



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

# IJIRSET

International Journal of Innovative Research in  
**SCIENCE | ENGINEERING | TECHNOLOGY**

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 3, March 2023

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

Impact Factor: 8.423

9940 572 462

6381 907 438

[ijirset@gmail.com](mailto:ijirset@gmail.com)

[www.ijirset.com](http://www.ijirset.com)

# A Systematic Review of Encryption and Keylogging for Computer System Security

Gawali Kartik Rakesh, Kshirsagar Prathmesh Dilip, Todkar Omkumar Murlidhar,

Yewale Yash Dattatray, Prof.B.R.Bhatti

Department of Computer Engineering, Shri Chhatrapati Shivajiraje College of Engineering Pune, India

**ABSTRACT:** Encryption encrypt data so that the one with a password or encryption key may access it. Encryption protect data content rather than preventing unlawful data transmission interception or access. Intelligence and security organizations utilize it, as well as personal security software that protects user data Advanced Encryption Standard (AES) is single of the proportional encryption algorithm that allows both parties sender and receiver, to use the similar key to encode and decode statistics.

The suggested a keylogger, sometimes known as keystroke logger, is a program that records or logs the keys you press on your console, usually invisibly so you are uninformed that yours activities are being monitored. Most people only perceive the negative aspects of this software, yet it has legitimate uses as well. Separately from presence used for vengeful purposes such as obtaining information and other private information for vindictive purposes, it can also be used in the office to monitor your employes at home to monitor your children`s activities, and bylaw enforcement to investigate and follow occurrences involving the use of CPUs. The project will be entirely written in Python, with the exception of the pynput module, which is not a common Python module and must be installed. The software we are going to make should keep track of keystrokes and save results of file.

**KEYWORDS:** Python, Keylogger, Encryption, Password, Security.

## I. INTRODUCTION

Keylogging and Encryption provides system security by protecting our data from various threats, cyber-attacks and unethical access. Following is the study and description about keylogging and Encryption.

**1.1 Keylogging:** Software, commonly known as keylogger is a sort of malware that may locate a user`s input from the keyboard in command to retrieve confidential information. As a result, hackers put commercial and personal transactions, online banking, email and chat at danger. The keyboard is the primary target since allows keyloggers to retrieve user input to this system and because it`s the almost current way for peoples to interact with machines. There are to sorts of keylogg on the market. Software and hardware are the two types. Software keylogger are the most mutual and easy to install and do significant damage. Keylogger essentially accomplish two task: steering into the client input stream to capture keystroke and transferring the data to a location (For example log file)

**1.2 Encryption:** it`s a fascinating technology that scrambles data so that its unintelligible by unauthorized parties. The advanced encryption structure stands a specification for the encryption of electronic data. It remainstoo known as Rijndael (its original name ). Encryption is the practice of encrypting messages or crucial information.

In such mode that it can only be delivered by authorized parties. Encryption does not prevent interception by itself, but it does deny the interceptor admittance to the information. Encryption, in simple terms is the procedure of creating a cryptogram text that can only be read by the person who has the decryption key. Advanced Encryption Standard (AES) is one of the Encryption techniques used to safeguard internet data from harmful threats (AES). In general, Symmetric key encryption techniques or public key encoding procedures are used in encryption. Encryption is extensively used

technology for safeguarding data against hackers. The AES algorithm encrypts data using specified structure to offer the highest level of security.

## II. PROPOSED SYSTEM

**2.1 Keylogger:** A keylogger is device that captures keystrokes on a keyboard, either through hardware or software. A keylogger will typically preserve the monitoring results of keyboard keystroke in a log/record/record file. Some keyloggers can even delivered the recording on a regular basis to a certain storage path. The employment of a keylogger might be advantageous or even destructive. Law enforcement surveillance of employe productivity, as well as the search for proof of a crime, are all valid objectives. Bad interests include data theft and passwords. The keystrokes and mouse events will begin to function. It will record every keystrokes that user make on the keyboard, as well as mouse clicks. It will obtain the title of the current window. The following information is also displayed on the screen. Using the keyboard APL, it will capture all keystrokes. As a outcome, without the usersknowledge, the software’s owner will monitor all of the data.

In this software we have two options: save monitored data and send monitored data via Log File. Any choice is available to us. We can save the gathered data in a certain folder at a specific time interval. We can send the collected data to certain log file address at a specific time period. As a outcome3rd parties will take access to user keystrokes and mouse events. Cyber criminals have access to privatematerial such as bank Passwords, pin numbers, and user names in this methods.

### Block Diagram:

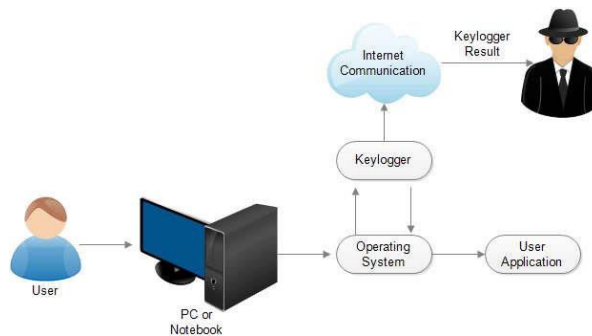


Fig 1:keylogger process in user activity

**2.2 AES Encryption:** AES Encryption is a widely used technology for protecting data from authorized access. The AES algorithm encrypt data using a specified structure to offer the highest level of security. AES is applied in software and hardware to encodedelicate data. It is crucial for administrationCPU safekeeping, cyber security, electronic data guard. The design and strength of key lengths of the AES system (i.e.,128, 192 and 256) are enough to protect confidential information up to the secret level. Top secret info will require use of either the 192 or 256 key distances.

AES has 10 slices for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. The AES encryption algorithm is a symmetrical block cryptograph algorithm with a chunk of 128-bits. Once it encrypt these chunks, it joins them together to form the cipher text. It is based on a substitution- permutation network, likewiseidentified as SP network. It consist of a sequence of connectedactions, including replacing input with specific outputs and others involving bit shuffling.

## III. CONCLUSION

a. The AES encryption algorithm is an extremely strong algorithm for preventing unauthorized access to content. For encryption, it uses a 128-bits fixed data blocks. The AES (Advanced Encryption Standard) algorithm is asymmetric



algorithm. Cryptography refers to the use of the same encryption key for both encryption and decryption. Before transferring the content, the receiver needs have an encryption key, which can be obtained from a safe and reputable source, where plain text is unencrypted content that anybody can access. Encrypted content is represented using cipher text for privacy.

b. Keyloggers are little programmers that operate in the background and capture every keystroke while obstructing normal keyboard operations. In today`s world, one of the most popular way`s to enter data, including credentials, is via the keyboard. Hackers may use them to gate unauthorized access to your personal information, while employers may use them to track employe activity. For information and network security, keyloggers are more useful.

#### REFERENCES

- [1] Singh, G. (2013). A study of Encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications,67(19).
- [2] Nadeem, H (2006). A Performance comparison of data encryption algorithms, “IEEE Information and Communication Technologies,” (pp. 84-89).
- [3] Stallings, W. (2006). Cryptography and network security: principles and practices. Pearson Education India.
- [4] Martin Vuagnoux, S.,P. (2009). Compromising electromagnetic emanations of wired and wireless keyboards. USENEX security symposium, 1-16.
- [5] Thorsten Holz, M.E. (2009). Learning more about the underground economy: a case study of keyloggers and dropzones. Thorsten Holz, Markus Engelberth, Felix C.Freiling, 1-18.





**INNO SPACE**  
SJIF Scientific Journal Impact Factor  
**Impact Factor: 8.118**



**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 **9940 572 462**  **6381 907 438**  **ijirset@gmail.com**



[www.ijirset.com](http://www.ijirset.com)

Scan to save the contact details