Technology (Ijciet), 8*(5), 1220-1227.

[9] El-Sofany, H., & Abou El-Seoud, S. (2019). A novel model for securing mobile-based systems against DDoS attacks in cloud computing environment. *IJIM, 13*(1) 85-98.

[10] Grimes, D. R. (2019). A dangerous balancing act: On matters of science, a well-meaning desire to present all views equally can be an Trojan horse for damaging falsehoods. *EMBO reports, 20*(8), e48706. https://doi.org/10.15252/embr.201948706

[11] Guha, K., Majumder, A., Saha, D., & Chakrabarti, A. (2020, November). Ensuring green computing in reconfigurable hardware based cloud platforms from hardware trojan attacks. In *2020 IEEE REGION 10 CONFERENCE (TENCON)* (pp. 1380-1385). IEEE. https://doi.org/10.1109/TENCON50793.2020.9293796

[12] Gunalan, N., Kavin Kumar, R., Saravanan, B., Surya, S., & Saran Sujai, T. (2023). Investing Data Flow Issue by using Rayleigh Model in Cloud Computing. *International Academic Journal of Innovative Research, 10*(1), 8–13.

[13] Khalid, H., Hashim, S. J., Ahmad, S., Hashim, F., & Chaudary, M. A. (2020). Cybersecurity in Industry 4.0 context: Background, issues, and future directions. *The nine pillars of technologies for industry*, *4*, 263-307.

[14] Kimmell, J. C., Abdelsalam, M., & Gupta, M. (2021, August). Analyzing machine learning approaches for online malware detection in cloud. In *2021 IEEE International Conference on Smart Computing (SMARTCOMP)* (pp. 189-196). IEEE. https://doi.org/10.1109/SMARTCOMP52413.2021.00046

[15] Labafniya, M., Picek, S., Borujeni, S. E., & Mentens, N. (2020). On the feasibility of using evolvable hardware for hardware Trojan detection and prevention. *Applied Soft Computing*, *91*, 106247. https://doi.org/10.1016/j.asoc.2020.106247

[16] Liao, X., Alrwais, S., Yuan, K., Xing, L., Wang, X., Hao, S., & Beyah, R. (2018). Cloud repository as a malicious service: challenge, identification and implication. *Cybersecurity*, *1*, 1-18. https://doi.org/10.1186/s42400-018-0015-6

[17] Makura, S. M., Venter, H. S., Ikuesan, R. A., Kebande, V. R., & Karie, N. M. (2020, February). Proactive forensics: Keystroke logging from the cloud as potential digital evidence for forensic readiness purposes. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)* (pp. 200-205). IEEE. https://doi.org/10.1109/ICIoT48696.2020.9089494

[18] Parmar, R., & Gajjar, N. (2023, December). Enhancing Trojan Detection using Machine Learning: Comparative Analysis of Classifier Performance on Embedded Hardware. In *2023 9th International Conference on Signal Processing and Communication (ICSC)* (pp. 331-338). IEEE. https://doi.org/10.1109/ICSC60394.2023.10440994

[19] Prakash, N., Gobichettipalayam, T. N. I., & Annapoorani, S. (2023). Network Security and Issues in Private Cloud. *Journal of Data Acquisition and Processing*, *38*(3), 1552.

[20] Rani, P., Singh, S., & Singh, K. (2024). Cloud computing security: a taxonomy, threat detection and mitigation techniques. *International Journal of Computers and Applications*, 1-14. https://doi.org/10.1109/ICSC60394.2023.10440994

[21] Rao, Y. S., Keshri, A. K., Mishra, B. K., & Panda, T. C. (2020). Distributed denial of service attack on targeted resources in a computer network for critical infrastructure: A differential e-epidemic model. *Physica A: Statistical Mechanics and Its Applications*, *540*, 123240. https://doi.org/10.1016/j.physa.2019.123240

[22] Rosli, N. A., Yassin, W., Faizal, M. A., & Selamat, S. R. (2019). Clustering analysis for malware behavior detection using registry data. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *10*(12), 93-102.

[23] Sethi, K., Kumar, R., Sethi, L., Bera, P., & Patra, P. K. (2019, June). A novel machine learning based malware detection and classification framework. In *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-4). IEEE. https://doi.org/10.1109/ICCCNT49239.2020.9225627

[24] Sindhu, S. (2023). The Effects of Interval Uncertainties and Dynamic Analysis of Rotating Systems with Uncertainty. *Association Journal of Interdisciplinary Technics in Engineering Mechanics, 1*(1), 49-54.

[25] Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future generation computer systems*, *92*, 178-188. https://doi.org/10.1016/j.future.2018.09.063

[26] SudalaiMuthu, T. (2022, November). Kernel Rootkit Secret Detection in Cloud Computing. In *2022 1st International Conference on Computational Science and Technology (ICCST)* (pp. 276-280). IEEE. https://doi.org/10.1109/ICCST55948.2022.10040354

[27] Supriya, S., & Dhanalakshmi, K. (2024). Review of Task Offloading and Dynamic Scheduling Methods in Edge-Cloud Computing. *International Journal of Advances in Engineering and Emerging Technology*, *15*(1), 13–18
[28] Xue, M., Gu, C., Liu, W., Yu, S., & O'Neill, M. (2020). Ten years of hardware Trojans: a survey from the attacker's perspective. *IET Computers & Digital Techniques*, *14*(6), 231-246. https://doi.org/10.1049/iet-cdt.2020.0041
[29] Zhang, J. (2018). Application of Artificial Intelligence Technology in Computer Network Security. *International Journal of Network Security*, *20*(6), 1016-1021.

Authors Biography

Yoghesh Dharangutti is an Assistant Professor at the Symbiosis Centre for Advanced Legal Studies and Research (SCALSAR), Symbiosis Law School, Pune (SLS-P), a constituent of Symbiosis International (Deemed University), India. His academic interests focus on advanced legal studies, policy analysis, and interdisciplinary legal research. He actively contributes to legal education, student mentorship, and scholarly research.

Dr. Sumitra Padmanabhan is an Associate Professor in the Department of uGDX at ATLAS SkillTech University, Mumbai, Maharashtra, India. With expertise in design, innovation, and interdisciplinary education, she is actively engaged in guiding students and contributing to academic research. Dr. Padmanabhan's work focuses on nurturing creative problem-solving, design thinking, and experiential learning.

R. Hannah Jessie Rani is an Assistant Professor in the Department of Electrical and Electronics Engineering, Faculty of Engineering and Technology, at Jain (Deemed-to-be University), Bangalore, Karnataka, India. She is actively involved in teaching and research in the field of electrical and electronics engineering, with interests in power systems, control engineering, and emerging technologies. Hannah is committed to academic excellence, innovation, and the holistic development of her students.

Manish Nagpal is affiliated with the Chitkara Centre for Research and Development at Chitkara University, Himachal Pradesh, India. His research interests focus on interdisciplinary studies, research impact assessment, and academic development. He is actively involved in fostering innovation, supporting academic research activities, and enhancing the overall research ecosystem within the institution.

Divya Paikaray is an Assistant Professor in the Department of Computer Science & IT at ARKA JAIN University, Jamshedpur, Jharkhand, India. She is actively engaged in teaching and research in the field of computer science, with interests in areas such as data science, software development, and emerging technologies. Divya is committed to academic excellence and to guiding students in developing technical and analytical skills.

Shreya Ghosal is affiliated with the Centre of Research Impact and Outcome at Chitkara University, Rajpura, Punjab, India. Her academic interests focus on research assessment, research impact enhancement, and interdisciplinary collaboration. She is actively involved in supporting research development initiatives, contributing to the growth of institutional research capacities.