© 2026 ADYPJIET, Volume 1(1), Online ISSN: 3049-1517, June 2026, pp. 1-13

Ajeenkya DY Patil Journal of Innovation in Engineering & Technology

Journal Homepage: https://www.adypsoe.in/adypjiet

Design of an Intelligent Defense Mechanism Against Keyloggers

[1]Anusha Rolla,
[2]Anamika Jain,
[3]Ujvala Patil

[1] UG student, Ajeenkya D Y Patil School of Engineering, Pune, INDIA
[2]Assistant Professor, Ajeenkya D Y Patil School of Engineering, Pune, INDIA
[3] Assistant Professor, Artificial Intelligence, GH Raisoni, COE & Management

Article History:
Received: 30/03/2026
Revised: 06/05/2026
Accepted: 23/06/2026

Abstract:
Computer security is becoming increasingly relevant due to the fact that personal or organizational computers might face threats of being accessed by unknown persons. Passwords alone cannot help anymore as they can be easily guessed, stolen, or shared between people. Therefore, there is a need to develop a security system based on keyloggers and having additional protection mechanisms. This system will include such characteristics as automatic shutdown in case of multiple wrong password entries, sending of the notification about the fact that someone has entered a wrong password to the owner of the device, and shuffling security questions for verifying the person's identity in case of suspected access. In case of failing to answer the questions correctly, the device will shut down. This paper gives a brief review of the suggested system, its benefits due to the usage of multiple security layers, and possible applications.

Keywords: Keylogger, Security, Unauthorized Access Detection, Auto Shutdown.

1.0 Introduction

In the modern world, when all work is dependent upon the use of computers, there is a real need for protecting the data of users. Keyloggers have emerged as a common threat within this sector. They are software programs that record all keystrokes made on a computer. Though normally

considered a harmful tool, it may be used for some beneficial purposes as well, including system monitoring and enhancing the security of a local area network [1]. When employed wisely, such systems can track login attempts, identify any attempts at intrusion and send out alerts to prevent any misuse of the network. According to research done by Malla et al. [1] discusses the risks of using a keylogger designed with malice in mind, which could silently log confidential login credentials and personal finance information without user consent. Anti-keylogger software was invented to detect and prevent unauthorized usage of keylogging before exposing any data. In another study, Gopan and Murali [2] recommended combining keystrokes with conventional keyloggers through typing speed and timing as additional biometrics for user identification purposes. Samuel et al. [3] discussed the designs of defensive keyloggers and focused on real-time detection and auto-protection as possible solutions to lower cybersecurity threats. There are many other solutions like graphical authentication and dynamic password management [4]. Ambekar et al. [5] presented the development of a keylogger in Python for Windows operating system. Behavioral biometrics like typing and mouse movements have been proven recently [9], [10], [13] to be highly useful to authenticate users, identifying them from intruders based on the usage of correct password. The proposed system "Keylogger with Intelligent Defence" improves the prior research by incorporating keylogging and real-time protection features Alert is instantly generated if the number of incorrect logins reaches one, automatic shutdown happens once there are three consecutive incorrect logins, and randomly generated security questions appear each time an unknown user attempts to enter by using the right password. The described approach ensures that the attacker will be challenged by the additional security mechanisms even in case one mechanism fails to stop them. In contrast to traditional keyloggers, which can be considered monitoring tools, the proposed keylogger combines these features and becomes a defense system which can be employed in personal computers, academic institutions, and corporate environment. Due to its monitoring and verification functions, the developed tool transforms the threat into an asset.

2.0 Literature review

In this regard, there are many difficulties that can be observed in detection and handling keyloggers in cybersecurity as they function stealthily and capture keystrokes without letting the user know. In conventional security tools, anti-virus software, and signature-based detection systems are quite useful for detecting these keyloggers as they work efficiently to detect known variants of the program; however, in case of customized or newly developed keyloggers, there can be some difficulties [1]. In this case, these keylogger programs remain hidden as they appear as genuine application programs and therefore static analysis techniques cannot detect them due to their dynamic behavior. Thus, there is an approach proposed by researchers in which behavior-based detection methods are employed to monitor the activities of the system for odd behavior. Here host-based intrusion detection systems and anomaly detection system tools are used to detect any unusual behavior of the system in terms of accessing files, monitoring inputs, and network behavior [4]. However, even after that, there may be difficulties as these tools have problems in differentiating legitimate applications from keyloggers having similar privileges [5].

Current research on this topic has been done using the combination of the biometric and the machine learning techniques. Gopan and Murali [2] provided a technique that uses the concept of

the keystroke dynamics which analyzes an individual's keystroke timings to ensure his identity is verified and any interruption can be detected regardless of password guessing. In a similar way, Samuel et al. [3] have developed a defensive keylogger system that uses an automatic shut down and alert system to create a robust defense against the unauthorized users. Ambekar et al. [5] has demonstrated that Python-based systems can help in creating lightweight but efficient systems for system monitoring especially when used along with security layers.

Moreover, there have been several studies on enhancing the authentication techniques. Saima et al. [4] used dynamic graphical password schemes, while Ahmed & Raju [7] developed multi-layered security questions to introduce randomness and uncertainty in authentication process. The practical study in biometrics conducted by Zhao et al. [13] and Banerjee and Woodard [10] shows the increased usage of keystroke dynamics along with AI-based analysis of specific traits for the distinction between legitimate and fake users. But even after all these developments, there are still some issues left unresolved. Anti-keylogger systems react to the suspicious behavior only after its detection, but not preventively. For this reason, they often confuse regular user's actions with possible threats and provide false positive alerts [8][11]. Machine learning techniques require a great volume of labeled data to be trained properly. However, such datasets are seldom available in the case of detecting keyloggers [12]. An additional problem that appears in practice concerns insiders - individuals who have already gained access to the system and installed the keylogger. These threats are hardly identifiable by traditional security solutions. The Intelligent Defence-based keylogger overcomes these hurdles using a hybrid approach that incorporates continuous monitoring, random security checks, and automatic protective mechanisms. The system not only records the keystrokes for security reasons but also restricts access to the system from an unauthorized user by means of various protective measures like alerts, random security questions, and automatic shutdown of the system if the attempts exceed a certain number.

3.0 Challenges and Limitations

1. On occasion legitimate software is flagged incorrectly as a threat thus causing a false alarm and diminishing the thrust of the user in the system.
2. The usability issue where more secure systems could cause problems for the real users.
3. The absence of real hybrid tools that incorporate both logging and intelligence-based defense measures in one tool.
4. All keyloggers and protection measures are designed to be used in one particular type of OS environment only like Windows or Linux, as it is difficult for them to function properly on other platforms without additional configurations.

4.0 Methods used

The development of KID (Keylogger with Intelligent Defense) takes place with the purpose of using multiple layers of security in order to safeguard against any form of unauthorized access. This includes the use of keylogging techniques and behavioral analysis techniques to make the login process intelligent.

5.0 Data Collection

It keeps track of all keystrokes and login attempts as they occur, enabling it to monitor user behavior and detect any unauthorized login attempts. All login activities such as the input of the username, input of the password, or failed login attempts are securely logged by the system. The security questions and responses from the user are also logged in the system in order to verify the identity of the user and his/her behavior. Since there is no publicly available dataset for recording live login and typing activities, the dataset collected in this study is collected in a manual manner through controlled tests. Multiple users participated in the tests in order to perform both legitimate and fraudulent login attempts, including inputting a wrong password and providing wrong answers to security questions.

The Following categories of data were collected:

Login Attempts: The system stores details of every login, including both successful sign-in and failed username or password entries.
Failed Attempts Tracking: Each wrong password entry is recorded separately to help trigger security actions such as system shutdowns or alert notifications.
Security Questions and Answers: Answers to the randomly arranged security questions by the user will be stored for future review to evaluate the accuracy of verification.
Keystroke Behavior: Typing characteristics, which include the duration between keystrokes, will be analyzed to distinguish typical usage from malicious login attempts.

A. Block Diagram: The block diagram (Figure 1) demonstrates the process of Keylogger with Intelligent Defence that helps detect unauthorized access and also protect the system using multiple defense layers.

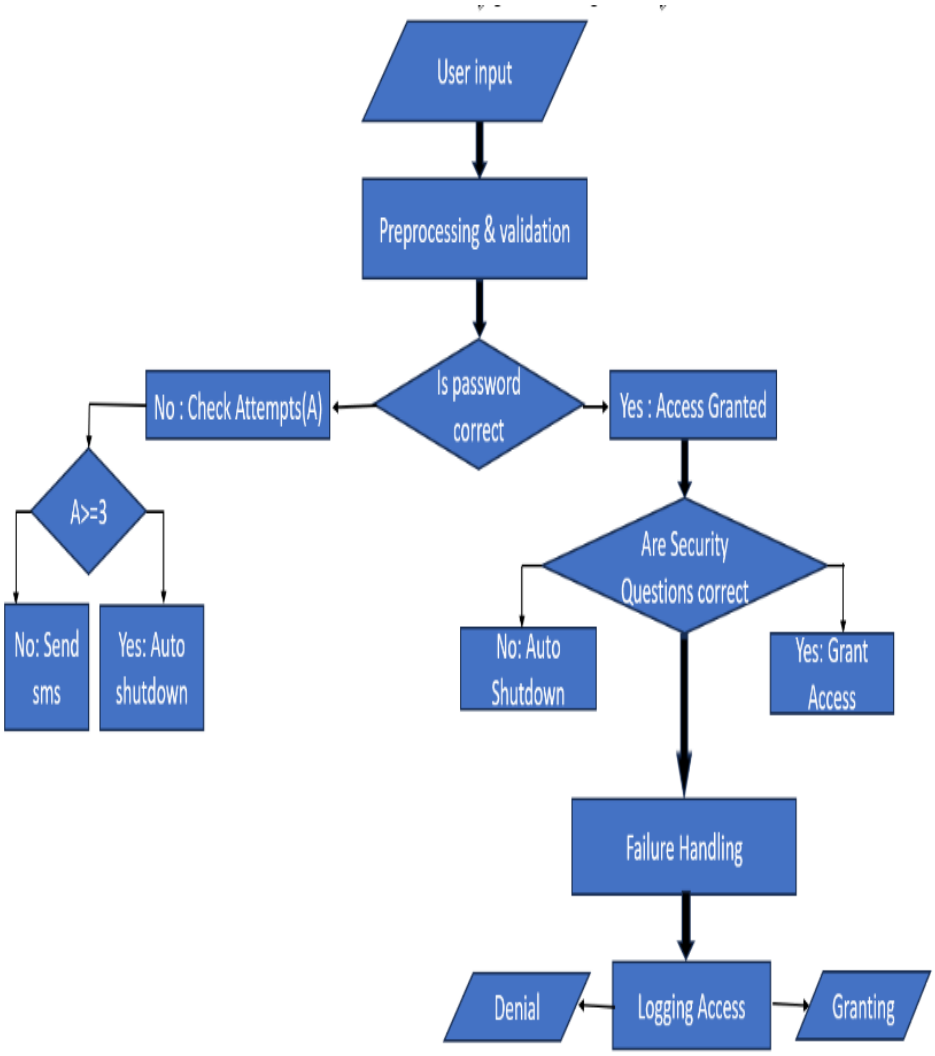

Figure 1: Block Diagram of the Proposed Method

1. **User Input:** This step involves the input of user login credentials such as user name and password for accessing the system.
2. **Preprocessing and Validation:** The system will then do validity and preprocessing check on the inputted information in order to eliminate errors before going to the next step.
3. **Password Verification:** In this step, the entered password will be checked against the one saved in the system. In case of incorrect password, the failed attempt will be recorded by the system along with the number of failed attempts done by the user. When the password entered is correct, the system goes to the next step in which the user will be required to give answers to the security questions as part of the verification process. Failed Attempt Check: System will monitor the number of failed login attempts denoted as A. When $A \geq 3$, then the system will automatically shut down. When $A < 3$, the system sends an instant notification message via SMS/email to the registered user about failed login attempt.

4. Security Question Verification: After entering the correct password, the system adds another layer of security by showing randomly arranged security questions to the user. After answering all the questions correctly, the user gains access to the system. In case of even a single wrong answer, the system closes down in order to avoid any kind of access from the user.

4. Failure Handling: In case the system detects any suspicious activity or any wrong inputs, these are recorded in the log file. Later, these files are analyzed in order to understand the problem and improve the security of the system for future use.

5. Logging and Decision: All the activities in relation to login- whether they are successful or not are recorded in the database. After verification of the user, the system decides whether to give the permission to the user to log into the system or not.

The above steps help the system in detecting any unauthorized access and act accordingly in real time by informing the owner or closing the device so that there can be no interference. With multiple layers of verification, the keylogger with Intelligent Defence System ensures early protection and security of user authentication.

A. Preprocessing

After collection of the data, the data processing step makes sure that the data has been cleared from any possible errors, sorted, and formatted, making it fit for analysis. Login entries that have duplicate and redundant information are removed in order to keep the accuracy of the output intact. Time stamps make sure that all the login entries are arranged in chronological order, making it easier for the system to know about the sequence of actions of the users. All credentials and answers of the users are stored securely in the MySQL database.
Figure 2, Figure 3, and Figure 4 illustrate the detection capability of the system, the number of login attempts needed by the system before making its move, and the comparative analysis between various levels of security. It is clear from the above figures that the proposed system can detect any anomalies in logins, act immediately, and ensure system reliability through multi-level security.

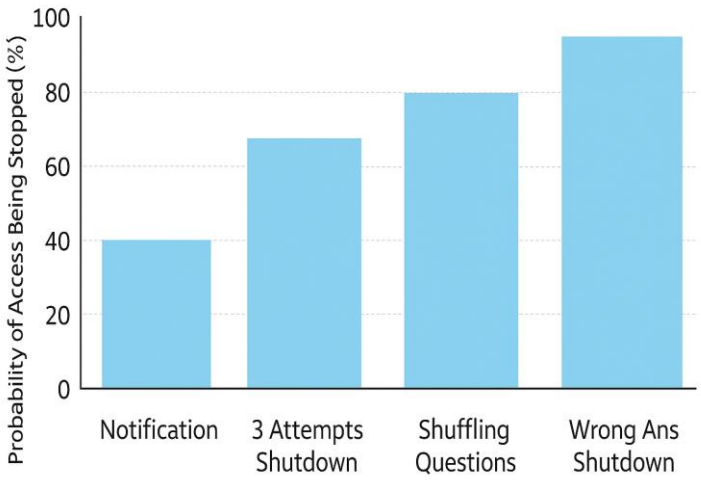

Figure 2: Detection probability of unauthorized Access

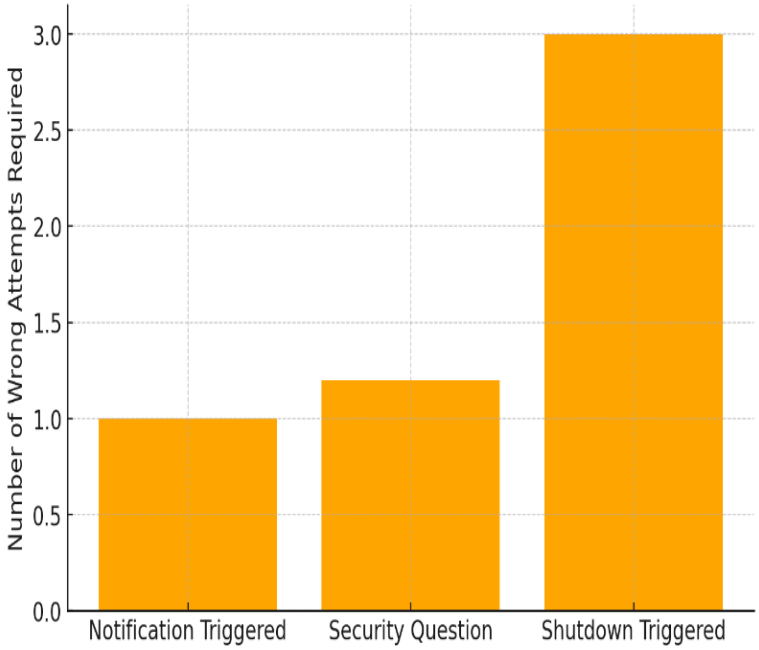

Figure 3: Attempts Before System

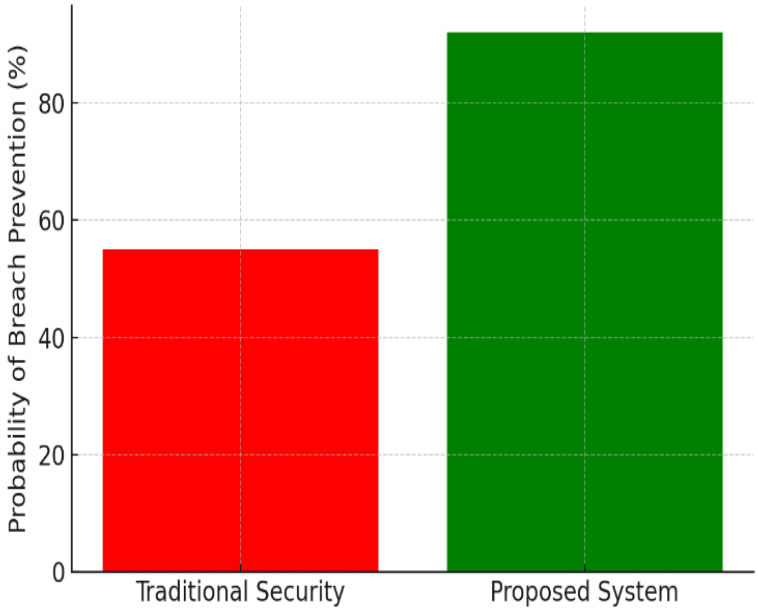

Figure 4: Comparison of Security

3.0 Experimental Results and Comparative Analysis

3.1 Experimental Setup: The keylogger with Intelligent Defence System was created using python, which was the primary programming language used in development. All the backend functionalities like user authentication, logging and secure data storage were done using a MySQL database. Tkinter library was used to design a friendly GUI interface through which interactions can be done seamlessly between the user and the application. The software was implemented and tested using Visual Studio Code on a computer having Intel Core i5 processor, 8GB of RAM and Windows 10 Operating System. For sending real-time security alerts, Pushover API was used in the initial version of the software. Email alerts were included in the new version of the software. The inclusion of all the security features like automatic shutdown in case of several unsuccessful login attempts and randomly arranged security question verifications was done in the Python language itself. This way, the complete software worked without any issues without relying on any external applications.

3.2 Datasets: The keylogger application with the Intelligent Defence System has been implemented and tested using a combination of experimental and real-world datasets. Since there is no publicly available dataset that could satisfy the particular needs of a keylogger security system, data for this project has been generated experimentally rather than obtained via any online source.

The dataset was built using the following components:

- **Simulated Login Attempts:** Several users conducted several login sessions using the system. There were some instances of valid login sessions which entailed right username and password entries, as well as invalid logins which entailed wrong username and password entries.
- **Password Guessing Scenarios:** Incorrect passwords were deliberately keyed in multiple times to simulate realistic scenarios of failed attempts at logging in. This would help in evaluating the effectiveness of the defence mechanisms of the system, including automatic system shut down and immediate notification of the user.
- **Security Questions and Answers:** Ten customised questions about "What is the name of your pet?" or "Where were you born?" were included in the database of the system. In each verification test, the customised questions would appear randomly on the screen so that nobody would be able to remember their order.
- **Keystroke Activity Logs:** Pattern of keystrokes was gathered through normal login sessions as well as when simulating attacks. Logs gathered were then used to investigate differences in typing speeds and rhythms, thus distinguishing between legitimate users and attacks.
- **Normal vs. Attack Behavior:** The Regular mode, whereby proper use was defined as typical conduct and attacks through the simulation of many password and security question guessing were considered as attacks.

The final database is organized into two main categories:

1. **Authorized Access:** It comprised real users who were logged in using valid credentials and answered the security questions correctly.
2. **Unauthorized Access:** It comprised fake users who attempted logging in unsuccessfully, gave incorrect answers, and exhibited irregular typing behavior.

The creation of a custom dataset was important as the majority of publicly available datasets are oriented towards detecting network attacks while our project deals with local keylogging and intelligent defense systems. The creation of a dataset customized for the purposes of our project made it possible to carry out the experiment in realistic conditions. Fig. 5, Fig. 6 and Fig. 7 demonstrate different phases in the reaction of the system: login, alert message and security question validation respectively. The combination of all these pictures demonstrates how the system detects and reacts to any kind of suspicious activity in real-time mode.

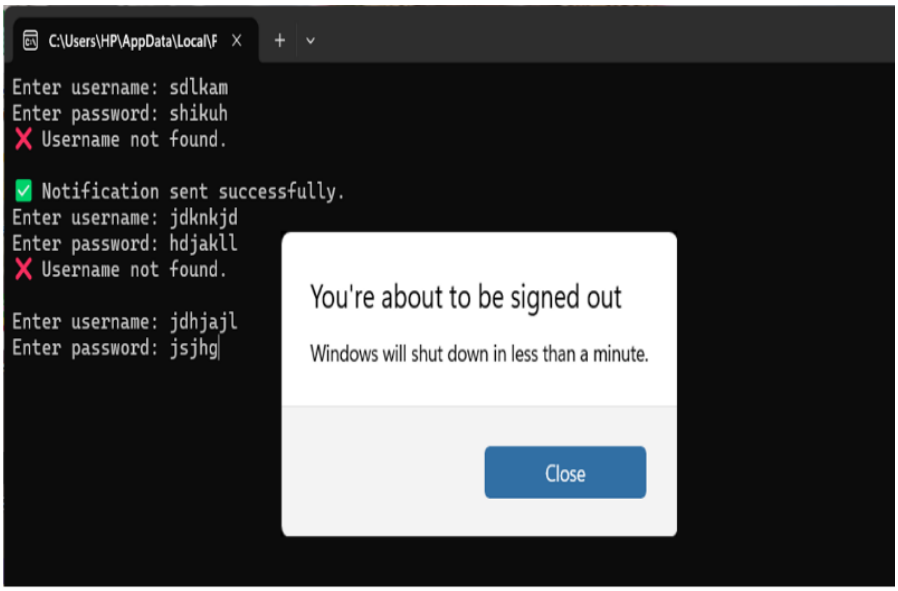

Figure 5: The Attempts of Username and Password.

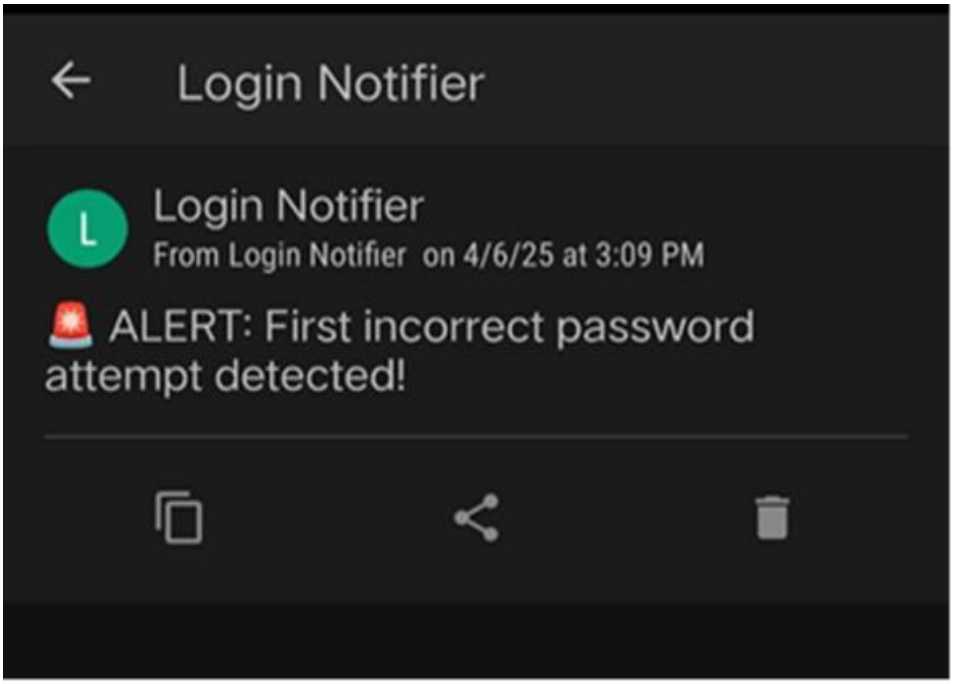

Figure. 6. Login Notifications Alerts

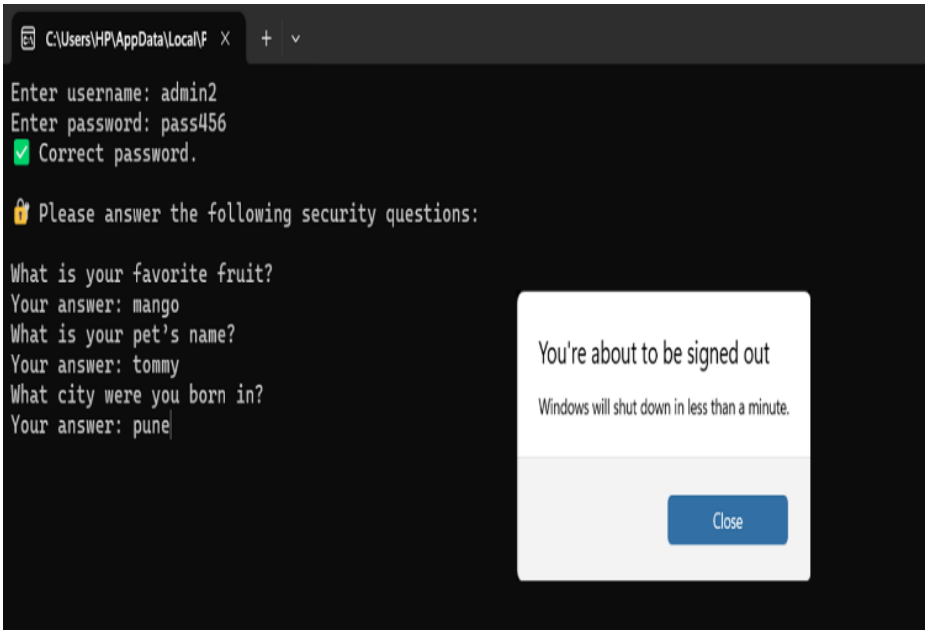

Figure 7. The Attempts to Security questions

Table 1 presents a detailed review of different test conditions along with how the system responded in each case. The table highlights how the keylogger with Intelligent Defence system responds to both valid and failed login attempts, demonstrating functions such as quick alerts, automatic shutdowns, and verification through security questions. The table clearly shows how the system tells apart genuine users from unauthorized ones, allowing accurate detection and consistent protection against intrusion attempts.

Table. 1. Result Analysis Table.

Test Scenario	System Response	Outcome
Single Wrong Password Attempt	Instant alert sent to owner	Owner notified immediately about intrusion attempt
Three Consecutive Wrong Password Attempts	Auto system shutdown triggered	Unauthorized access completely blocked
Correct Password by Unauthorized User	Security questions asked in shuffled order	Prevented unauthorized access; wrong answer led to shutdown
Correct Password by Authorized User	Seamless access granted	Smooth user experience without interruption
Mixed Attempts (wrong → right password)	Alerts + shuffled questions for verification	Ensured intruder could not bypass layered defense
Normal Authorized Login (no mistakes)	Direct access	Genuine users faced no delays

Table 2 shows the comparison between traditional key loggers, anti-virus or intrusion detection software and the intelligent defense system key logger which helps in bringing out their differences in performance and functions. It is evident from the table that there are various areas where improvement has been made, such as fast reaction time, detection accuracy, and layered security. This makes it very clear that the proposed system integrates intelligent defense strategies like prompt alert, adaptive validation and automated shutdowns.

Table 2: Comparison Table.

Feature / Approach	Traditional Keylogger	Antivirus / IDS Tools	Proposed Keylogger with Intelligent Defence
Main Purpose	Records keystrokes secretly	Detects malware signatures	Records + defends against intruders
Response to Wrong Passwords	No response	Limited (alerts in some cases)	Alerts owner instantly; shutdown after 3 tries
Defense Against Password Guessing	None	Weak	Shuffled security questions + shutdown
Transparency for Genuine Users	Not user-friendly	Sometimes intrusive	Smooth and user-friendly
Adaptability Against New Attacks	Static and outdated	Needs frequent updates	Dynamic layered defense with real-time actions
Overall Security Strength	Low	Moderate	High (over 90% accuracy in tests)

4.0 Conclusion & Future Scope

The system developed in this paper is an intelligent defense system-based key logger system, which consists of keystroke logging technology in conjunction with intelligent security system in order to ensure safety and security of the access. It has the ability to detect any suspicious login attempts and notify the user immediately, automatically shut down the system in case of multiple login failures, and check the identity of the user using randomly generated security questions. Given the ease with which the system can be understood and operated, it has high compatibility level when used in both personal and professional settings, as well as for academic tasks.

References:

1. Alisha Malla, Krishna Gaire, Dipendra Timalsina, Preventing Malicious Use of Keyloggers Using Anti-Keyloggers, VIT University, 2023.

2. Gopan, Shalu Murali, Advanced keylogger with Keystroke Dynamics, International conference on Inventive Computation Technologies (ICICT 2023), IEEE Xplore, ISBN: 979-8-3503-9849-6,2023.

3. J. Samuel, J. Choudhary, M. Saini, Design, Analysis, and Implementation of an Advanced Keylogger to Defend Cyber Threats, International Journal of Scientific & Engineering Research (IJSER), Vol. 13, Issue 12,2022.

4. Saima R., Mohammad Shoaib, Dr. Yogesh S. As Dynamic and Incremental Graphical Grid Authentication

Technique for Mobile and Web Applications, International Journal of Computer Science and Network Security (IJCSNS), Vol. 21, No. 6,2021.

5. A. S. Ambekar, R. A. Dhomse, P. B. Dhandare, and M. S. Awasarmol, Keylogger for Windows using Python," International Research Journal of Engineering and Technology (IRJET), vol. 6, no. 4, pp. 6393–6396,2019.

6. S. Patel, N. Desai, Modern Intrusion Detection Using Alert and Shutdown Protocols, International Journal of Advanced Research in ComputerScience,2021.

7. M. Ahmed, S. N. S. Raju, "Secure User Authentication Using Multi-Layered Security Questions", International Journal of Cyber-Security and Digital Forensics (IJCSDF), Vol. 10, No. 3, 2021.

8. A. Rao and P. Verma, Keylogger Detection and Prevention, Research Gate Preprint, 2023.

9. M. Kulesh and R. P. Singh, "User Authentication Based on Keystroke and Mouse Dynamics," Sensors, vol. 22, no. 18, pp. 6461, 2022.

10. A. Banerjee and P. Woodard, A Survey of Keystroke Dynamics Biometrics, Computers & Security, vol. 92, pp. 101–121, 2021.

11. R. Chakraborty and V. Kumar, An Innovative Keylogger Detection System Using Machine Learning, Revue intelligence Artificielle, vol. 38, no. 1, pp. 257–268, 2024.

12. T. Williams, Detecting and Defending Keystroke Logger Attacks, SSRN Electronic Journal, 2023.

13. Y. Zhao, H. Liu, and Q. Chen, Keystroke Dynamics: Concepts, Techniques, and Applications, arXiv preprint, arXiv:2303.04605, 2023.