International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

# An Appraisal of a Keylogging and Cryptography-Based Real-Time Keystroke Monitoring System for Enhancing Cloud Security

**Rohit Mourya[1], Kunika Patil[2], Srivaramangai R[3]**

[1]University of Mumbai, Department of Information Technology, Vidyanagari, Santacruz (E), Mumbai-400098, India
Email: *rohitmourya455[at]gmail.com*

[2]University of Mumbai, Department of Information Technology, Vidyanagari, Santacruz (E), Mumbai-400098, India
Email: *kunikapatil[at]gmail.com*

[3]University of Mumbai, Department of Information Technology, Vidyanagari, Santacruz (E), Mumbai-400098, India
Email: *rsrimangai[at]gmail.com*

Abstract: ***An insider attack is a security threat that occurs when someone with authorized access to an organization's systems or data maliciously misuses that access for malicious purposes. This type of attack is particularly dangerous because the insider often has knowledge of the organization's systems, processes, and sensitive information, making it easier for them to avoid detection and carry out their nefarious activities. To mitigate the risks associated with insider attacks, organizations should implement security measures such as access controls, monitoring and logging of user activities, employee training on security best practices, and regular security audits to detect any suspicious behavior. It is essential for organizations to have a comprehensive insider threat management program in place to prevent, detect, and respond to insider attacks effectively. This work explores the concept of keylogging as a potentially beneficial tool for enhancing cybersecurity measures, particularly in the context of safeguarding data stored in cloud computing environments. Keylogging, traditionally associated with malicious activities like identity theft and financial fraud, is harnessed in this research to counter insider threats to cloud data security. By developing a system that employs keylogging techniques alongside cryptography, real-time alerts can be generated to notify authorized individuals of suspicious activities, enabling immediate actions to be taken to protect sensitive cloud information. The project aims to shift the narrative around keylogging from a tool of intrusion to a tool of defense, highlighting its potential to be utilized as a safety measure in cybersecurity practices. By leveraging keylogging and cryptography in a proactive manner, organizations can better mitigate internal threats and enhance the overall security of their cloud infrastructure.***

**Keywords:** Keylogger, Cryptography, Insider malicious, Keystroke logging, Public Key Infrastructure

## 1. Introduction

Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored. Keylogging can also be used to study human computer interaction. A keylogger is a type of malware (hardware or software) that has the ability to log each keystroke entered on an infected device. The keylogger is capable of recording private information. As a result, it poses a serious risk to cybersecurity since it enables cybercriminals to access private data without authorization and utilize it for nefarious objectives like identity theft, financial fraud, or other destructive acts. An instrument called a keylogger may record keystrokes made on a keyboard automatically and because of this, an attacker can employ this method to access private information in a secured database without having to break into the house Numerous keylogging methods exist: they range from hardware and software-based approaches to acoustic analysis. Keyloggers have become a significant threat to cybersecurity, posing a major challenge to individuals and organizations alike. These malicious programs, either hardware or software based, can stealthily record every keystroke entered on a compromised device, capturing sensitive information such as passwords, credit card numbers, and personal messages. This stolen data can then be exploited by cybercriminals for various nefarious purposes, including identity theft, financial fraud, and illegal activities. The objective of this research is to apply keylogging for the securing the data on cloud in the easiest way possible. Keylogging has been always used as the intrusion method to steal the data or to harm any organization. But it can also be used as a safety measure. Cloud computing is the major growing platform for the storage of the data and also becoming the center of attraction to the attackers. Organizations have all the possible security approaches to safeguard their systems from the outside attacker but it is weak for insider mitigators. Organizations mostly acknowledge the breaches long time after it has committed. In this approach the main objective is to record the keystrokes and send the real time alert to the authorized person to take the immediate actions to safeguard the system. The purpose of this project is to safeguard the cloud information from such malicious insider with the help of keylogging and cryptography.

## 2. Literature Survey

This section gives a detailed analysis of various research works that has been done in three areas identified by the authors namely insider attack, Key logging and Cryptography.

### 1) Insider Attack

Zulkefli Mohd Yusopa &Jemal Abawajyb[47] reviews existing research on mitigating insider threats, including methods based on attack trees and dependency graphs. However, these methods may not be scalable for large-scale cloud deployment. The authors conclude that there is no perfect solution yet, and further research is needed to develop effective mitigation strategies for insider threats in cloud computing. Olivier De Vel et al [48] examines how data analytics can be used to address insider threats in information systems. It focuses on three main insider types: traitors, masqueraders, and unintentional insiders. Uniquely, it considers early-stage threats that could lead to someone becoming a malicious insider. The survey categorizes existing mitigation schemes on the basis of the data source used for analysis: host, network or contextual data. The effectiveness of each scheme against various insider threats, data extraction methods, and decision-making algorithms is reviewed and compared. Finally, this study identifies research gaps and challenges in mitigating insider threats using data analytics. Kunal Kumar Mandal & Debayan Chatterjee [49] focuses on insider threats in cloud computing, particularly from rogue system administrators and outsourced resources. Although technical solutions exist, the authors argue that the most effective approach is to combine technical measures with strong security policy. The proposed solution provides strong protection, but it may lead to a slower response time and an increase in HR costs for managing system administrators. This study acknowledges the trade-off between security and user experience and proposes possible adjustments to address these limitations. Adrian Duncan et al [50] examines insider threats in cloud computing. In view of the increasing dependence on cloud storage, understanding insider attacks is crucial. This study explores how traditional insider threat definitions might not fully capture the nuances of cloud environments. It highlights new potential insider categories in the cloud, including nation-states and other cloud customers. It also discusses the challenges associated with the detection of insider attacks due to the hidden nature of cloud data management and the potential involvement of third parties. William R Claycomb & Alex Nicoll [51] examines insider threats in cloud computing. While traditional insider threats continue to be relevant, cloud environments offer new attack possibilities. The authors explore three types of cloud-related insider threats: rogue administrators, those exploiting cloud vulnerabilities for theft, and those using the cloud to attack internal systems. It argues that existing data protection techniques can still be effective if they are applied rigorously. Atulay Mahajan &Sangeeta Sharma [52] investigate the security risks associated with hostile insiders in cloud computing environments. Because they have authorised access, malicious insiders like rogue administrators can steal or misuse data. In order to combat insider threats in the cloud, the paper highlights the necessity for enhanced security measures. Creating plans for the identification, stop, and lessening of such attacks is part of this. The authors advocate for industry-wide guidelines and recommended practices to tackle vulnerabilities unique to cloud computing settings. T. Gunasekhar et al [53] suggests a technique that makes use of several cloud service providers to safeguard sensitive data stored in cloud storage. Malevolent insiders who might pilfer or alter data are the cause for concern. Strong encryption is used to encrypt data, and the encrypted data and encryption keys are then stored in different clouds as part of the solution. In this manner, the data cannot be decrypted by an insider who has access to a single cloud. The paper notes certain limitations, such as possible side-channel attacks and the complexity of key management. To address these issues, they intend to conduct more research.

**2) Keylogging**

Robbi Rahim et al [14] stated that a keylogger, whether hardware or software-based, monitors and records keyboard keystrokes, sometimes even sending logs to specific emails periodically. While it can be legitimately used for monitoring employee productivity or law enforcement purposes, it can also be misused for data theft and password capture. The system employs an exact string matching algorithm to convert user-entered words like "Password" into ASCII form for comparison and recording. This particular keylogger is developed using Visual C# and operates on the Windows 8.1 OS, capturing activities in Microsoft Word and browsers. Kavya .C and Suganya.R [15] details various password attack techniques employed by hackers to compromise systems and gain unauthorized access. Techniques include dictionary and brute force attacks targeting weak passwords, phishing methods using deceptive emails or links, rainbow table attacks exploiting hash functions, and shoulder surfing where attackers glean passwords by observing users. Additionally, there's mention of keyloggers, both hardware and software-based, which covertly record keystrokes and other sensitive data, enabling hackers to capture credentials and personal information. The article emphasizes the pivotal role of keyboards in these attacks, where keyloggers intercept and log every key pressed, compromising user data like bank details. Lulu Yang et al [16] created new method called KCA using a special network and learning technique to analyze keystrokes. They combine this method with voting to improve accuracy in authentication. They test the KCA method on a dataset called Clarkson II and show promising results. Mayank Srivastava et al [17] created a program called a key logger. It secretly records the keys pressed by the person using the computer and also notes the applications they are using. The information is stored securely in a file and uploaded to a server every hour. It also collects additional details like the person's IP address, MAC address, and username. Abdul Ahad et al [18] discussed keystroke logging, which involves recording every key pressed on a computer, capturing details like key names, duration of presses, and timestamps. Keyloggers can be either hardware or software-based, with hardware keyloggers discreetly placed between a keyboard and a computer, while software versions operate invisibly on a target system. Software keyloggers can be local, capturing data on the same system, or remote, enabling monitoring from afar. The implementation leverages Python 3.10.7 and various libraries like `pynput` for device monitoring, `smtplib` for email communication, and `datetime`, `os`, and `urllib` for tasks such as time tracking, system commands, and network requests, respectively. The overall objective of this approach is to clandestinely gather user keystrokes, potentially exposing sensitive information, and transmit this data to designated recipients. Manan Kalpesh Shah [19] proposed method involves a program that prompts users to sign in using their email credentials. If incorrect details are entered, an error appears, preventing data transmission. Correct inputs initiate keystroke recording, with

conditions set such as a word limit. Upon reaching this limit, the recorded keystrokes trigger actions like taking a screenshot using `pyscreenshot.grab()` and saving it. The program encodes this data into a string using MIMEText and sends it to the user's provided email. Essential functional components include an SMTP server, an email library, and an active internet connection. However, this approach poses a security risk, as sensitive information like passwords can be captured and sent to potential intruders. Preeti Tuli and Priyanka Sahu[20] proposed the method that integrates both signature-based and hook-based techniques to detect and counteract keyloggers. Signature-based detection identifies keyloggers by recognizing specific files, DLLs, and registry entries but may miss unknown threats. Hook-based detection employs functions like SetWindowsHookEx() to monitor system events such as key presses; anti-keyloggers can intercept this, preventing keystroke capture. Setting hooks involves binding filter functions to system events in a sequential chain, enabling tracking or modification of events. Centralizing company workflows through a universal inbox facilitates comprehensive recording and monitoring of internal communications. Furthermore, integrating all office devices creates a unified platform for efficient and centralized monitoring, enhancing overall security and oversight. Sahil Prasad Bejo and et. al [30] provides a comprehensive guide on the usage, detection, and protection using keyloggers, detailing both hardware and software variants. Through experiments, the authors demonstrate the capability of keylogger applications to record keyboard-related user behaviors, with results automatically stored in accessible log files and transmitted to the owner via email. They outline plans for an updated version of the software capable of recording remote and local activities, including virtual keyboard keystrokes, alongside video and audio capture, with encryption for log file security. Marco Salas-Nino[31] explores the historical evolution and current landscape of keyloggers, questioning the effectiveness of traditional anti-keylogger approaches in today's cybersecurity realm. With keyloggers continuously evolving, including recent AI-driven attacks like 'BlackMamba', the future of anti-keyloggers faces uncertainty. Developers must innovate to counteract these sophisticated threats, emphasizing the need for evolving anti-keylogger technologies to safeguard against emerging cyber risks. S. Sagiroglu and G. Canbek [32] includes the positive and negative impact of the keyloggers this paper discusses the various types of keylogging techniques including software keyloggers, kernel-level keyloggers, software keyloggers, windows keyboard hook method etc. This paper also includes the positive uses of the the keylogging. Bhardwaj Akashdeep & Goundar Sam[33] thoroughly examines keyloggers, detailing their history, types, functionalities, and the risks they pose to individuals and organizations. It also delves into detection and prevention techniques, including anti-virus software and biometric authentication, while discussing their effectiveness and limitations. Additionally, the paper emphasizes the importance of awareness and education in combating keylogger threats and explores future trends such as advanced encryption and Threat Intelligence solutions. Overall, it underscores the urgent need for proactive measures to safeguard sensitive data in the face of growing keylogger attacks, serving as a valuable resource for understanding and addressing this ongoing cybersecurity challenge. Darshanie Sukhram Thaier Hayajneh [34] The paper underscores the importance of user awareness and robust password practices to counter sophisticated phishing and social engineering threats, noting keyloggers' ability to compromise even strong passwords. It assesses the efficacy of keylogging and anti-keylogging software in capturing information and thwarting keylogger threats, alongside discussing risk assessment and mitigation strategies. Additionally, it advocates for organizations to augment password managers and two-factor authentication with validated anti-keylogging tools, highlighting the complementary focuses of anti-keyloggers and anti-virus software. Ultimately, organizations are encouraged to tailor their cybersecurity measures based on individual risk assessments to ensure comprehensive protection. Reiner Creutzburg [35] provides a literature review of keyloggers, covering both hardware and software variants, including those designed for mobile devices. It discusses their functionalities, availability, and detection methods. Part II of the article will delve into keyloggers specifically for mobile devices, as well as the ethical and legal considerations surrounding their use. Shreya Jaiswal1, Prof. B. Jana2 [36] discusses keyloggers' role as rootkit malware, capturing keystroke events to collect sensitive data covertly, posing a threat to activities like online banking and email communication. While antivirus software is ineffective against unknown keylogger variants, the paper offers an overview of keylogger programs, their characteristics, and operational methods, alongside examination of detection techniques and proactive measures. Ultimately, the paper aims to raise awareness about keylogger threats, provide insights into detection, and propose countermeasures against potential security risks. Thorsten Holz Markus Engelberth Felix Freiling [37] explores the underground economy trading stolen digital credentials, with a focus on keylogger-based theft via dropzones. Over seven months in 2008, data from over 70 dropzones revealed a significant trove of stolen information, shedding light on attacker motivations and the scale of illicit markets. However, the study acknowledges limitations in its user simulation method, which may overlook specific instances of keylogger activity. Notably, keyloggers primarily target major online banking sites and extract data from Protected Storage, but they may miss narrower targets. To address this, employing advanced malware analysis techniques like multi-path execution and taint tracking could enhance detection accuracy and improve overall system effectiveness. Mehdi Dadkhah and et al [38] explores how keyloggers are used by cyber attackers to steal user credentials across various online platforms. Despite the presence of security software meant to identify keyloggers, the paper argues that these tools can be modified to avoid detection. The authors intend to illustrate this by developing a keylogger and altering its design, then testing it against prominent security software. The goal is to underscore the difficulty in detecting keyloggers and to stress the importance of improving detection techniques to combat increasingly sophisticated threats. Akashdeep Bhardwaj and Sam Goundar [39] emphasizes that regular scanning, antivirus, and user awareness are crucial for safeguarding against keyloggers. However, the authors demonstrated a keylogger technique capable of capturing keystrokes and screenshots undetected by any scanner. They propose a virtual keyboard layout that enhances security by randomly exchanging vertically adjacent keys from the traditional QWERTY layout, with random spacing, ensuring both accessibility and security.

Aarushi Dwivedi and et al [40] This study presents an advanced software keylogger compared to existing ones, focusing on features and CPU efficiency. The findings suggest that the proposed keylogger offers enhanced functionality while consuming minimal CPU resources, making it harder for users to detect. Additionally, software keyloggers are favored over hardware counterparts, as demonstrated in a comparison between the top Windows-based software keyloggers of 2020 and the "Adv_Klogger" introduced in this research. The evaluation highlights specific features of each keylogger, aiding in understanding their capabilities. Sivarajeshwaran and et.al [41] This project tackles the threat of software keyloggers that steal user information. The authors created a user-space keylogger to understand its behavior and then developed an anti-keylogger to detect and close such programs running in stealth mode. This anti-keylogger compares running software with a model to identify and terminate potential keyloggers, protecting users from their malicious activities. The project was successfully tested in Microsoft Visual Studio, demonstrating its potential as a valuable security measure. Yadav Sarita et al [54] In this paper, the keylogger under discussion is a user-space programme that can be easily deployed and executed because it doesn't require any special permissions to function. For monitoring purposes, it logs keystrokes, mouse events, and window titles. The programme provides the ability to email gathered data at predetermined intervals or save it locally. It also has a stealth mode that hides its existence from the user and makes it hard to find—even with antivirus software. It functions like a regular Windows application and saves keystroke data in encrypted format, guaranteeing data security even with its stealth capabilities. M. B. Bondada and S. M. S. Bhanu [55] The proposed approach addresses the major concern of insider threats in cloud computing by utilising a host-based user profiling technique based on keystroke dynamics. By analysing user behaviour and implementing a retraining mechanism, the system effectively reduces the risk of insider attacks without the need for additional hardware or changes to existing cloud infrastructure. The results show a significant increase in the number of keystrokes detected before an imposter is identified, demonstrating the effectiveness of the approach in improving cloud security. Future enhancements may include incorporating additional behavioural analysis techniques to improve system efficiency.

### 3) Cryptography

Lei Zhang et al [21] discussed the significance of cryptography in addressing security challenges in cloud storage services. The paper reviews various cryptography-based approaches to ensure cloud storage security, focusing on methods that enable users to maintain and verify their own security without complete reliance on a fully trusted cloud service provider (CSP). Matt Blumenthal [22] This study introduces advancements in public-key cryptography and evaluates their limitations and proposes strategies to enhance the weaknesses. This paper mainly disscus about symmetric encryption(Secret-key encryption) and asymmetric(Public-key encryption) encryption method along with their strength and weakness with the solution over weakness. Dr.Asha.V et al [23] discussed ways to enhance cloud database security by using cryptography, blockchain, and other technologies. It also addresses challenges and security threats related to patient databases in current systems. Cryptography is identified as an effective method to secure and protect sensitive data in the cloud. The study analyzes existing systems and proposes a new model to overcome their limitations. Md. Abu Musa and Md. Ashiq Mahmood [24] implemented a symmetric key encryption technique. The approach encrypts files locally on the client-side before uploading them to the cloud. During decryption, the file is decrypted on the client-side using the encryption-generated key. The algorithm uses a unique method to calculate the key value, providing improved security and performance for large files. This extra layer of security helps prevent unauthorized access to sensitive information and addresses the lack of standardization. Shaffali Wadhawan and Shilpa [42] The paper provides an in-depth exploration of network security and cryptography, emphasizing their role in protecting communication against hostile environments. It discusses the use of both software and hardware technologies to safeguard data stored and transmitted over wireless networks. Cryptography is highlighted as crucial for encrypting data and employing techniques like steganography to thwart cyber attacks. Overall, the study underscores the importance of cryptographic techniques and network security measures in safeguarding company data and communication from malicious actors in today's technology-driven landscape. A. Joseph Amalraj, Dr. J. John Raybin Jose [43] This paper provides a comprehensive overview of cryptography techniques such as AES, DES, 3DES, Blowfish, RSA, and CL-PKC, underscoring their importance in securing data amidst widespread online transactions. Through an analysis of various encryption methods, including AES, 3DES, Blowfish, and DES, the study concludes that Blowfish demonstrates superior performance. Looking ahead, the paper suggests optimizing encryption techniques for reduced time and power consumption, while maximizing speed and energy efficiency. Additionally, it emphasizes the crucial role of cryptography in ensuring network security, particularly in email systems that employ Public Key Infrastructure (PKI) to enhance security and efficiency, despite facing challenges like certificate management and scalability. Dr. Qaim Mehdi Rizvi, Rahul Singh Kushwah [44] Exploring Modern Cryptography provides a comprehensive examination of contemporary cryptography, elucidating its role in securing digital data and communication. It covers the history, principles, techniques, and real-world applications of cryptography, emphasizing its significance in ensuring confidentiality, integrity, and authenticity. Despite challenges like quantum computing and key management complexities, cryptography evolves to tackle emerging threats and advancements. Future directions include developing post-quantum cryptographic algorithms, enhancing privacy techniques, securing IoT devices, and integrating with emerging technologies, reaffirming its critical role in safeguarding sensitive information and fostering trust in the digital realm. Li, Huixin, and Yubo Wang [45] Cryptography has played a crucial role in secure communication throughout history, evolving from ancient times to modern eras with technological progress. Initially used for military and religious purposes, it expanded into various applications, notably during World War II, influencing cipher development. Today, cryptography remains significant, with the widespread adoption of cryptocurrencies showcasing its modern applications. This essay explores the historical

evolution of cryptography and its diverse uses across different time periods, highlighting its enduring relevance and impact on secure communication. Rusul Mansoor et al [46] The literature survey provides an overview of cryptography, focusing on secure communication techniques and encryption algorithms. It discusses key theoretical components such as cryptography, secure key exchange, digital signatures, and authentication, all aimed at ensuring data confidentiality, integrity, and reliability. The survey emphasizes the critical role of encryption algorithms in data security, highlighting the importance of algorithm robustness and key confidentiality. Additionally, it explores modern cryptography techniques, encryption algorithm types, optimal choices, and the impact of different attacks on the encryption process.

**4) Analysis of the Literature**

The close inspection of various research papers has revealed that software keyloggers have been used extensively by 14 papers compared to hardware keyloggers and hybrid variety. Figure 2 describes the types of techniques used for detecting and preventing insider attack. It depicts that in most of the papers, machine learning and encryption are used 40%. Figure 3 depicts that Python is highly used as a development tool for machine learning and encryption.

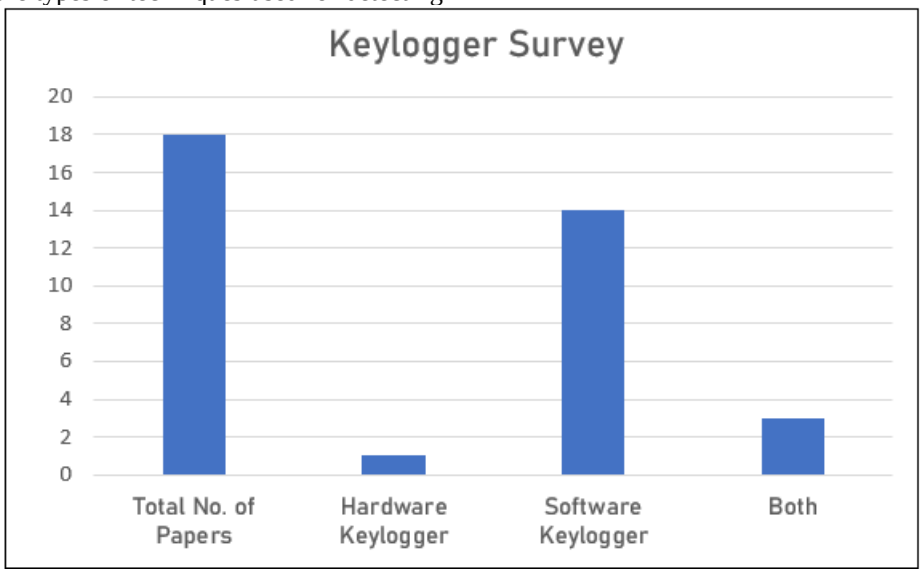


**Figure 1:** Types of Keyloggers used

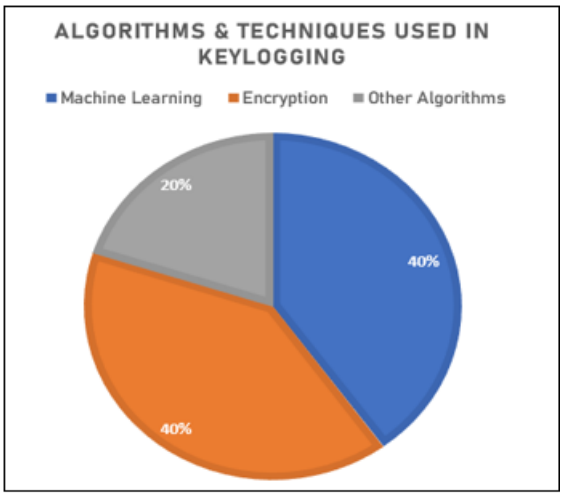


**Figure 2:** Algorithms and Techniques used in Keylogging

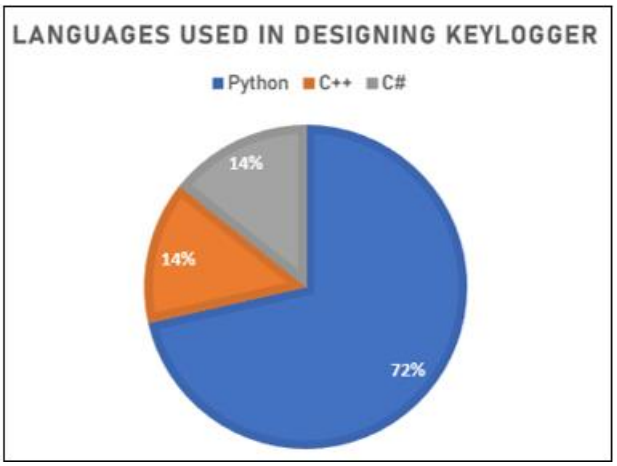


**Figure 3:** Programming Languages Used in Designing Keylogger

**Table 1:** Strengths and Weaknesses of Different Cryptography methods [22]

| Cryptography Method | Strengths | Weaknesses |
|---|---|---|
| Secret-key Cryptography | - Robust resistance to brute force attacks | - Necessity for secure exchange of private keys, which can be impractical - Compromise of a single private key compromises all users' security, especially as the number of participants increases |
| Public-key Encryption | - Eliminates the need for secure key exchange - Each user has unique public and private keys - Offers secure information exchange without requiring a prior secret key arrangement | - Computationally costly compared to secret-key cryptography - Vulnerable to certain brute force attacks - Vulnerable to man-in-the-middle attacks, where a malicious third party intercepts and alters communication |

| | | |
|---|---|---|
| Digital Signatures | - Provides verifiable sender authenticity and message integrity - Protects against message tampering - Enables sender identity confirmation through private key encryption and public key decryption by the recipient | - Lack of inherent time stamping makes it susceptible to unauthorized use of compromised private keys - Difficulty in repudiating false messages without generating new private keys |
| Certificate Authorities | - Prevents man-in-the-middle attacks by verifying sender identity and issuing digital certificates | - Vulnerable to compromise, leading to issuance of false certificates - Can be exploited by attackers to discreetly impersonate parties involved in the communication |

Table 1 indicates the strengths and weaknesses of cryptographic methods as being reviewed by Matt[22]. Though many weaknesses are presented, cryptography is still considered to be one of the effective method of protection which in recent years have been developed using machine learning method. Thus a hybrid approach of machine learning and deep learning with cryptography has a lot of scope in defending the attacks.

## 3. Conclusion

Insider attacks pose a significant threat to organizations due to the malicious exploitation of authorized access by individuals with knowledge of sensitive information. To safeguard against such threats, implementing security measures such as access controls, monitoring user activities, training employees, and conducting regular security audits is crucial. Furthermore, this research suggests leveraging keylogging techniques in conjunction with cryptography as a proactive defense mechanism to enhance cybersecurity measures in cloud computing environments. By reframing keylogging from a tool of intrusion to a tool of defense, organizations can effectively mitigate internal threats and strengthen the security of their cloud infrastructure. The paper explores various keylogging methods, types of keyloggers, and effective mitigation strategies against insider threats. It also discusses the use of different cryptographic techniques to secure sensitive data. The findings indicate that software keyloggers are prevalent due to their simplicity and lower detection probability. Additionally, some keyloggers integrate advanced technologies such as machine learning algorithms like neural networks and SVM for enhanced performance. Encryption plays a vital role in safeguarding captured keylogs, with methods like whitespace encryption and Base64 algorithms being commonly employed. The survey underscores the critical role of cryptography in protecting data integrity.

## References

[1] Bulla, Chetan & Bhojannawar, Satish & Danawade, Vishal. (2013). Cloud Computing: Research Activities and Challenges. ijettcs. 2. 206.

[2] J. Surbiryala and C. Rong, "Cloud Computing: History and Overview," 2019 IEEE Cloud Summit, Washington, DC, USA, 2019, pp. 1-7, doi: 10.1109/CloudSummit47114.2019.00007.

[3] A. Mondal, S. Paul, R. T. Goswami and S. Nath, "Cloud computing security issues & challenges: A Review," 2020 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2020, pp. 1-5, doi: 10.1109/ICCCI48352.2020.9104155.

[4] Jathanna, Rohan & Jagli, Dhanamma. (2017). Cloud Computing and Security Issues. International Journal of Engineering Research and Applications. 07. 31-38. 10.9790/9622-0706053138.

[5] Cloud Computing: Security Issues and Research Challenges Moulika Bollinadi Under Graduate Student, MGIT, Hyderabad, Telangana, India. Vijay Kumar Damera Assistant Professor of IT, MGIT, Hyderabad, Telangana, India.

[6] Vaikunth Pai T. & Aithal, P. S. (2016). Cloud Computing Security Issues - Challenges and Opportunities. International Journal of Management, Technology and Social Sciences (IJMTS), 1(1), 33-42. DOI: http://dx.doi.org/10.5281/zenodo.569920.

[7] S. Surianarayanan and T. Santhanam, "Security issues and control mechanisms in Cloud," 2012 International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM), Dubai, United Arab Emirates, 2012, pp. 74-76, doi: 10.1109/ICCCTAM.2012.6488075.

[8] L. B. Bhajantri and T. Mujawar, "A Survey of Cloud Computing Security Challenges, Issues and their Countermeasures," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2019, pp. 376-380, doi: 10.1109/I-SMAC47947.2019.9032545.

[9] A. Narang and D. Gupta, "A Review on Different Security Issues and Challenges in Cloud Computing," 2018 International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, India, 2018, pp. 121-125, doi: 10.1109/GUCON.2018.8675099.

[10] P. Padma, R. Akshaya, H. Akshaya and R. Harini, "Perlustrate Study on Cloud Security and Vulnerabilities," 2021 4th International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, 2021, pp. 293-296, doi: 10.1109/ICCCT53315.2021.9711797.

[11] R. K. Nema, A. K. Saxena and R. Srivastava, "Survey of the Security Algorithms over Cloud Environment to Protect Information," 2022 10th International Conference on Emerging Trends in Engineering and Technology - Signal and Information Processing (ICETET-SIP-22), Nagpur, India, 2022, pp. 1-6, doi: 10.1109/ICETET-SIP-2254415.2022.9791643.

[12] Deepika, R. Kumar and Dalip, "Security Enabled Framework to Access Information in Cloud Environment," 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON), Faridabad, India, 2022, pp. 578-582, doi: 10.1109/COM-IT-CON54601.2022.9850906.

[13] Abukar, Yahye & Maarof, Mohd & Hassan, Fuad & Mohamed, Abshir. (2014). Survey of Keylogger Technologies. International Journal of Computer Science and Telecommunications. 5. 25-31.

[14] Rahim, Robbi & Nurdiyanto, Heri & Ahmar, Ansari & Abdullah, Dahlan & Hartama, Dedy & Napitupulu, Darmawan. (2018). Keylogger Application to Monitoring Users Activity with Exact String Matching Algorithm. Journal of Physics: Conference Series. 954. 012008. 10.1088/1742-6596/954/1/012008.

[15] Kavya.C,Suganya.R, "SURVEY ON KEYSTROKE LOGGING ATTACKS", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.9, Issue 4, pp.503-508, April 2021, Available at :http://www.ijcrt.org/papers/IJCRT2104074.pdf

[16] L. Yang, C. Li, R. You and B. Tu, "A Keystroke-based Continuous User Authentication in Virtual Desktop Infrastructure," 2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS), Chengdu, China, 2021, pp. 753-758, doi: 10.1109/ICCCS52626.2021.9449286.

[17] M. Srivastava, A. Kumari, K. K. Dwivedi, S. Jain and V. Saxena, "Analysis and Implementation of Novel Keylogger Technique," 2021 5th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2021, pp. 1-6, doi: 10.1109/ISCON52037.2021.9702433.

[18] A. Ahad, M. S. Khan and P. Saxena, "Analysis of Keylogging spyware for information theft," 2023 1st International Conference on Intelligent Computing and Research Trends (ICRT), Roorkee, India, 2023, pp. 1-4, doi: 10.1109/ICRT57042.2023.10146672.

[19] Devashree Kataria , Manan Kalpesh Shah , S Bharath Raj , Priya G, 2020, Real Time Working of Keylogger Malware Analysis, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 09, Issue 10 (October 2020),

[20] Priyanka Sahu et al, International Journal of Computer Science and Mobile Computing Vol.2 Issue. 3, March-2013, pg. 106-111

[21] L. Zhang, H. Xiong, Q. Huang, J. Li, K. -K. R. Choo and J. Li, "Cryptographic Solutions for Cloud Storage: Challenges and Research Opportunities," in IEEE Transactions on Services Computing, vol. 15, no. 1, pp. 567-587, 1 Jan.-Feb. 2022, doi: 10.1109/TSC.2019.2937764.

[22] Blumenthal, Matt. "Encryption: Strengths and weaknesses of public-key cryptography." CSRS 2007 1 (2007).

[23] A. V, A. P. Nirmala, B. K, A. Christi and N. A, "A Review on Cloud Cryptography Techniques to Improve Security in E-health Systems," 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2022, pp. 100-104, doi: 10.1109/ICCMC53470.2022.9753999.

[24] A. Musa and A. Mahmood, "Client-side Cryptography Based Security for Cloud Computing System," 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), Coimbatore, India, 2021, pp. 594-600, doi: 10.1109/ICAIS50930.2021.9395890.

[25] A. R. Patel, "Biometrics based access framework for secure cloud computing," 2020 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2020, pp. 1318-1321, doi: 10.1109/CSCI51800.2020.00246.

[26] Ahuja, M.S., Chabbra, S. (2011). Biometric Encryption: Combining Fingerprints and Cryptography. In: Mantri, A., Nandi, S., Kumar, G., Kumar, S. (eds) High Performance Architecture and Grid Computing. HPAGC 2011. Communications in Computer and Information Science, vol 169. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-22577-2_69

[27] Kun Huang, Jiangyong Shi, Ming Xian and Jian Liu, "Achieving robust biometric based access control mechanism for cloud computing," 2013 International Conference on Information and Network Security (ICINS 2013), Beijing, 2013, pp. 1-7, doi: 10.1049/cp.2013.2471.

[28] S. Alwahaishi and J. Zdrálek, "Biometric Authentication Security: An Overview," 2020 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), Bengaluru, India, 2020, pp. 87-91, doi: 10.1109/CCEM50674.2020.00027.

[29] S. P. Bejo, B. Kumar, P. Banerjee, P. Jha, A. N. Singh and M. K. Dehury, "Design, Analysis and Implementation of an Advanced Keylogger to Defend Cyber Threats," 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2023, pp. 2269-2274, doi: 10.1109/ICACCS57279.2023.10112977.

[30] Salas-Nino, Marco, Grant Ritter, Daniel Hamdan, Tao Wang and Tao Hou. “The Evolution of Keylogger Technologies: A Survey from Historical Origins to Emerging Opportunities.” ArXiv abs/2312.10445 (2023): n. pag.

[31] S. Sagiroglu and G. Canbek, "Keyloggers: Increasing threats to computer security and privacy," in IEEE Technology and Society Magazine, vol. 28, no. 3, pp. 10-17, Fall 2009, doi: 10.1109/MTS.2009.934159.

[32] Bhardwaj, Akashdeep & Goundar, Sam. (2020). Keyloggers: silent cyber security weapons. Network Security. 2020. 14-19. 10.1016/S1353-4858(20)30021-0.

[33] D. Sukhram and T. Hayajneh, "KeyStroke logs: Are strong passwords enough?," 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, USA, 2017, pp. 619-625, doi: 10.1109/UEMCON.2017.8249051.

[34] Creutzburg, Reiner. (2017). The strange world of keyloggers - an overview, Part I. Electronic Imaging. 2017. 139-148. 10.2352/ISSN.2470-1173.2017.6.MOBMU-313.

[35] Jaiswal, Shreya, and B. Jana. "Survey on Security Detection Techniques Using Keylogger." (2023).

[36] Holz, Thorsten & Engelberth, Markus & Freiling, Felix. (2009). Learning More about the Underground Economy: A Case-Study of Keyloggers and Dropzones. 1-18. 10.1007/978-3-642-04444-1_1.

[37] Dadkhah, Mehdi & Jazi, Mohammad & Ciobotaru, Ana-Maria & Barati, Elaheh. (2014). An Introduction to Undetectable Keyloggers with Experimental Testing. International Journal of Computer Communications and Networks. 4. 1-5.

[38] Bhardwaj, Akashdeep & Goundar, Sam. (2020). Keyloggers: silent cyber security weapons. Network Security. 2020. 14-19. 10.1016/S1353-4858(20)30021-0.
[39] Dwivedi, A., Tripathi, K. C., & Sharma, M. (2021). Advanced Keylogger- A Stealthy Malware for Computer Monitoring. Asian Journal For Convergence In Technology (AJCT) ISSN -2350-1146, 7(1), 137-140. https://doi.org/10.33130/AJCT.2021v07i01.028.
[40] S. Sivarajeshwaran, G. Ramya, and G. Priya, "Developing software based key logger and a method to protect from unknown key loggers," International Journal of Innovative Science and Modern Engineering (IJISME), vol. 7, pp. 2319–6386, 2015
[41] Shaffali Wadhawan, & Shilpa. (2023). A Study on Cryptography. International Journal of Engineering and Management Research, 13(2), 99–103. https://doi.org/10.31033/ijemr.13.2.15
[42] Amalraj, A. Joseph, and JJ Raybin Jose. "A survey paper on cryptography techniques." International Journal of Computer Science and mobile computing 5, no. 8 (2016): 55-59.
[43] Rizvi, Qaim Mehdi, and Rahul Singh Kushwaha. "EXPLORING MODERN CRYPTOGRAPHY: A COMPREHENSIVE GUIDE TO TECHNIQUES AND APPLICATIONS."
[44] Li, Huixin, and Yubo Wang. "The History of Cryptography and Its Applications." International Journal of Social Science and Education Research 5, no. 3 (2022): 343-349.
[45] Al-Amri, Rusul Mansoor, Dalal N. Hamood, and Alaa Kadhim Farhan. "Theoretical Background of Cryptography." Mesopotamian Journal of CyberSecurity 2023 (2023): 7-15.
[46] Yusop, Zulkefli & Abawajy, Jemal. (2014). Analysis of Insiders Attack Mitigation Strategies. Procedia - Social and Behavioral Sciences. 129. 581-591. 10.1016/j.sbspro.2014.03.716.
[47] L. Liu, O. De Vel, Q. -L. Han, J. Zhang and Y. Xiang, "Detecting and Preventing Cyber Insider Threats: A Survey," in IEEE Communications Surveys & Tutorials, vol. 20, no. 2, pp. 1397-1417, Secondquarter 2018, doi: 10.1109/COMST.2018.2800740.
[48] Kunal Kumar Mandal, Debayan Chatterjee . Insider Threat Mitigation in Cloud Computing. International Journal of Computer Applications. 120, 20 ( June 2015), 7-11. DOI=10.5120/21341-4352
[49] Duncan, Adrian & Creese, Sadie & Goldsmith, Michael & Quinton, Jamie. (2013). Cloud Computing: Insider Attacks on Virtual Machines During Migration. 493-500. 10.1109/TrustCom.2013.62.
[50] Claycomb William & Nicoll Alex. (2012). Insider Threats to Cloud Computing: Directions for New Research Challenges. Proceedings - International Computer Software and Applications Conference. 387-394. 10.1109/COMPSAC.2012.113.
[51] Mahajan, Atulay and Sangeeta Sharma. "The Malicious Insiders Threat in the Cloud." (2015).
[52] T, Gunasekhar & Komati, Thirupathi Rao & Reddy, Vuyyuru & Pasupuleti, Sai Kiran. (2015). Mitigation of Insider Attacks through Multi-Cloud. International Journal of Electrical and Computer Engineering. 5. 136-141. 10.11591/ijece.v5i1.pp136-141.
[53] Yadav Sarita & Mahajan, Anuj & Prasad, Monika & Kumar, Avinash. (2020). ADVANCED KEYLOGGER FOR ETHICAL HACKING. International Journal of Engineering Applied Sciences and Technology. 5. 634-638. 10.33564/IJEAST.2020.v05i01.112.
[54] M. B. Bondada and S. M. S. Bhanu, "Analyzing User Behavior Using Keystroke Dynamics to Protect Cloud from Malicious Insiders," *2014 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, Bangalore, India, 2014, pp. 1-8, doi: 10.1109/CCEM.2014.7015481.

## Author Profile

**Kunika Patil** is a student of second year of M.Sc(IT-Security) from the University Department of Information Technology, University of Mumbai, Mumbai, India.

**Rohit Mourya** is a student of second year of M.Sc(IT-Cloud Computing) from the University Department of Information Technology, University of Mumbai, Mumbai, India.

**Srivaramangai R** is currently heading the University Department of Information Technology, University of Mumbai, Mumbai, India.