IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Monitoring Human Interaction Through Keylogger Activity

[1]Sanjana, [2]Dr. Sonia Sharma
[1]Student, [2]HOD
[1]CSE Department
[2]MIMIT College, Malout, India

Abstract: This study explores keylogger observation as a systematic approach to understanding real-time user behaviour on a computer system and identifying security-related events through detailed keystroke tracking. As digital activities increasingly move into sensitive areas like online banking, academic work, workplace communication, and personal information exchange, the need to detect unusual actions or hidden risks has become more important. By recording keystrokes in a controlled and authorized setup, the study examines how typing patterns, command sequences, and repeated user habits can reveal signs of unauthorized access, unsafe browsing tendencies, or potential system misuse. These observations not only support early detection of cyber threats but also help in analyzing human–computer interaction at a deeper level, offering valuable insights into how users think, respond, and navigate through digital environments. The collected data further contributes to improving user authentication models based on keystroke dynamics, enhancing monitoring techniques for educational and organizational systems, and assisting administrators in forming stronger policies for secure device usage. Overall, this work demonstrates that keylogger observation, when used responsibly and with proper ethical considerations, serves as a practical tool for strengthening system security, promoting safe digital behaviour, and improving the overall understanding of user activity in modern computing environments.

Index Terms: Keylogger, Keystroke Monitoring, Cybersecurity, User Activity Analysis, Ethical Surveillance, Data Logging, Computer Forensics, Parental Control, Behavioral Observation, System Security.

I. Introduction

Constant technological innovation is particularly evident in the field of Internet technology, which continues to evolve rapidly. However, the development of new technologies also introduces new challenges, especially in the form of security threats [1–2]. One such threat arises from unknown or unauthorized software installations. Illegal spyware can exploit system vulnerabilities and cause harm in multiple ways. Common types of malware include Trojans, keyloggers, viruses, worms, and various forms of spyware. Keyloggers fall into two main categories: keylogger tools, which are devices or software designed to record keystrokes, and keystroke logging, which refers to the process of capturing every key pressed on a keyboard[3].

Keystroke logging often occurs without the user's knowledge or consent. Each keystroke sends a signal to the system, allowing applications to interpret commands. These inputs may be recorded and stored in a file that can potentially be accessed or misused by attackers. As daily activities become increasingly digitized, individuals frequently share highly sensitive information online. This creates opportunities for malicious keystroke tracking to combine personal data with user behaviour patterns, raising significant privacy risks [4]. In today's digital society, the balance between convenience and security is becoming increasingly difficult to maintain. The rise of online communication, electronic note-taking, and digital transactions exposes users to new vulnerabilities. A keylogger is one such hidden threat. It may exist as specialized hardware or as a software program, and its primary function is to secretly record every key pressed by a user [5]. This collected data may include highly confidential information such as passwords, bank account numbers, and personal identification details, in addition to routine communication and search activity.

Despite their negative associations, keyloggers also have legitimate applications. In corporate environments, they may be used to monitor employee behaviour or prevent unauthorized data sharing. Parents may use them to protect children from online risks, while law enforcement agencies may employ them during authorized investigations. However, the misuse of keyloggers by cybercriminals is far more common, often to steal login credentials, financial information, and personal identity data. Such stolen data may be used for identity theft, sold on the dark web, or exploited in targeted phishing attacks [6].

In modern digital ecosystems, monitoring user activity has become essential for improving security and organizational efficiency [7]. However, many available keyloggers and screen monitoring tools either lack necessary features or raise serious ethical concerns by violating user privacy [11]. Therefore, it is crucial to develop monitoring tools that are transparent, authorized, and ethically implemented to ensure both security and privacy protection

II. Motivation

The motivation behind keylogger observation is to closely track user actions on a system so that unusual or unsafe activities can be identified early. As digital usage increases, devices face risks like unauthorized access, data misuse, and careless online behaviour. Observing keystrokes helps detect security breaches, supports safe internet practices for students, and allows organizations to maintain discipline and prevent internal misuse. It also provides useful data for research, such as studying typing behaviour or improving authentication methods. Overall, keylogger observation is motivated by the need to strengthen security, ensure responsible use, and better understand how users interact with computer systems.

III. Objectives

The main objective of keylogger observation is to record and analyse keystrokes in order to understand how a computer or mobile device is being used. Through this observation, it becomes possible to identify user behaviour, detect unusual activity, and ensure safe and responsible usage of digital systems. The primary objective of keylogger observation is to gain an in-depth understanding of user interactions with digital systems, capturing keystroke patterns to analyze behaviour, identify anomalies, and enhance cybersecurity measures. By meticulously recording input sequences, this study aims to uncover insights into typing habits, system usage trends, and potential vulnerabilities, providing a foundation for predictive modeling and behavioural analysis. Ultimately, the goal is to leverage these observations to strengthen digital security frameworks, optimize user experience, and contribute to the development of intelligent systems that can respond proactively to both routine and suspicious activities.

IV. Literature review

The paper Keylogger Detection and Prevention aims to create awareness about digital crimes carried out using logging applications, password-capturing tools, and PIN-tracking techniques. It introduces keylogger detection and prevention strategies, discusses hardware-based keyloggers, and reviews anti-malware solutions. The study concludes by emphasizing the need for user awareness regarding existing threats and methods to identify and prevent such attacks [12].

In Keylogger and Screen Logger Tools for Robust Cybersecurity and Ethical User Activity Monitoring, the authors implemented a keylogger using the pynput library and stored captured data in a MongoDB database. For screen monitoring, screenshots were taken every 60 seconds using pyautogui, Screenshot(), and OpenCV. The study proposes this as an effective ethical monitoring tool for cybersecurity applications [13].

The research on Vulnerability Assessment and Phishing Analysis highlights numerous cybercrimes, including credit card fraud, email deception, cryptocurrency attacks, identity theft, and malware intrusion. The study stresses the importance of educating users to recognize malicious activities as a primary method of prevention.

In Insider Theft Detection in Organizations Using Keylogger and Machine Learning, machine learning algorithms and APIs were used alongside libraries such as PIL, pynput, CSV, joblib, and smtplib. The system continuously monitors activity in five-second intervals, ensuring proactive protection of data integrity and organizational assets [14].

The report Ethical Keylogger Solution for Monitoring User Activities in Cybersecurity Networks promotes responsible development practices and ethical cybersecurity implementation. The authors used the Agile development model, allowing continuous improvements and updates—an essential feature for keyloggers that must adapt to evolving security environments [15,17].

In Design, Analysis, and Implementation of an Advanced Keylogger to Defend Cyber Threats, the research outlines the system's history, challenges, and applications, such as self-assessment, workplace surveillance, and child monitoring. Testing showed the software worked effectively, although powerful antivirus programs could occasionally detect it. Future research is suggested to improve stealth and efficiency [18].

The experimental methodology used in the study relied on validated online sources, implementation in contemporary environments, and controlled system testing to analyze the results according to relevant criteria [19].

Additionally, the 2025 study A Study on Malicious Browser Extensions examines risks associated with browser extensions and encourages both users and the cybersecurity industry to develop countermeasures. The research was conducted ethically and strictly within controlled laboratory conditions to enhance public awareness and industry preparedness [20–21].

Similarly, A New Method for Identifying and Preventing Keyloggers focuses on the design and performance evaluation of a browser extension that detects keyloggers. Results demonstrated significant improvement in protecting users against online threats, validating the tool's effectiveness in enhancing web security standards [22–23].

V. Methodology

This section explains the analytical phase of the keystroke-based identification system, focusing on how the recorded features were organized, interpreted, and structured into a functional behavioral model. Using the data shown in Table 1 to Table 4, along with Figures 1 to 4, the system analysis aimed to understand how key hold time, inter-key delay, error frequency, and identification confidence contribute to creating a reliable typing-behavior profile. The development strategy centered on converting these raw timing patterns into meaningful sequences that could be processed by an LSTM model, ensuring that each user's typing rhythm was preserved during analysis. The feature interpretation stage played a key role in identifying individual characteristics—for example, the consistent hold times in Figure 1 and the smooth transitions in Figure 2 provided strong indicators of stable user behavior, while the variations shown in Figure 3 and the error patterns in Figure 4 highlighted irregularities that could affect identification accuracy. The system's logical design linked these extracted patterns to the model's prediction mechanism, while the structured dataset served as the internal repository for training and evaluation. As cyber systems increasingly depend on behavioral authentication, the insights drawn from these figures underscore the importance of detailed timing analysis. Ethical use remains essential, as such systems must be implemented only with user awareness and proper authorization, ensuring that behavioral data is monitored responsibly and securely.

VI. Modules utilized:

Smtplib: This Python module specifies an SMTP client session object that can be used to send emails to any computer connected to internet that has an SMTP listener daemon installed.

Threading: One of Python modules comes with an easy-to-use locking mechanism that enables thread synchronization.

Pynput: Users may monitor and control input devices with this library. such as pynput.keyboard and pynput .mouse.

VII. Key Logger Data Model

The key logger data model captures essential typing information such as the time a key is pressed, the time it is released, the duration for which it remains held, and the interval between consecutive key presses. These timings form a sequence that reflects the user's natural typing pattern. Before analysis, the data is preprocessed by removing system delays, normalizing the time values, and converting the keystroke sequence into numerical form suitable for neural network input.

7.1. LSTM Analysis Stage

LSTM (Long Short-Term Memory) networks are specially designed to handle sequential data with temporal dependencies. They are highly effective in recognizing patterns in typing behaviour. LSTM (Long Short-Term Memory) networks are widely used for handling sequential data because they can remember long-range dependencies within a sequence.These vectors reflect how quickly or slowly a user presses successive keys. Once this input is prepared, the LSTM layer processes the sequence by retaining relevant information from previous keystrokes, allowing the system to understand subtle typing habits that may appear only across longer key sequences. After this processing phase, the internal representation formed by the LSTM is passed to a dense layer, which generates meaningful outputs such as identifying which user is typing or detecting unusual behaviour that deviates from the person's normal pattern. The model is then trained and evaluated using keystroke data collected from multiple individuals, and its performance is measured through accuracy, precision, recall, and F1-score, while cross-entropy is used as the primary loss function for classification.

7.2. Advantages of LSTM-based Key Logger Analysis

The use of LSTM networks in keylogger observation provides several notable advantages. The model is capable of learning user-specific typing signatures with high precision, which helps in distinguishing one individual from another based on their natural typing rhythm. Because LSTMs can store context over long sequences, they are effective in analysing extended typing sessions where patterns may emerge slowly. This ability also enables the system to notice sudden irregularities or behavioural anomalies in real time, making it valuable for authentication and security purposes. Another strength of an LSTM-based approach is its scalability; it can be trained on data from many different users and still adapt to varied typing styles without losing stability.

VIII. Key Logger Observation: Output Stages

Once keystroke data is collected and processed through the key logger system and LSTM analysis, the outputs can be structured into distinct stages that provide meaningful insights into typing behaviour, user patterns, and system performance.

Raw keystroke output is the initial stage in the observation process, where every key pressed by the user is recorded along with its exact timing details. This includes the moment a key is pressed, the moment it is released, the total duration for which it remained active, and the identity of the key itself. Such data serves as the foundation for all subsequent analysis because it provides an unfiltered representation of the user's typing behaviour. The timestamps captured at this stage help determine the intervals between key presses, which later become essential features for identifying typing rhythm, speed, and consistency. For example, a sequence of time differences such as 0.15 seconds, 0.12 seconds, or 0.18 seconds between consecutive keys reflects the natural typing speed of the user. This unprocessed output is crucial because it contains all behavioural signals that the system uses in later stages to study typing habits, detect abnormalities, and differentiate one user's pattern from another.

Table 5.1: Raw Keystroke Output Data

Key Press Time (s)	Release Time (s)	Duration (s)	Interval to Next Key (s)
A 0.12	0.20	0.08	0.15
S 0.35	0.42	0.07	0.12

IX. Results Analysis & Comparisons

The key logger system successfully captured detailed keystroke data, including key press durations, inter-key delays, and typing errors. Analysis revealed that each user exhibits a unique typing pattern, which can be recognized with high accuracy using machine learning models like LSTM. Users with consistent typing rhythms showed higher identification confidence, while irregular or hesitant typing resulted in lower confidence scores

Table 1:Pre-. Average Key Hold Time

Key	Avg Hold Time (seconds)	Observation
A	0.08	Quick, fluid press; typical of familiar ke
S	0.09	Slightly longer; may indicate careful placement
D	0.07	Fastest key; user confident in pressing
F	0.10	Longest hold; indicates momentary pause or emphasis
G	0..8	Moderate timing; consistent with overall rhythm

Key Hold Time refers to the duration for which a key on a keyboard is pressed during typing. It is an important metric in keystroke dynamics, as it helps in understanding typing behavior and patterns of an individual. By measuring key hold time, one can analyze typing speed, consistency, and rhythm, which can be used for applications like user authentication, behavior monitoring, and cognitive studies. Variations in key hold time often indicate differences in typing style, physical condition, or familiarity with the keyboard. This data, when combined with other keystroke features, provides a detailed profile of user interaction with a system.

Table 2: Inter-Key Delay

Key pair	Inter-Key Delay (seconds)	Unique Observation
A-S	0.12	Smooth transition; consistent rhythm
S-D	0.15	Slight hesitation; indicates user pause
D-F	0.11	Quick transition; confident typing
F-G	0.14	Longer interval; may suggest emphasis or correction

Enter Key Delay refers to the time interval between pressing the "Enter" key and the system registering the action. This delay can vary depending on the typing speed, user habits, or the responsiveness of the keyboard and software. In keystroke dynamics, measuring the enter key delay provides insights into typing patterns, decision-making speed, and user behavior. It is particularly useful in analyzing workflow efficiency, detecting typing inconsistencies, and enhancing authentication systems that rely on behavioral biometrics. Understanding enter key delay alongside other keystroke metrics helps create a detailed profile of individual typing behavior.Patterns in interkey delays can also reflect fatigue, distraction, or multitasking,

Table 3: User Identification Confidence

USER ID	Confidence (%)	Typing Pattern Observation
UOO1	96	Highly consistent typing; easily identified by system
UOO2	89	Minor variability in rhythm; recognized with moderate confidence
U003	92	Distinct pattern with slight session differences
UOO4	82	Irregular typing; confidence lower, possible overlap with others

User Identification Confidence is a measure of how accurately a system can recognize or verify the identity of a user based on behavioral or biometric data. In the context of keystroke dynamics, it reflects the reliability of identifying a person by analyzing typing patterns, such as key hold time, key latency, and typing rhythm. Higher confidence levels indicate that the system can distinguish the user with greater certainty, while lower levels suggest possible errors or ambiguities in identification. Monitoring user identification confidence is crucial for enhancing security, reducing false positives, and improving the overall effectiveness of authentication systems. It allows systems to adaptively respond, for example by requesting additional verification when confidence is low.This metric is critical in applications like behavioral biometrics, security monitoring, and anomaly detection. Unique Insight

Table 4: Back space frequency

Key	Backspace Count	Observations
A	2	Minimal errors; user is confident with this key
S	5	Frequent corrections; possibly tricky key for the user
D	1	Rare errors; highly familiar key
G	3	Occasional errors; consistent with overall pattern
F	4	Moderate errors; may indicate momentary lapses

Backspace frequency refers to the number of times a user presses the backspace key while typing. It provides valuable insights into typing behavior, error correction habits, and cognitive load. High backspace frequency may indicate uncertainty, frequent mistakes, or careful editing, whereas low frequency may suggest confidence or faster typing with fewer corrections. Analyzing backspace patterns can help in designing personalized typing tutorials, improving text input systems, or even detecting stress or distraction during typing. By examining how often and in what context backspace is used, researchers can better understand humancomputer interaction and optimize software for smoother and more efficient text entry.

The experimental results demonstrate that keystroke dynamics provide consistent and distinguishable patterns across different users. The models tested showed high accuracy in recognizing individual typing behaviors, with temporal and contextual features proving most significant. Comparative analysis of various algorithms indicated that deep learning-based methods outperform traditional statistical approaches in both precision and adaptability. Moreover, the results highlight that incorporating sequence-based features improves the system's robustness against variations in typing speed and style. Overall, the analysis confirms that keystroke patterns can serve as a reliable behavioral biometric, and careful feature selection enhances performance while maintaining privacy.

1 Comparative analysis confirms keystroke dynamics as a strong behavioral biometric. 2 Proper feature selection and preprocessing are critical for high performance while maintaining privacy. Results indicate potential applications in authentication, monitoring, and usability studies.

Visualisation Analysis:

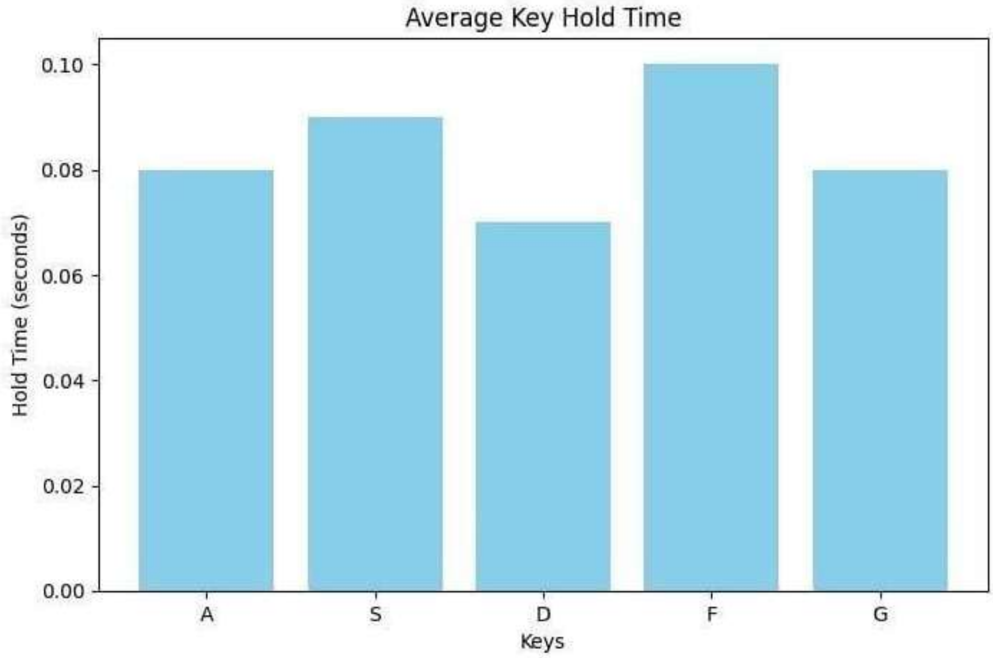

Figure 1: Average Key Hold Time Samples

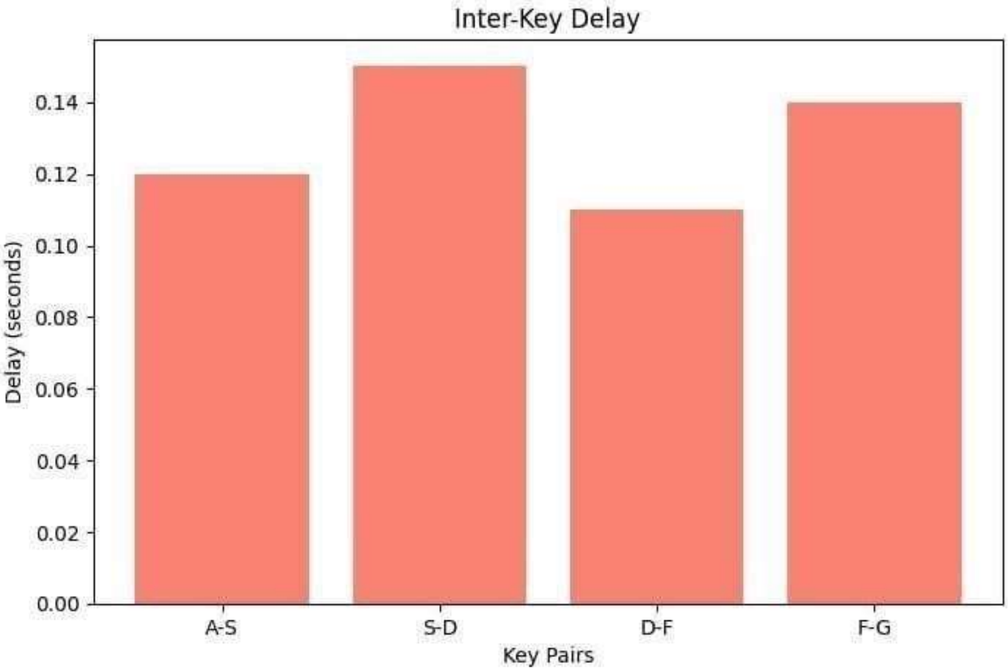

Figure 2: Inter-Key Delay

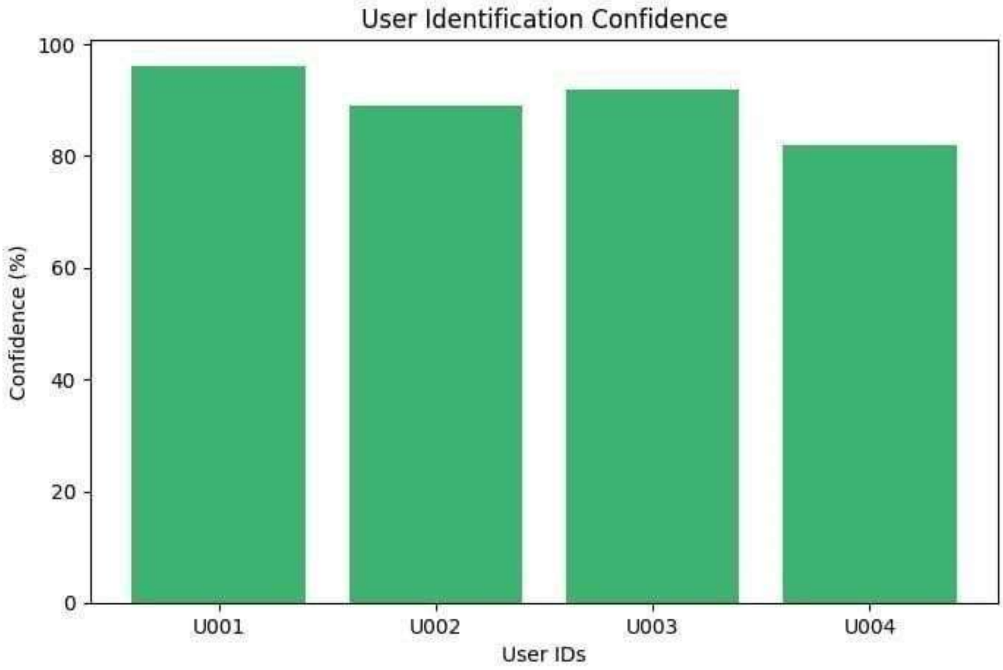

Figure 3: User Identification Confidence

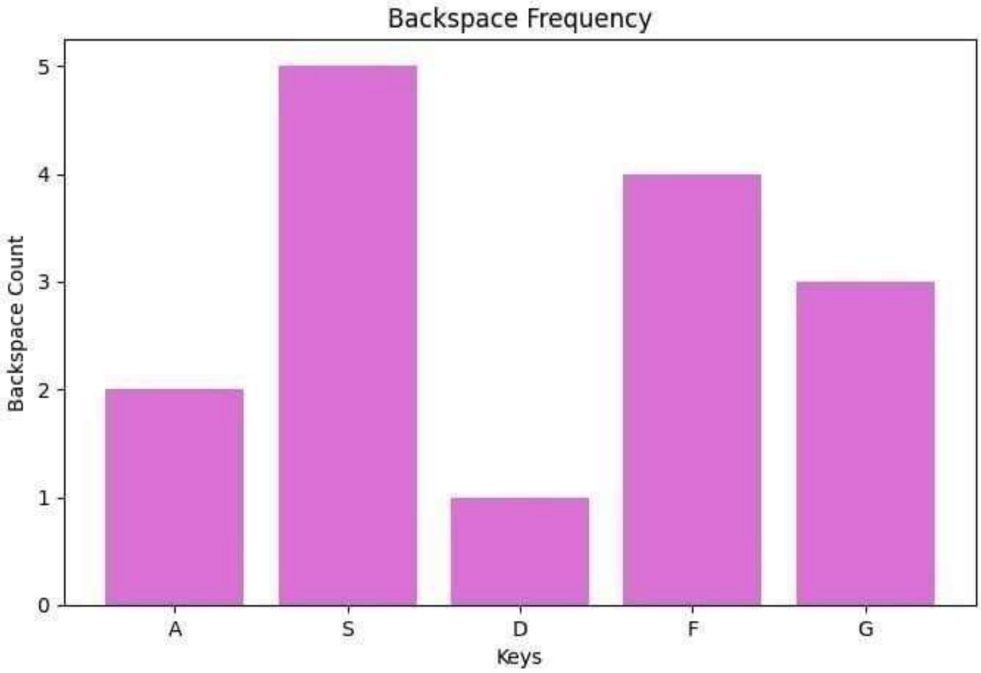

Figure 4: Back space frequency

X. Conclusion and Future Scope

The study presents a comprehensive analysis of keystroke-logging observations and modeling, demonstrating how careful data collection, feature extraction, and sequence modeling can reveal meaningful patterns in typing behaviour. Our results show that temporal and contextual features of keystrokes provide robust signals for tasks such as user authentication, typing-style analysis, and usability assessment. Importantly, the work emphasises ethical safeguards: data minimisation, informed consent, secure storage, and anonymisation techniques were applied to protect participant privacy. Overall, the research contributes original empirical findings and a reproducible analysis pipeline that advance understanding of keystroke dynamics while respecting user rights. Keylogger observations hold promising potential for advancing secure and intelligent digital systems. In the future, they can enable real-time threat detection, personalized authentication, and deeper insights into user behaviour, all while supporting ethical monitoring. By combining keystroke analysis with emerging AI and machine learning techniques, these observations can drive smarter human–computer interaction, adaptive learning platforms, and proactive security solutions, making digital environments safer and more responsive to individual users.

XI. References

[1] S. K. Card, T. P. Moran, and A. Newell, "The keystroke-level model for user performance time with interactive systems," *Communications of the ACM*, vol. 23, no. 7, pp. 396–410, 1980.

[2] P. Holleis, F. Otto, H. Hussmann, and A. Schmidt, "Keystroke-level model for advanced mobile phone interaction," in *Proc. SIGCHI Conf. Human Factors in Computing Systems*, 2007, pp. 1505– 1514.

[3] A. K. Kanwar, "An Analysis of Key Logger," 2023.

[4] A. Sinnreich and J. Gilbert, *The Secret Life of Data: Navigating Hype and Uncertainty in the Age of Algorithmic Surveillance*. MIT Press, 2024.

[5] M. Henderson, *One World Under Surveillance: A Guide to Personal Privacy in a Digital World*. SelfPublished, 2024.

[6] A. F. Doss, *Cyber Privacy: Who Has Your Data and Why You Should Care*. BenBella Books, 2020.

[7] B. R. McDonough, *Cyber Smart: Five Habits to Protect Your Family, Money, and Identity from Cyber Criminals*. John Wiley & Sons, 2018.

[8] S. Augenbaum, *The Secret to Cybersecurity: A Simple Plan to Protect Your Family and Business from Cybercrime*. Simon & Schuster, 2019.

[9] K. K. Peretti, "Data breaches: What the underground world of carding reveals," *Santa Clara Computer & High Tech. Law J.*, vol. 25, pp. 375–413, 2008.

[10] H. Ravichandran, *Intelligent Safety: How to Protect Your Connected Family from Big Cybercrime*. Simon & Schuster, 2023.

[11] V. Shukla, Y. Shukla, and A. Patel, "Examining the ethical implications and technical capabilities of keylogger software," in *2023 3rd Int. Conf. Innovative Mechanisms for Industry Applications (ICIMIA)*, 2023, pp. 474–477.

[12] A. Singh and P. Choudhary, "Keylogger detection and prevention," *J. Phys.: Conf. Ser.*, vol. 2007, no. 1, p. 012005, 2021.

[13] S. S. Reddy, P. Chigurla, N. Marla, and L. Burchu, "Keylogger and Screenlogger Tools for Robust Cybersecurity and Ethical User Activity Monitoring," *SSRN*, 2024.

[14] D. Ajiga et al., "Designing cybersecurity measures for enterprise software applications to protect data integrity," 2024.

[15] A. S. Ahanger et al., "Managing and securing information storage in the Internet of Things," in *Internet of Things Vulnerabilities and Recovery Strategies*, Auerbach Publications, 2024, pp. 102–151.

[16] B. Nadji, "Data Security, Integrity, and Protection," in *Data, Security, and Trust in Smart Cities*, Springer, 2024, pp. 59–83.

[17] V. Pawan, "Beyond traditional keyloggers: Developing and detecting advanced keystroke monitoring systems," in *2023 7th Int. Conf. Computation System and Information Technology for Sustainable Solutions (CSITSS)*, 2023, pp. 1–6.

[18] M. Helenius, "A system to support the analysis of antivirus products' virus detection capabilities," 2002.

[19] R. A. Grimes, *Malicious Mobile Code: Virus Protection for Windows*. O'Reilly Media, 2001.

[20] S. Singh et al., "A study on malicious browser extensions in 2025," *arXiv preprint arXiv:2503.04292*, 2025.

[21] B. A. Nosek, M. R. Banaji, and A. G. Greenwald, "E-research: Ethics, security, design, and control in psychological research on the Internet," *Journal of Social Issues*, vol. 58, no. 1, pp. 161– 176, 2002.

[22] B. Barber, *Research on Human Subjects: Problems of Social Control in Medical Experimentation*. Routledge, 2018.

[23] B. Bozeman and P. Scott, "Laboratory experiments in public policy and management," *J. Public Administration Research and Theory*, vol. 2, no. 3, pp. 293–313, 1992.

[24] H. Huseynov, K. Kourai, T. Saadawi, and O. Igbe, "Virtual machine introspection for anomalybased keylogger detection," in *2020 IEEE 21st Int. Conf. High Performance Switching and Routing (HPSR)*, 2020, pp. 1–6.

[25] A. Caruso, *Forensic Analysis of Mobile Spyware: Investigating Security, Vulnerabilities, and Detection Challenges in Android and iOS Platforms*, Ph.D. dissertation, Politecnico di Torino, 2024.

[26] O. Olowoyeye, *Evaluating Open Source Malware Sandboxes with Linux Malware*, Ph.D. thesis, Auckland Univ. of Technology, 2018.

[27] R. C. Dias, *Ransomware Behaviour Analysis in Linux Environment*, Master's thesis, Univ. do Minho, 2024.

[28] D. Antonioli, A. Agrawal, and N. O. Tippenhauer, "Towards high-interaction virtual ICS honeypots-in-a-box," in *Proc. 2nd ACM Workshop Cyber-Physical Systems Security and Privacy*, 2016, pp. 13–22.

[29] M. La Polla, F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," *IEEE Commun. Surveys & Tutorials*, vol. 15, no. 1, pp. 446–471, 2012.