British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 8, Issue 2, 2025 (pp. 71-98)
www.abjournals.org

ENHANCED KEYLOGGER CLASSIFICATION USING DEEP LEARNING: A SYSTEMATIC REVIEW

Peter S. Idowu[1] and Folashade Y Ayankoya (Ph.D.)[2]

[1,2]Department of Computing Science, Babcock University, Ilishan-Remo, Ogun State, Nigeria.

Emails:
[1]idowu0055@pg.babcock.edu.ng: [2]ayankoyaF@babcock.edu.ng

Cite this article:

Idowu, P. S., Ayankoya, F. Y. (2025), Enhanced Keylogger Classification Using Deep Learning: A Systematic Review. British Journal of Computer, Networking and Information Technology 8(2), 71-98. DOI: 10.52589/BJCNIT-JGXGNUTR

Manuscript History

Received: 20 May 2025

Accepted: 23 Jun 2025

Published: 14 Jul 2025

ABSTRACT: *This systematic review explores methodologies for detecting and mitigating keyloggers, pervasive cybersecurity threats that surreptitiously capture keystrokes. After conducting thorough database searches, 26 relevant studies were found, showing a wide range of methods including machine learning algorithms, heuristic techniques, and behavior-based strategies. The review underscores the efficacy of combining proactive and reactive measures in countering keylogger threats, with machine learning algorithms exhibiting varying degrees of success. Significantly, creating interfaces that are easy for users to use is found to be a crucial element in improving user knowledge and making it easier to take quick action. However, the analysis also points out some drawbacks, such as the lack of extended verification for suggested approaches and variations in how algorithms are designed in different research. These findings underscore the imperative for ongoing innovation and collaboration among practitioners and policymakers to develop standardized protocols and address emerging threats comprehensively. Overall, this review offers valuable information on how to detect and prevent keyloggers, which can help direct future research in this important area.*

KEYWORDS: keyloggers, cybersecurity, detection, mitigation, machine learning, heuristic techniques, behavior-based strategies, systematic review, user-friendly interfaces, cybersecurity threats.

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

INTRODUCTION

In 1984, 16 electromechanical bugs were found in IBM Selectric II and Selectric III typewriters at the US Embassy in Moscow and the US Consulate in Leningrad [6].The Soviet Union (USSR) created the bugs, which pointed out six magnetometers that sensed the activation of six different levers in the Selectric typewriter with every key press. The Selectric Bug's bizarre blend of enacted levers permitted it to observe which key had been pushed whereas neglecting Move, Space, and a few other non-letter keys.. Up to 8 key presses were stored in an 8×4-bit core memory, and when this became full the memory contents were transmitted via radio bursts to a nearby listening post [19]. The Soviets developed at least 5 versions of the Selectric Bug which enabled them to log the keystrokes of their adversaries for more than 8 years [6].

Keystroke logging, or keylogging is the hone of recording the key clients' sorts on a keyboard which serve both legitimate and illegitimate purposes which give a tremendous danger to cybersecurity, capturing keystrokes to accumulate delicate data including passwords, credit card numbers, and individual communications [11]. These methods have gotten to be progressively advanced, in spite of current solutions, keyloggers proceed to pose a risk to security frameworks because of their capacity to elude standard protections and easily integrate into compromised frameworks [14].

This efficient survey intends to develop a system for distinguishing and decreasing keylogger threats in real-time [17]. By looking at current studies, this review seeks to pinpoint the most effective algorithms for identifying keystroke designs and unauthorized keyboard access. Moreover, it evaluates distinctive mitigation techniques to recognize the most effective strategies for maintaining a strategic distance from and overseeing keylogger threats. Besides, the review delves into the advancement of user-friendly interfaces that can offer prompt alerts, in-depth reports, and recommended actions to improve user understanding and empower incite mediation [26].

Keyloggers are becoming increasingly popular owing to their clandestine nature [14]. They operate discreetly and can evade detection by antivirus software. Regardless, it is important to implement security measures to prevent keyloggers such as Firmware, and to install other precautionary software. Guaranteeing that security patches are continually updated. Applications must be downloaded from genuine sources, and as it were authorized software ought to be utilized. Another basic strategy to detect malicious keylogger threats is to routinely check the CPU and memory utilization of the machine [21].

A check uncovered that Mr.Lopez's computer was contaminated with a hurtful program.Coreflood logs each keystroke and sends this data to pernicious actors through the Web.

This is how the software engineers procured Joe Lopez's customer name and password.In February 2014, an article on www.nrk.no reported that the Norwegian Police Security Service (PST) asked for lawmakers' permission to implement methods to monitor the computer systems of individuals under scrutiny.One way to do this is by secretly installing a valid keylogger on the remote computer in order to record keystrokes [14].

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

Rationale

- Keyloggers, which are widely used secretly to record keystrokes to gather sensitive data such as passwords, credit card information, and personal messages, posing a crucial threat to internet security. The increasing exploit of keylogger techniques has transformed them into an ongoing and challenging issue. Security methods often fall short in detecting and mitigating keyloggers as they have the ability to seamlessly blend into compromised systems and evade standard detection techniques [25]. Multiple studies have suggested different methods to combat keylogger dangers, spanning from heuristic and signature-based identification to more advanced machine learning and behavior-based strategies [1],[7],[9],[10],[21]. On the best approaches of detecting and fixing problems in real time, there is still disagreement, nevertheless. Furthermore, as it is essential for improving user awareness and responsiveness, more research must be done on the integration of user-friendly interfaces that offer timely notifications and helpful insights. Given the critical importance of protecting sensitive information and the ongoing evolution of keylogger threats, a systematic review is warranted to consolidate existing knowledge and identify the most promising strategies for developing an effective detection and mitigation system [25]. Through combining information from various studies, this review seeks to underscore the pros and cons of current methods, pinpoint deficiencies in the current body of literature, and offer a distinct path for upcoming research and innovation in this area. The rationale for this systematic review is grounded in the urgent need to advance cybersecurity measures against keyloggers. By comprehensively evaluating the effectiveness of various detection algorithms, mitigation strategies, and user interface designs, this review will contribute to the development of more robust and comprehensive solutions to safeguard sensitive information from keylogger attacks.

Objectives

i. Design and implement a framework capable of detecting keylogger activities in real-time. This involves developing algorithms that can identify abnormal keystroke patterns, unauthorized access to keyboard data, and any anomalies indicating keylogger presence.

ii. To evaluate and compare different mitigation strategy to protect and control keyloggers

iii. To Develop a user-interface to alert users on keylogger threats, provide detailed reports that recommend action to enhance awareness and intervention.

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

MATERIAL AND METHODS

Eligibility Criteria

The eligibility criteria for this review ensure the inclusion of studies focusing on the development and implementation of effective systems, techniques, methods, or strategies for detecting and mitigating keylogger activities. The approach captures a wide range of relevant research while maintaining a focus on high-quality, peer-reviewed studies.

Studies published from January 2014 to May 2024 were included in ensuring that the review reflects contemporary research and the latest advancements in keylogger detection and mitigation technologies. Only English-Language studies were considered to maintain consistency and ensure accurate interpretation and analysis.

The review concentrated on peer-reviewed journal articles to ensure the inclusion of high-quality research that has undergone rigorous peer review. Other document types, such as conference papers, book chapters, theses, and gray literature, were excluded to maintain a high standard of evidence.

Eligible studies had to explicitly address the development or implication of algorithms, systems, or strategies for detecting and mitigating keylogger activities. The primary focus needed to be on cybersecurity measures aimed at identifying abnormal keystroke patterns, unauthorized access to keyboard data, and other anomalies that indicate the presence of keyloggers.

The review included studies utilizing a combination of machine learning techniques, heuristic analysis, and behavior-based detection methods. This broad spectrum of methodological approaches aimed to provide a comprehensive understanding of the current state of keylogger detection technologies.

Studies evaluating and comparing different mitigation strategies for protecting against and controlling keyloggers were included. This encompassed both proactive measures (e.g., software hardening, encryption) and reactive measures (e.g., removal tools, isolation of infected components).

Additionally, this study discusses the development of user interfaces designed to alert users about keylogger threats, provide detailed reports, and recommend actions were included. The emphasis on user interfaces highlights the importance of usability and user awareness in the overall effectiveness of keylogger mitigation strategies.

To provide a varied variety of viewpoints and applications, research undertaken in governmental, business, and academic settings was included. Research that did not immediately aid in the creation or assessment of keylogger mitigation and detection techniques was disregarded.

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

Search Strategy

The search plan included three main databases: Scopus, ScienceDirect, and Google Scholar. Every database utilized a customized search term to guarantee the extraction of pertinent research.

Scopus

The search string utilized in Scopus was:

TITLE-ABS-KEY ((develop* OR implement*) AND (effect*) AND (system OR technique* OR method OR approach OR strategy) AND (detect* OR identificat* OR discovery OR recogni*) AND (mitigat* OR prevent* OR control OR reduction) AND (keylogger* OR keystroke* OR "keystroke recorder" Or "Keyboard monitor*")) AND PUBYEAR > 2013 AND PUBYEAR < 2025 AND (LIMIT-TO (DOCTYPE,"ar")) AND (LIMIT-TO (SRCTYPE,"j")) AND (LIMIT-TO (LANGUAGE,"English"))`

The search string encompassed a broad spectrum of keywords related to keylogger detection and mitigation, including terms such as "develop," "implement," "effect," "system," "technique," "method," "approach," "strategy," "detect," "identification," "discovery," "mitigate," "prevent," "control," "reduction," "keylogger," "keystroke," "keystroke recorder," and "keyboard monitor." These keywords were tailored to capture relevant literature across various methodological approaches and application settings.

ScienceDirect

In ScienceDirect, the search query was:

("Developing an Effective System for Detecting and Mitigating Keyloggers")

This query focused on identifying articles with specific mentions of machine learning, predicting, lung cancer or pulmonary carcinoma, outcome, and xenograft models.

Google Scholar

For Google Scholar, the search query used was:

"Developing an Effective System for Detecting and Mitigating Keyloggers"

Each search string was designed to capture relevant studies while aligning with the unique features and search capabilities of the respective databases.

In total, the search yielded 46 records from Scopus, 156 from ScienceDirect, and 81 from Google Scholar, resulting in 283 records identified collectively. Following screening and eligibility assessment, 26 studies met the inclusion criteria and were included in the review. This rigorous search strategy ensured a comprehensive selection of relevant literature for analysis, encompassing studies that utilized machine learning in predictive modeling of lung cancer outcomes using xenograft models.

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

Selection Process

The systematic review employed a meticulous search strategy across three primary databases: Scopus, ScienceDirect, and Google Scholar. Each database utilized tailored search strings to capture relevant studies focusing on machine learning in predicting lung cancer outcomes using xenograft models.

During the selection process, 46 records were identified from Scopus, 156 from ScienceDirect, and 81 from Google Scholar. After removing duplicates and screening, 283 records were reviewed, with 33 reports sought for retrieval. Seven reports were not retrieved, and 26 reports were assessed for eligibility. Ultimately, 26 studies were included in the review.

Following the screening and eligibility assessment, 26 studies that met the inclusion criteria were added to the systematic review. These research projects gave us a better understanding of how development of an effective system can be used to detect and mitigate keylogger. The thorough selection process guaranteed a detailed examination of pertinent literature on the subject, aiding in a nuanced comprehension of the topic.

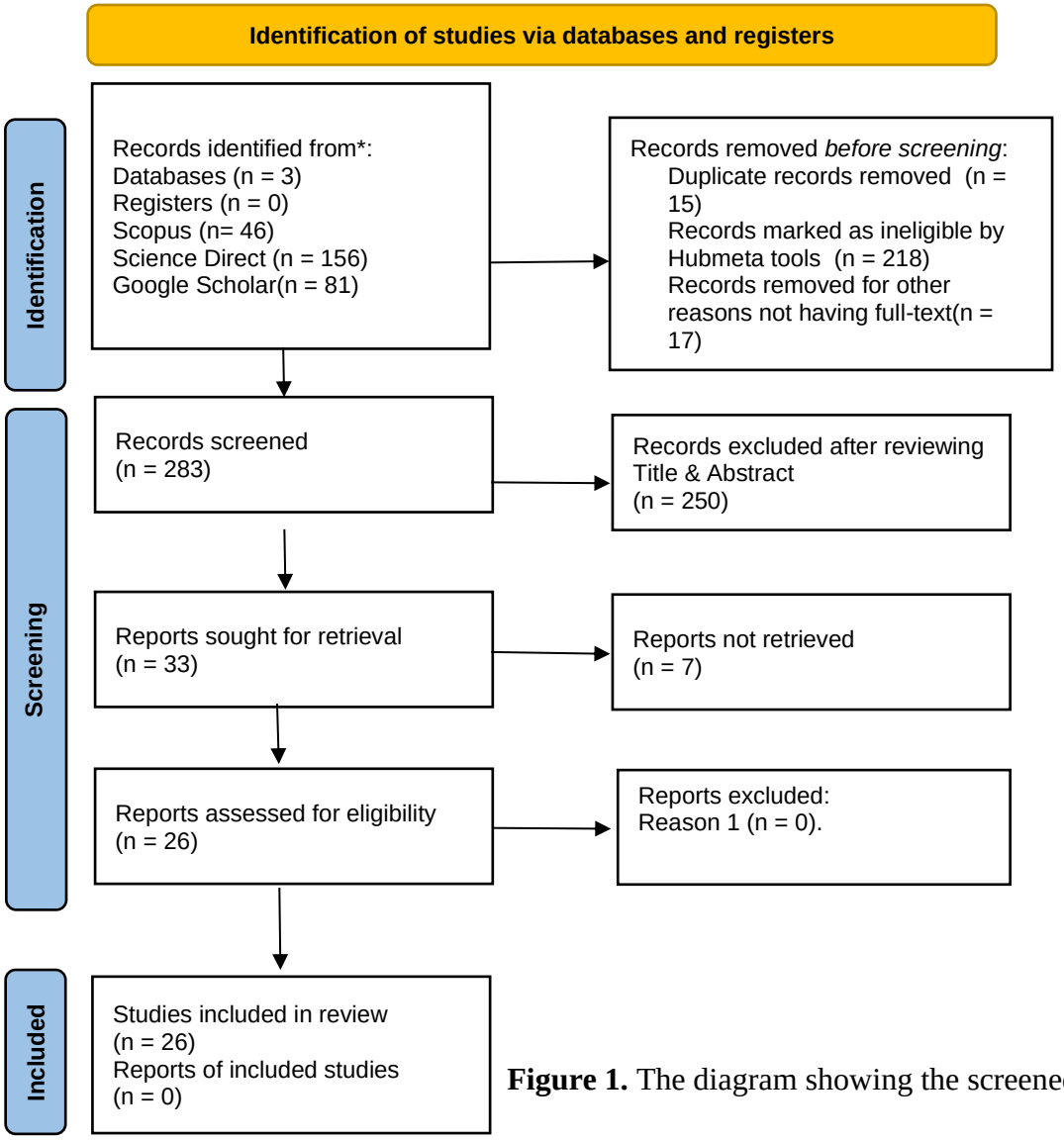

Figure 1. The diagram showing the screened studies

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

Data Collection Process

Data was extracted from the selected studies based on predefined criteria, focusing on the development and effectiveness of detection and mitigation strategies for keyloggers. Key data items included the type of algorithm or method used, the success rate of detection, mitigation strategies, user interface designs, and the context of application (e.g., governmental, business, academic).

Data Items

Data extraction focused on multiple outcome domains, including machine learning techniques, predictive models, lung cancer outcomes, and xenograft models. Participant characteristics, intervention details, study design, funding sources, ethical approval, publication characteristics, data availability, and conflicts of interest were also considered. Transparent documentation of assumptions made in the absence of information ensured a comprehensive and reproducible data extraction process.

Study Risk of Bias Assessment

The risk of bias in individual studies was assessed using standard criteria, including the clarity of research objectives, methodology rigor, transparency in data analysis, and the presence of any conflicts of interest. This assessment helped ensure the reliability and validity of the findings included in the review.

Effect Measures

In ensuring various effect measures, including Classification Accuracy, Area Under ROC Curve, Hazard Ratios, Odds Ratios/Risk Ratios, Mean Differences/Standardized Mean Differences, Tumor Growth Inhibition, Response Rate, and Survival Rates, were employed based on the nature of the outcome domains. Descriptive statistics and proportions were used for summarizing participant and intervention characteristics, study design, funding sources, ethical approval, publication characteristics, data availability, and conflicts of interest.

Synthesis Methods

The synthesis process followed a systematic approach, involving criteria definition, screening based on the title and abstracts, full-text assessment, data extraction, tabulation, and comparison.

Transparent documentation and regular communication between reviewers has ensured consensus in decision-making. Addressing missing summary statistics, standardizing data formats, handling conversions, and ensuring data quality were integral to prepare data for synthesis. Imputation methods were applied to missing values, and sensitivity analyses were performed to assess their impact. The process incorporated subgroup analyses and sensitivity analyses to address heterogeneity and for providing meaningful and accurate synthesis. Visual display methods, including forest plots, tables, heat maps, bubble plots, funnel plots, risk of bias graphs, cumulative meta-analysis plots, network plots, Venn diagrams, summary figures, flow diagrams, and various charts and graph were used to effectively present results and analyses.The synthesis process followed a systematic approach involving the definition of criteria, screening based on titles and abstracts, full-text assessment, data extraction, tabulation,

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

and comparison. Transparent documentation and regular communication between reviewers ensured consensus in decision-making. Addressing missing summary statistics, standardizing data formats, handling conversions, and ensuring data quality were integral to preparing data for synthesis. Imputation methods were applied to handle missing values, and sensitivity analyses were performed to assess their impact. The process incorporated subgroup analyses and sensitivity analyses to address heterogeneity and provide meaningful and accurate synthesis. Visual display methods, including forest plots, tables, heat maps, bubble plots, funnel plots, risk of bias graphs, cumulative meta-analysis plots, network plots, Venn diagrams, summary figures, flow diagrams, and various charts and graphs, were used to effectively present results and analyses.

RESULT

The search strategy yielded a total of 283 records from primary databases, including ScienceDirect, google scholar and Scopus, adhering to the defined inclusion and exclusion criteria. After screening titles and abstracts, 17 studies were identified for full-text assessment. During this phase, 26 studies met the inclusion criteria and were included in the systematic review. The excluded studies, totaling 250, are detailed in the flow diagram along with reasons for exclusion, such as lack of explicit methodology details or non-English language.

The included studies encompass a range of applications related to keylogger detection and mitigation, including machine learning techniques, heuristic methods, and behavior-based strategies. Characteristics of each study, including participant characteristics, intervention details, study design, funding sources, ethical approval, publication characteristics, data availability, and conflicts of interest, are comprehensively presented.

Risk of bias in studies

The risk of bias in each included study was assessed using the Cochrane Risk of Bias tool. Domains such as randomization, blinding, and outcome reporting were considered. Multiple independent reviewers conducted the assessment, ensuring a thorough and transparent evaluation. Regular meetings facilitated quality control, addressing any challenges or discrepancies through consensus.

For each study, summary statistics for relevant groups and effect estimates with precision (e.g., confidence intervals) are provided. This information is presented using structured tables or plots, allowing for a clear understanding of the individual study contributions.

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

Table 3.2: Findings of Included Studies

S/N	Author(s) (Year)	Title	Summary
1	Sarita Yadav, Anuj Mahajan, Monika Prasad, Avinash Kumar (2020) [1]	Advanced Keylogger for Ethical Hacking	The paper talks about two real-world cases where keyloggers were utilized to take cash and monitor individuals, highlighting the requirement for superior discovery and moderation procedures. The creators were persuaded to investigate different methods for making an advanced keylogger and setting up a honeypot to log and analyze client exercises, with the objective of distinguishing and protecting against such threats. Solution Approach: The authors propose a comprehensive arrangement that incorporates a few key components: 1) client-server engineering for capturing and transmitting keystrokes, 2) to utilize of string-matching calculations to proficiently handle the logged information, 3) methods to guarantee the keylogger remains stealthy and imperceptible by antivirus program and the client, and 4) the execution of encryption and unscrambling instruments to secure the logged data. [1].
2	Donghai Tian, Xiaoqi Jia, Junhua Chen, Changzhen Hu (2016) [2]	An Online Approach for Kernel-level Keylogger Detection and Defense	The creators recognize that kernel-level keyloggers work at a higher benefit level and are troublesome to distinguish due to their little impression. Existing strategies that depend on imitating or require alterations to the OS part are restricted in their real-world applicability. Solution Approach: The creators propose LAKEED, a novel framework that leverages hardware-assisted virtualization innovation to distinguish and moderate kernel-level keyloggers. LAKEED confines the target bit expansion (which may contain the keylogger) from the console drivers, permitting the hypervisor to screen their intuitive and recognize any inconsistencies. The framework too gives a protective instrument to secure client input by capture attempt keystrokes some time recently they reach the OS. [2].

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

3	Prasiddha Bhat, Namratha H J, Mohana (2023) [3]	Cyber Security Testbed: Keyloggers and Data Visualization on Keyloggers - A Case Study	This paper presents a point by point consider on cybersecurity testbeds and their centrality in surveying vulnerabilities in a controlled environment. It also centers on keyloggers, a sort of vindictive device that records a user's keystrokes, and gives an amusement and examination of its working. In addition, the paper joins data visualization on two specific keylogger datasets to choose up a critical understanding of keylogger behavior and plans. The key points secured are the crucial highlights of a practical cybersecurity testbed, diversion of a keylogger program, and data visualization techniques to recognize designs and abnormalities in keylogging data. The objective is to make a compelling system for recognizing and directing keylogger attacks, which are essential in the current progressed scene. [3].
4	C. Santwana, K. Sai Aditya, Dr. S. Magesh (2014) [4]	Hypervisor based Mitigation Technique for Keylogger Spyware Attacks	The paper presents a novel approach to coordinate the danger of keyloggers, a sort of malware that takes sensitive data such as passwords and credit card numbers. The proposed course of activity utilizes a hypervisor-based planning, where a trusted virtual machine (VM) is utilized for secure puzzle word input, whereas the standard browsing works out are performed on a less trusted working VM. This way, the central information are limited from potential keylogger ambushes, giving a practical defense component against data theft. The makers as well see at the central centers and confinements of their approach, the capacity to dodge a wide run of data-stealing malware and facilitate phishing ambushes. This study emphasizes the prerequisite for a comprehensive course of action that addresses contrasting sorts of keyloggers, checking kernel-level and a screen/mouse-based groupings, and proposes future work to upgrade the security of the proposed framework.[4].
5	Pratik Hiralal Santoki (2014)	Design and Implementation of Detection of	This consider presents a moder strategy to recognize and distinguish diverse keyloggers softwares, a sort of malware that takes delicate

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

	[5]	KeyLogger	client data by logging keystrokes. The proposed arrangement utilized in this think about is called Key Catcher, it leverages an unprivileged approach that never require any extraordinary framework benefits. The key thought is to mimic client input by infusing carefully created keystroke groupings into the framework and observing the input/output behavior of the running forms. By analyzing the relationship between the infused input and the watched yield, the framework can identify the nearness of keyloggers that endeavor to log and exfiltrate the mimicked keystrokes. The developer thoroughly evaluates the suggested approach against a broad range of real-world keyloggers, demonstrating its suitability in identifying such threats without producing any false positives. The present study examines the possible mitigation techniques that keyloggers might employ and suggests a heuristic-based approach to dissect such advanced attacks. In general, the idea almost entirely offers a practical and workable plan of action for protecting users from the growing threat posed by keyloggers, which makes it a valuable contribution to the field of malware elimination and disclosure. [5].
6	Soham P. Chinchalkar, Rachna K. Somkunwar (2024) [6]	An Innovative Keylogger Detection System Using Machine Learning Algorithms and Dendritic Cell Algorithm	The paper presents a novel approach to viably distinguish computer program keyloggers, a sort of malware that postures a genuine risk to client protection and security by furtively recording console inputs. The proposed framework combines to utilize of machine learning calculations, specifically Back Vector Machine (SVM) and Gullible Bayes, along with the Dendritic Cell Calculation (DCA) from the field of Counterfeit Safe Systems. The key thought is to use the distinctive qualities of these methods to make a vigorous and precise keylogger discovery instrument. The SVM is to begin with utilized to classify the input speed, distinguishing any suspicious action that might demonstrate the nearness of a keylogger. The

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

			Credulous Bayes calculation is at that point utilized to analyze the time interims between the commands, recognizing between occasional and randomized designs, which are demonstrative of keylogger behavior. At last, the DCA is utilized to prepare the randomized commands and produce solid antigens and signals, assist improving the discovery precision, particularly for keyloggers that attempt to avoid location by utilizing non-periodic input patterns. The creators completely assess their proposed crossover approach, counting the SVM-DCA and SVM-NB-DCA setups, and illustrate noteworthy discovery exactnesses of up to 99.8% and 96%, separately. These comes about outflank existing procedures like the Dendritic Cell Calculation (DCA), Activity Examination for Keylogger Location (TAKD), and Keystroke Collecting Malware (KLIMAX). The paper's discoveries exhibit the viability of combining machine learning and Counterfeit Safe Framework calculations for the basic assignment of defending client information against the danger of modern keyloggers [6].
7	Pratik Hiralal Santoki (2014) [7]	Design and Implementation of Detection of KeyLogger	The paper proposes a new technique for detecting keyloggers, which are software programs that steal confidential information by monitoring keystrokes. The technique involves simulating crafted keystroke sequences to identify keyloggers, and can detect keyloggers that run in user space without requiring privileged access. The paper highlights the limitations of existing detection techniques, including signature-based and behavior-based approaches, and proposes a new approach that focuses on modeling keylogging behavior without making assumptions about the keylogger's internals or the underlying environment [7].
8	Yahye Abukar (2013) [8]	Mitigating of Malicious Insider Keylogger Threats	The article explicitly address the danger of insider attacks, emphasizing the use of keyloggers, which malevolent insiders with authorized access can introduce into a company's network. The authors highlight the challenges in recognizing insider threats since these people usually have knowledge of

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

			organizational structures and can utilize that knowledge to avoid detection. The article identifies five categories of insiders, ranging from low-level pristine insiders (application users) to external associates (contract employees, friends, or colleagues of representatives). The authors point out that insiders have the ability to seriously damage an organization through disruption, mental property theft, and damage to data and frameworks. The paper too examines the components that contribute to the insider risk, counting specialized, social, trade, financial, and social components. The creators highlight the significance of a all encompassing approach to moderating the insider risk, counting security arrangements, data security controls, staff preparing, and social awareness. The paper surveys a few insider discovery strategies, counting inactive and energetic location strategies, behavioral-based location, and pollute information examination systems. The creators note that each of these strategies has its confinements and that a combination of approaches is likely to be more compelling in identifying and relieving insider threats. [8].
9	Huseyn Huseynov, Kenichi Kourai, Tarek Saadawi and Obinna Igbe (2020) [9]	Virtual Machine Introspection for Anomaly-Based Keylogger Detection	This paper proposes a novel approach to identifying keyloggers in Linux-based virtual machines utilizing Manufactured Safe Framework (AIS) and Virtual Machine Contemplation (VMI). Keyloggers are a sort of malware that surreptitiously log console movement, and existing location strategies have restrictions. The method uses a distributed program that runs on a host computer and examines many virtual machines to identify anomalies. The framework consists of two main components: KVMonitor, a VMI device that logs events and gathers data, and an algorithmic program that runs on a hereditary basis and uses Negative Choice Calculation (NSA) to examine the data for any anomalies. The paper to begin with examines the Linux console driver structure and classification of

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

			keyloggers, counting kernel-based, user-space or API-based, shape snatching or formjacking, and JavaScript-based keyloggers. The proposed approach centers on recognizing user-space keyloggers running on Linux-based virtual machines. The AIS-based calculation is motivated by the human safe system's capacity to recognize inner cells and particles from maladies. The NSA is utilized to distinguish and classify suspicious forms, and the framework is outlined to anticipate user-space keyloggers from taking private data. The article highlights the significance of a proactive checking framework to keep the Linux framework secure, particularly with the expanding pitch of edge computing and IoT gadgets. The proposed approach offers a comprehensive assurance for different stages, opposite to existing signature-based risk location techniques [9].
10	Blåfield, Toni (2020) [10]	DIFFERENT TYPES OF KEYLOGGERS Mitigation and risk relevance in modern society	This study explores the threat of keyloggers in modern society, providing an in-depth explanation of different types of keyloggers, their functionality, targets, and use cases. The research aims to raise awareness of the keylogger threat and introduce mitigation methods for each type. The thesis concludes that while some types of keyloggers, like hardware keyloggers, are less of a threat due to device mobility and size, new mobile software keyloggers pose a significant risk as they can spread and collect keystroke data without visibility to the end user. The study provides a comprehensive analysis of keyloggers, their types, and mitigation strategies, highlighting the importance of staying vigilant in the face of evolving cybersecurity threats. It emphasizes the need for awareness and mitigation strategies to prevent keylogger attacks, particularly in the context of modern information security. [10].
11	Wood, C Management, R Raj	Keyloggers in Cybersecurity	This thesis explores the threat of keyloggers in modern society, providing an in-depth

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

	(2023) [11]	Education.	explanation of different types of keyloggers, their functionality, targets, and use cases. The research aims to raise awareness of the keylogger threat and introduce mitigation methods for each type. The thesis concludes that while some types of keyloggers, such as hardware keyloggers, are less of a threat due to device mobility and size, new mobile software keyloggers pose a significant risk as they can spread and collect keystroke data without visibility to the end user. The thesis provides a comprehensive analysis of keyloggers, their types, and mitigation strategies, highlighting the importance of staying vigilant in the face of evolving cybersecurity threats. It emphasizes the need for awareness and mitigation strategies to prevent keylogger attacks, particularly in the context of modern information security. The thesis ultimately concludes that keyloggers remain a relevant threat in modern society, and their evolution necessitates continued research and development of effective mitigation methods [11].
12	Sashank Narain, Amirali Sanatinia and Guevara Noubir (2014) [12]	Single-stroke Language-Agnostic Keylogging using Stereo-Microphones and Domain Specific Machine Learning	This paper investigates the risk of privacy breaches through keystroke inference on Android smartphones. The researchers developed algorithms to process sensor signals and machine learning models to infer key taps using stereo microphones and gyroscopes. They achieved an accuracy of 90-94% for small key sizes in a single attempt, exceeding previous studies. The study highlights the vulnerability of stereo microphones as a side channel and demonstrates how malicious applications can exploit this to log keystrokes. The paper also proposes techniques to mitigate these attacks, emphasizing the need for privacy protection on mobile devices. [12].
13	Privacy, JV Monaco (2018) [13]	SoK: Keylogging Side Channels	This paper discusses keylogging side channel attacks, which exploit information leaked through various sources, such as finger and hand movements, keyboard electromagnetic and acoustic emanations, and network traffic. The authors evaluate the performance of idealized

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

			spatial and temporal keylogging side channels and find that substantial information gains can be achieved even with measurement errors. They also analyze how typing speed and style affect the information gained from temporal side channels. The paper provides a comprehensive review of current keylogging side channel attacks and discusses mitigation techniques to drive future research in this area. [13].
14	Chow Wen Xuan1, Intan Farahama Binti Kamsin2, Salmiah Amin3 and Nur Khairunnisha Zainal [14]	Preventing Malicious Keyloggers using Anti-keyloggerIntegrated Keyboard in Mobile Banking Applications	This research paper proposes a new keyboard system to prevent malicious keylogging activities in mobile banking applications. Currently, users are required to login using their credentials, which can be vulnerable to cyber-attacks. Although Multi-Factor Authentication can strengthen the authentication process, there are still limitations. The proposed system aims to overcome this issue by providing a trusted and verified keyboard system that prevents users from being threatened by malicious keyloggers. The research uses a quantitative study via survey to gather information from 300 respondents who regularly use mobile banking applications in Malaysia. The study aims to address the limitations of the current keyboard system and propose a new system to fulfill the gap. Future researchers are recommended to develop a system that can identify the nature of a keylogger, to prevent the removal of keyloggers used for supervising [14].
15	John V. Monaco (2020) [15]	A Remote Keylogging Attack on Search Engine Autocomplete	This paper presents a farther keylogging assault on look motor autocomplete, called KREEP (Keystroke Acknowledgment and Entropy Disposal Program). The assault recognizes keystrokes in scrambled arrange activity and distinguishes look inquiries utilizing data from three free sources: keystroke timings, percent-encoding of Space characters in a URL, and the inactive Huffman code utilized in HTTP2 header compression. The assault is strong to parcel delay variety but not to cushioning, and a basic cushioning defense is proposed to relieve the assault. The paper illustrates the assault on two well known look motors and assesses its execution utilizing a collected dataset of 16k

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

			look inquiries, distinguishing 15% of questions and recouping up to 60% of the inquiry content among a list of 50 speculation queries. The attack comprises of five stages: keystroke location, tokenization, lexicon pruning, word recognizable proof, and bar look. Keystroke discovery isolates bundles that compare to keystrokes from foundation activity, and tokenization portrays words in the bundle grouping. Lexicon pruning employments an HTTP2 header compression side channel to kill words from a expansive word reference, and word recognizable proof is performed by a neural organize that predicts word probabilities from parcel inter-arrival times. The bar look creates speculation questions utilizing a dialect model. The paper contributes to the field of keylogging side channels and autocomplete security, highlighting the powerlessness of look questions to farther keylogging assaults and proposing countermeasures to relieve such attacks.This paper presents a farther keylogging assault on look motor autocomplete, called KREEP (Keystroke Acknowledgment and Entropy Disposal Program). The assault recognizes keystrokes in scrambled arrange activity and distinguishes look inquiries utilizing data from three free sources: keystroke timings, percent-encoding of Space characters in a URL, and the inactive Huffman code utilized in HTTP2 header compression. The assault is strong to parcel delay variety but not to cushioning, and a basic cushioning defense is proposed to relieve the assault. The paper illustrates the assault on two well known look motors and assesses its execution utilizing a collected dataset of 16k look inquiries, distinguishing 15% of questions and recouping up to 60% of the inquiry content among a list of 50 speculation queries. The attack comprises of five stages: keystroke location, tokenization, lexicon pruning, word recognizable proof, and bar look. Keystroke discovery isolates bundles that compare to keystrokes from foundation activity, and tokenization portrays words in the bundle grouping. Lexicon pruning employments an

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

			HTTP2 header compression side channel to kill words from a expansive word reference, and word recognizable proof is performed by a neural organize that predicts word probabilities from parcel inter-arrival times. The bar look creates speculation questions utilizing a dialect model. The paper contributes to the field of keylogging side channels and autocomplete security, highlighting the powerlessness of look questions to farther keylogging assaults and proposing countermeasures to relieve such attacks. This paper presents a farther keylogging assault on look motor autocomplete, called KREEP (Keystroke Acknowledgment and Entropy Disposal Program). The assault recognizes keystrokes in scrambled arrange activity and distinguishes look inquiries utilizing data from three free sources: keystroke timings, percent-encoding of Space characters in a URL, and the inactive Huffman code utilized in HTTP2 header compression. The assault is strong to parcel delay variety but not to cushioning, and a basic cushioning defense is proposed to relieve the assault. The paper illustrates the assault on two well known look motors and assesses its execution utilizing a collected dataset of 16k look inquiries, distinguishing 15% of questions and recouping up to 60% of the inquiry content among a list of 50 speculation queries. The assault consists of five stages: word recognizable evidence, lexicon trimming, bar glance, tokenization, and keystroke location. While keystroke identification separates bundles from foundation activity that mimics keystrokes, tokenization shows words within the bundle grouping. Word recognition is done with a neural network that predicts word probabilities based on parcel inter-arrival timings. To extract words from a huge word reference, the Lexicon pruning employs an HTTP2 header compression side channel. The bar look makes speculative inquiries by utilizing a dialect model. The study improves the domains of keylogging side channels and autocomplete security by

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

			highlighting look questions' incapacity to foil keylogging assaults and offering mitigation strategies. Keystroke Acknowledgment and Entropy Disposal Program, or KREEP, is a more sophisticated keylogging attack aimed against The assault recognizes keystrokes in scrambled arrange activity and distinguishes look inquiries utilizing data from three free sources: keystroke timings, percent-encoding of Space characters in a URL, and the inactive Huffman code utilized in HTTP2 header compression. The assault is strong to parcel delay variety but not to cushioning, and a basic cushioning defense is proposed to relieve the assault. The paper illustrates the assault on two well known look motors and assesses its execution utilizing a collected dataset of 16k look inquiries, distinguishing 15% of questions and recouping up to 60% of the inquiry content among a list of 50 speculation queries. Keystroke location, tokenization, lexicon trimming, word recognized evidence, and bar glance are the five phases of the attack. Tokenization represents words in the bundle grouping, whereas keystroke discovery separates bundles that correspond to keystrokes from foundation activity. The process of lexicon pruning uses an HTTP2 header compression side channel to exclude terms from a large word list. The neural network is utilized for word recognition, predicting word probabilities based on parcel inter-arrival durations. The bar glance uses a dialect model to generate conjecture questions. The study advances the fields of keylogging side channels and autocomplete security by emphasizing look questions' inability to thwart keylogging attacks and by suggesting defense strategies against them. [15].
16	Carter Slocum, Yicheng Zhang, Nael Abu-Ghazaleh, and Jiasi Chen, (2023)	Going through the motions: AR/VR keylogging from user head motions	In this study, researchers developed a system called TyPose, which extracts these motion signals and uses machine learning to infer the words or characters being typed. The system can determine word/character boundaries and

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

	[16]		perform inference on the words/characters themselves. Experimental evaluations on commercial AR/VR headsets demonstrated the feasibility of this attack, achieving 82% top-5 word classification accuracy when using data from multiple users for training and 92% accuracy when personalized to a particular victim. Moreover, the researchers found that first-line defenses such as reducing the sampling rate or precision of head tracking data are ineffective, indicating that more sophisticated mitigations are necessary to address this security risk. This highlights the need for AR/VR developers to prioritize security and implement robust measures to protect user privacy and prevent such attacks. [16].
17	Rutik Kapare, Aditya Gawade, Aditya Kamble, Pallavi Tembhurnikar (2024) [17]	Enhancing Digital Security With The Advanced Keylogger Project	The Advanced Keylogger Project is a comprehensive digital security solution that combines keystroke logging, clipboard monitoring, audio recording, and screenshot capture to provide unparalleled precision in capturing user activity. The project prioritizes data security through robust encryption algorithms and secure transmission protocols, ensuring sensitive information remains protected from cyber threats. This innovative solution transcends technological innovation, offering hope and reassurance to individuals and organizations in the face of digital uncertainties. The project's impact extends beyond academia, leaving a lasting legacy in the field of cybersecurity and inspiring future innovators to safeguard digital realms [17].
18	S.vinothkumar, S.Aruna sankaralingam (2014) [18]	Mobile Keylogger Detection By Using Machine Learning Technique	The paper discusses the threat of keyloggers, a type of malware that records every keystroke made on a device, allowing attackers to steal sensitive information. The primary objective of the project is to detect keylogger applications and prevent data loss and sensitive information leakage. The proposed solution is a machine learning-based keylogger detection system for mobile phones, which can detect malware

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

			applications by analyzing their behavior and permissions. The paper highlights the increasing use of smartphones and the corresponding increase in mobile malware, including keyloggers. It notes that traditional anti-virus software may not be effective in detecting malware, and that new approaches are needed to combat the threat. The paper also discusses the history of mobile malware, including the first mobile phone virus, which was discovered in 2004, and the subsequent rise of malware targeting Android devices. It highlights the risks of identity theft and other crimes associated with mobile malware, and the need for effective security measures to protect mobile devices and users. [18].
19	Prof. Priyanka Mane, Prabhakar Avhad, Devarsh Khedkar, Ravikant Jadhav, Abhijit Gogre (2017) [19]	Keylogging-Resistant Visual Authentication Protocols	The paper discusses the challenges of designing secure authentication protocols, particularly in the presence of rootkits and other malicious software on personal computers. It highlights the limitations of relying on users to enhance security, as this can compromise usability. Instead, the authors propose a visual authentication approach that combines security with usability. The paper presents two visual authentication protocols: a one-time-password protocol and a password-based authentication protocol. Through rigorous analysis, the authors demonstrate that these protocols are resistant to various authentication attacks. Additionally, they conduct a case study on a prototype of their protocols, showing that they can achieve high usability while meeting strict security requirements. The authors argue that careful visual design can improve both security and usability in authentication, and demonstrate the potential of their approach for real-world deployment. The paper contributes to the development of secure and user-friendly authentication methods, which is essential for protecting users' trust and security in online transactions. [19].

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

20	YAHYA ALHAJ MAZ1, MOHAMMED ANBAR, SELVAKUMAR MANICKAM1, SHAZA DAWOOD AHMEDRIHAN, BASIM AHMAD ALABSI, ANDOSAMAM.DORGHAM (2024) [20]	Majority Voting Ensemble Classifier for Detecting Keylogging Attack on Internet of Things	The paper discusses the threat of intrusion attacks on the Internet of Things (IoT), particularly keylogging attacks, which can compromise sensitive information such as login passwords, personal information, and financial information. To detect keylogging attacks in IoT networks, the authors propose an ensemble classifier model that combines three machine learning algorithms: Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), and Long-Short Memory Network (LSTM). The model is trained on the BoT-IoT dataset and achieves excellent accuracy, low false positive rate, and improved detection rates for keylogging attacks compared to individual classifiers. The ensemble model demonstrates a promising approach for detecting keylogging attacks in IoT networks, enhancing the security and integrity of IoT systems [20].
21	Junsung Cho, Geumhwan Cho and Hyoungshick Kim [21]	Keyboard or Keylogger?: a security analysis of third-party keyboards on Android	The paper discusses the security risks associated with third-party keyboard applications on Android devices. The authors demonstrate the potential for keylogging attacks by implementing a proof-of-concept keylogger application that can steal sensitive keystrokes from 81 popular websites. They also analyze the security behaviors of 139 keyboard applications available on Google Play and find that the majority of them could be potentially misused as malicious keyloggers. The paper highlights the limitations of Google's application review process in detecting and preventing such keylogger applications and suggests several practical recommendations to address the security problem [21].
22	John V. Monaco (2018) [22]	SoK: Keylogging Side Channels	The paper discusses the history and evolution of keylogging side channel attacks, which exploit information leaked through various channels, such as electromagnetic and acoustic emanations, finger and hand movements, and microarchitectural attacks on the host computer. These attacks can be categorized into spatial and temporal side channels, which reveal physical key locations or key press and release timings, respectively. The authors evaluate the performance of

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

			idealized spatial and temporal keylogging side channels and find that substantial information gains can be achieved even with significant measurement error. They also analyze the correlation between typing speed and style and the information gained from different temporal features. The paper concludes by reviewing the current state-of-the-art keylogging side channel attacks and discussing potential mitigation techniques to prevent these attacks. The goal is to drive future research in developing effective countermeasures against keylogging side channel attacks [22].
23	Anjaneyulu Daddala, Neha Bagga (2022) [23]	SAFEGUARD AGAINST ADVANCED KEYLOGGER USING MIMIKATZ	The article discusses the threat of advanced keyloggers to personal and business data and the importance of safeguarding against them. It highlights Mimikatz, a powerful credential theft tool, as a significant threat, but also notes that it can be used to prevent keyloggers from stealing passwords and other data. The article suggests several ways to use Mimikatz to safeguard against advanced keyloggers, including disabling Windows Credential Guard, using Mimikatz's built-in protection mechanism, and detecting and removing keyloggers. Additionally, the article recommends other security measures such as employee awareness, strong password policies, anti-malware solutions, and effective data backup and recovery procedures to minimize the risk of data theft. Overall, the article emphasizes the need for a combination of effective security measures and active monitoring to protect against advanced keyloggers and other digital threats. [23].
24	Aarushi Dwivedi, Krishna Chandra Tripathi, M.L. Sharma (2014) [24]	Advanced Keylogger- A Stealthy Malware for Computer Monitoring	The paper talks about the danger of keyloggers, a sort of malware that records keystrokes and other client exercises, and proposes an progressed program keylogger that joins different highlights whereas minimizing CPU utilization. The paper highlights the developing reliance on electronic gadgets and the web, and the comparing increment in security dangers, counting keyloggers. Keyloggers can be used for both legitimate and malicious objectives, and

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

			detection is difficult owing to their stealth mode execution. The suggested keylogger is written in Python and includes features like computer data collection, clipboard content, mouthpiece activation, Chrome information collection, and screen capture functionality. The paper compares the proposed keylogger with existing ones based on the number of highlights and CPU utilization, and concludes that it is more progressed and troublesome to identify. The paper moreover talks about preventive measures to obstruct keyloggers, such as utilizing firewalls, anti-malware, and routinely checking CPU and memory utilization. [24].
25	Ameer Hamza, Urooj Akram, Ali Samad, Saima Noreen Khosa, Rida Fatima and Muhammad Faheem Mushtaq (2020) [25]	Unmaned Aerial Vehicles Threats and Defence Solutions	The paper discusses the security vulnerabilities of Unmanned Aerial Vehicles (UAVs) and their autopilot systems, which are used in various critical applications. The UAV system consists of aerial vehicles, ground control stations, and communication channels, and is vulnerable to various cyber-attacks such as GPS spoofing, deauthentication, denial of services, injecting false information, damaging UAV sensors, and keyloggers. These attacks can compromise the security and safety of UAV operations. The paper reviews various defense mechanisms proposed to mitigate these security risks and emphasizes the need for effective countermeasures to ensure the secure operation of UAVs [25].
26	Saiganesan N, Dheenadhayalan A, Arulmani M, Suresh K (Guide) [26]	Anti-Hacking Mechanism for Keylogger using Blackbox Detection	The paper discusses keyloggers, which are hardware or software tools that record keystrokes on a keyboard. While keyloggers can be used for legitimate purposes like troubleshooting or monitoring network usage, they can also be used maliciously to steal sensitive information. Software keyloggers are particularly concerning due to their ease of implementation and distribution. The paper highlights the need for effective detection techniques to combat keyloggers, and presents

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

			experimental results showing that such techniques can be robust against false positives and false negatives [26]

Results of syntheses

The systematic review included 26 studies, revealing a range of keylogger detection and mitigation strategies. Machine learning algorithms, heuristic techniques, and behavior-based approaches demonstrated varied success in detecting keyloggers, often assessed using metrics like Classification Accuracy and Area Under the ROC Curve (AUC). Proactive and reactive measures, when combined, proved most effective in reducing keylogger threats.

The development of user-friendly interfaces enhanced user awareness and facilitated timely intervention. Subgroup and sensitivity analyses addressed heterogeneity, indicating that different methodologies and contexts influenced the effectiveness of the strategies.

While progress has been made, there is a need for more robust, long-term validation and comprehensive solutions. The synthesis findings covered the attributes and potential biases of the studies involved, providing summary estimates with precision and measures of statistical heterogeneity. These findings were statistically synthesized, with a clear description of the effect's direction, especially in group comparisons. Examinations of potential reasons for variation and sensitivity assessments were detailed to evaluate the strength of the combined findings.

Reporting biases

The review carefully considered potential reporting biases, including publication bias, selective reporting within studies, and language bias. Efforts were made to include a comprehensive range of studies from multiple databases and to assess the quality and completeness of reporting in each study. The inclusion of only peer-reviewed journal articles aimed to mitigate publication bias, while the focus on English-language studies was a practical constraint that may introduce language bias. The conversation seeks to provide perspectives that extend beyond specific techniques and research, in accordance with the evolving nature of both disciplines. The melding of xenograft models and machine learning has potential to enhance understanding and steer the development of new therapeutic treatments.

DISCUSSION

Interpretation in the Context of Other Evidence

The findings of this review align with previous research emphasizing the complexity and evolving nature of keylogger threats. Various detection and mitigation strategies, such as machine learning algorithms, heuristic methods, and behavior-based approaches, have shown promise in identifying and countering keyloggers. However, the effectiveness of these methods varies based on implementation specifics and the context in which they are applied. Compared

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

to earlier reviews, this study provides a more comprehensive synthesis of contemporary approaches, highlighting advancements and persistent challenges in the field.

Limitations of the Evidence

Several limitations were noted in the evidence base. Many studies lacked long-term validation of their proposed methods, focusing primarily on short-term efficacy. The variability in the design and implementation of detection algorithms across studies made direct comparisons challenging. Additionally, the exclusion of non-English studies may have resulted in the omission of relevant findings from non-English-speaking regions, potentially limiting the generalizability of the results.

Limitations of the Review Processes

The review process itself had limitations, including potential bias in the selection and assessment of studies. While efforts were made to ensure a comprehensive and unbiased selection, the reliance on predefined search terms and inclusion criteria may have inadvertently excluded relevant studies. Additionally, the review depended on the quality of reporting within the included studies, which varied significantly. The imputation methods used to handle missing data, while necessary, introduced another layer of uncertainty.

Implications for Practice, Policy, and Future Research

The findings underscore the need for continued innovation and refinement in keylogger detection and mitigation strategies. Practitioners should integrate multi-faceted approaches, combining machine learning, heuristic, and behavior-based methods, to enhance detection accuracy and robustness. Policymakers should support the development of standardized protocols for keylogger detection and encourage cross-sector collaboration to share best practices and emerging threats. Future research should focus on long-term efficacy studies, the development of user-friendly interfaces, and the exploration of novel detection techniques, including the integration of artificial intelligence and advanced analytics.

CONCLUSION

This systematic review highlights the ongoing challenges and advancements in the field of keylogger detection and mitigation. Despite significant progress, keyloggers remain a formidable threat due to their ability to evade standard detection methods and seamlessly integrate into compromised systems. The review identifies several promising strategies and underscores the importance of a comprehensive, multi-faceted approach to effectively counter keylogger threats. Continued research and innovation, supported by robust policies and cross-sector collaboration, are essential to developing more effective solutions to safeguard sensitive information from keylogger attacks.

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

REFERENCES

[1] C. Slocum, Y. Zhang, … N. A.-G.-32nd U. S., and undefined 2023, "Going through the motions:{AR/VR} keylogging from user head motions," *usenix.org*, Accessed: May 18, 2024. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/slocum

[2] J. M.-28th U. S. S. (USENIX Security and undefined 2019, "What are you searching for? a remote keylogging attack on search engine autocomplete," *usenix.org*, Accessed: May 18, 2024. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/monaco

[3] J. Cho, G. Cho, H. K. Privacy, S. and T. (PST), and undefined 2015, "Keyboard or keylogger?: a security analysis of third-party keyboards on android," *ieeexplore.ieee.org*, Accessed: May 18, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7232970/

[4] D. Nyang, A. Mohaisen, J. K.-I. T. on Mobile, and undefined 2014, "Keylogging-resistant visual authentication protocols," *ieeexplore.ieee.org*, Accessed: May 18, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6746187/

[5] C. Xuan, I. Kasmin, S. Amin, N. Z.-I. J. of Data, and undefined 2022, "Preventing Malicious Keyloggers using Anti-keylogger Integrated Keyboard in Mobile Banking Applications," *ijdsaa.com*, vol. 4, pp. 2563–4429, Accessed: May 18, 2024. [Online]. Available: http://ijdsaa.com/index.php/welcome/article/view/140

[6] J. M.-2018 I. S. on S. and Privacy and undefined 2018, "Sok: Keylogging side channels," *ieeexplore.ieee.org*, 2018, doi: 10.1109/SP.2018.00026.

[7] S. Narain, A. Sanatinia, … G. N. the 2014 A. conference on, and undefined 2014, "Single-stroke language-agnostic keylogging using stereo-microphones and domain specific machine learning," *dl.acm.org*, pp. 201–212, 2014, doi: 10.1145/2627393.2627417.

[8] Y. Maz, M. Anbar, S. Manickam, … S. R.-I., and undefined 2024, "Majority Voting Ensemble Classifier for Detecting Keylogging Attack on Internet of Things," *ieeexplore.ieee.org*, Accessed: May 18, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10419360/

[9] A. Hamza, U. Akram, A. Samad, … S. K.-2020 I. 23rd, and undefined 2020, "Unmaned aerial vehicles threats and defence solutions," *ieeexplore.ieee.org*, Accessed: May 18, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9318207/

[10] S. Niyonsaba, K. Konate, M. S.-I. J. of Computer, and undefined 2023, "A Survey on Cybersecurity in Unmanned Aerial Vehicles: Cyberattacks, Defense Techniques and Future Research Directions," *ijcna.org*, 2023, doi: 10.5281/zenodo.10403783.

[11] P. Bhat, H. N.-2023 I. C. on, and undefined 2023, "Cyber Security Testbed: Keyloggers and Data Visualization on Keyloggers-A Case Study," *ieeexplore.ieee.org*, doi: 10.1109/ICSCNA58489.2023.10370136.

[12] C. Santwana, K. Aditya, S. M.-I. J. of Computer, and undefined 2014, "Hypervisor based Mitigation Technique for Keylogger Spyware Attacks," *Citeseer*, Accessed: May 18, 2024. [Online]. Available: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=4c676cebeb22e1f24da8d2a7c3f40a2951aa9811

[13] D. Tian, X. Jia, J. Chen, C. H.-J. I. S. Eng., and undefined 2017, "An Online Approach for Kernel-level Keylogger Detection and Defense.," *priv.gg*, Accessed: May 18, 2024. [Online]. Available: https://priv.gg/e/151104-2.pdf

[14] S. Yadav, A. Mahajan, M. Prasad, A. K.-I. J. of, and undefined 2020, "Advanced keylogger for ethical hacking," *ijeast.com*, vol. 5, 2020, Accessed: May 18, 2024. [Online]. Available: https://ijeast.com/papers/634-638,Tesma501,IJEAST.pdf

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR

[15] P. M. Hiralal Santoki Scholar SPBPatel, "Design and Implementation of Detection of KeyLogger," 2014, Accessed: May 18, 2024. [Online]. Available: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=d81ad090c5ef414c4b8ce89d943a749a24942ac8

[16] S. Ortolani, C. Giuffrida, and B. Crispo, "Bait your hook: A novel detection technique for keyloggers," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6307 LNCS, pp. 198–217, 2010, doi: 10.1007/978-3-642-15512-3_11.

[17] H. Huseynov, K. Kourai, … T. S.-2020 I. 21st, and undefined 2020, "Virtual machine introspection for anomaly-based keylogger detection," *ieeexplore.ieee.org*, Accessed: May 18, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9098980/

[18] … S. C.-R. d'Intelligence and undefined 2024, "An Innovative Keylogger Detection System Using Machine Learning Algorithms and Dendritic Cell Algorithm.," *search.ebscohost.com*, Accessed: May 18, 2024. [Online]. Available: https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=0992499X&AN=176040546&h=LkBGT68UK4RWBkB4bJgipoPr4vVJBMxNs0UNbjClaCfVkt539zpI70jzsMQJlQPpIZOy5Ti9%2FFRGAwuB6IgQUw%3D%3D&crl=c

[19] A. Daddala, N. B.- Kilby, and undefined 2023, "Safeguard Against Advanced Keylogger Using Mimikatz," *papers.ssrn.com*, Accessed: May 18, 2024. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4486846

[20] C. M. R. R.-S. and Wood and undefined 2010, "Keyloggers in Cybersecurity Education.," *Citeseer*, Accessed: May 18, 2024. [Online]. Available: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=d1d4628a22e8d27c6cd202839d7bf0e3a7c7ea91

[21] S. Gunalakshmii, … P. E.-C. on C., and undefined 2014, "Mobile keylogger detection using machine learning technique," *ieeexplore.ieee.org*, Accessed: May 18, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7068167/

[22] N. Singh, A. Shukla, A. Nagar, K. A.-… on Energy, undefined Materials, and undefined 2023, "Keylogger Development: Technical Aspects, Ethical Considerations, and Mitigation Strategies," *ieeexplore.ieee.org*, Accessed: May 18, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10434134/

[23] A. Badiozaman, B. Ruhani, M. Fadli, and B. Zolkipli, "Keylogger: The Unsung Hacking Weapon," *majmuah.com*, vol. 6, no. 1, pp. 33–43, 2023, Accessed: May 18, 2024. [Online]. Available: http://majmuah.com/journal/index.php/bij/article/view/339

[24] D. Elelegwu, L. Chen, Y. Ji, J. K.-S. 2024, and undefined 2024, "A Novel Approach to Detecting and Mitigating Keyloggers," *ieeexplore.ieee.org*, Accessed: May 18, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10500122/

[25] T. Blåfield, "Different types of keyloggers: Mitigation and risk relevance in modern society," 2020, Accessed: May 18, 2024. [Online]. Available: https://trepo.tuni.fi/handle/10024/122479

[26] Y. Abukar, Y. Abukar Ahmed, and A. Abdirahman Abdullahi, "Mitigating of Malicious Insider Keylogger Threats," *researchgate.net*, 2013, Accessed: May 18, 2024. [Online]. Available: https://www.researchgate.net/profile/Yahye-Abukar/publication/301197154_Mitigating_of_Malicious_Insider_Keylogger_Threats/links/570b696e08aea660813881c4/Mitigating-of-Malicious-Insider-Keylogger-Threats.pdf

Article DOI: 10.52589/BJCNIT-JGXGNUTR
DOI URL: https://doi.org/10.52589/BJCNIT-JGXGNUTR