ZKG INTERNATIONAL ISSN: 2366-1313

KEYLOGGER INTRUSION AND DETECTION

[1]Mrs. S.Spandana,[2]Mrs.Dr.G.Kalyani,[3]Polapragada. Sai Prerana,[4]Solapur. Ruchitha

[1]Assistant Professor,[2]AssociateProfessor, Dept. of CSE-Cyber Security, Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301,

sspandana.cse@gcet.edu.in,drgkalyani.cse@gcet.edu.in

[3, 4,BTech] Student, Dept. of CSE-Cyber Security,Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301,

polapragada.prerana@gmail.com,solapur.ruchitha63srdt@gmail.com

ABSTRACT:

Keyloggers are a type of computer malware that records keystroke events on the keyboard and saves them to a log file, allowing it to steal sensitive data like passwords. Malicious software captures usernames, PINs, and passwords as a result. Without drawing the user's attention, the hacker Keyloggers possess a big threat to both Transactions such as commercial and personal i.e., E-commerce, online banking, email chatting, and other similar activities are examples of online activities. An attacker can collect valuable data without entering into a strong database or file server using this method. The main purpose of keyloggers is to tamper with the chain of events that occur when a key is pressed, and information is displayed on the screen as a result of the keystroke. Keyloggers can be used for both lawful and illegitimate objectives, depending on the user who is utilizing it. Keyloggers for systems, i.e., for identifying fraudulent users, can be used by system administrators. Keyloggers can help a computer forensics analyst examine digital files more effectively. Keyloggers are extremely useful for keeping track on ongoing criminal activity.

Keywords: Keyloggers, Detection.

I INTRODUCTION

In the contemporary digital geography, where individualities, pots, and governments calculate heavily on computers and connected systems for colorful tasks, the security and sequestration of sensitive

ISSN: 2366-1313

information have come consummate enterprises. Among the multitudinous pitfalls lurking in the digital realm, one of the most insidious and invasive is the keylogger — a stealthy tool used by cybercriminals to cover and record keystrokes on a victim's computer, potentially compromising nonpublic data similar as watchwords, credit card figures, and particular dispatches. The term" keylogger" encompasses a diapason of vicious software and tackle bias designed to covertly capture keyboard inputs without the stoner's knowledge or concurrence. Keyloggers pose a grave trouble to individualities and associations likewise, as they can be stationed for a multitude of unrighteous purposes, including spying, identity theft, fiscal fraud, and commercial spying. Their capability to operate surreptitiously, frequently escaping discovery by traditional security measures, makes them a redoubtable adversary in the ongoing battle for cyber security. Given the inflexibility of the trouble posed by keyloggers, significant attention and coffers have been directed toward both understanding their styles of intrusion and developing effective discovery and mitigation strategies. This multifaceted bid involves a combination of technological invention, cyber security education, legislative measures, and cooperative sweats among assiduity stakeholders to combat this pervasive imminence.

The primary objective of this project includes developing and creating a keylogger to understand the intrusion and threat it causes. The secondary objective is to develop a executable of the primary project which is used majorly by the attackers to mask it on the victim system. The third objective is to use this executable file to understand the keylogger intrusions, integrating different techniques to identify, isolate, and neutralize potential key logging activities within diverse digital environments. The project aims to incorporate antivirus capabilities and utilize Virus Total integration to enhance keylogger detection efficiency. By leveraging both local antivirus solutions and cloud-based Virus Total analysis, the system seeks to fortify cyber security measures, proactively identifying and eradicating keylogger threats. The goal is to safeguard sensitive user information, bolster system integrity, and contribute to comprehensive defense mechanisms against keylogging intrusions in digital ecosystems. The objective of keylogger intrusion and detection is to protect sensitive information from being

ISSN: 2366-1313

stolen by malicious users. Keyloggers can record every keystroke made on a device, potentially capturing sensitive data such as credit card numbers, passwords, and other personal information. By detecting and preventing keylogger intrusions, individuals and organizations can maintain their privacy and security. Keylogger detection involves identifying and removing keylogger software or hardware thathas been installed on a device without authorization. This can be done through various methods, including antivirus software, manual inspection of active processes, and reviewing installed programs. Keylogger prevention involves taking steps to prevent keylogger installation in the first place. This can include using antivirus software, being cautious when clicking links or downloading files, avoiding public devices, and using tools such as firewalls and intrusion detection systems. By focusing on keylogger intrusion and detection, individuals and organizations can better protect themselves from cyber threats and maintain their privacy and security. The objective of keylogger intrusion and detection is to prevent and identify the installation of keyloggers, which are malicious software or hardware that record every keystroke made on a device. Keyloggers can be used to steal sensitive information like credit card numbers, passwords, and other personal data, causing significant harm to individuals and organizations.

II. LITERATURE SURVEY

1. Keylogger for Windows using Python Authors: - Santripti Bhujel1, Mrs. N. Priya2

Keyloggers pose a significant threat to system security and privacy, as they can capture sensitive information such as passwords, user IDs, document contents, credit card details, and other critical data. The paper outlines the intent to observe various types of keyloggers, understand their insertion into systems, analyze current detection techniques, and propose proactive steps to counteract these threats. Key logging program also known as keyloggers is a kind of malware that has capability to maliciously track input of the user from the keyboard in aim to retrieve private information. Keyloggers thus cause a major threat to business and personal activities of kind like transactions, online banking, email and chat. The keyboard is the prime target as it allows keyloggers to retrieve user input to the system as it is the most common way user interacts with a computer. There are two types of keyloggers that exists in market,

ISSN: 2366-1313

a software keylogger and a hardware keylogger among which software keylogger are widely used and are easy to plant and cause substantial damage. Keyloggers essentially performs two tasks that is guiding into client input stream to get keystrokes and moving the information to a distant area (for example- mail). The fundamental goal of keyloggers is to meddle in the chain of occasions that happen when a key is squeezed and when the information is shown on the screen because of a keystroke. Keylogger can be used for legitimate as well as illegitimate purposes, it basically depends on user who is using it. System administrators can use keyloggers for systems, i.e. for detecting suspicious users. Keyloggers can effectively assist a computer forensics analyst in the examination of digital media. Keyloggers are especially effective in monitoring ongoing crimes. Keystroke loggers can be used to capture and compile a record of all typed keys. Keyloggers can at times be utilized as a spying instrument to bargain business and state-possessed organization's information.

2. Survey On Keystroke Logging Attacks
Authors: - Kayak .C, Suganya.R

Malware is the process of disturbing system like collect sensitive data and gain access to systems. Ancient authentication systems want to defend access to on-line services (such as passwords) square measure prone to attack by the introduction of a keystroke faller to the service user's pc. Detecting and preventing malware attack is very important in cyber world as malwares can badly affect computer operation. Once a hacker got access to private user data, he/she can easily make money transfer from user account to untrusted account. The private data can have many consequences which can prove to be more hazards than particular individual's financial loss. We can summarize malware as program intentionally developed for damaging computer specifically those have internet connection. Keyloggers square measure a significant threat to users and therefore the user's information, as they track the keystrokes to intercept passwords and different sensitive data typewritten in through the keyboard. this provides hackers the good thing about accesses the PIN codes and account numbers, passwords to on-line searching sites, email id's, email logins and different hint etc. when the hackers get access to the user's private and sensitive information, they can take advantage of the extracted data to perform online money transaction the user's account. Keyloggers will typically, be used as a spying tool to compromise business and state-owned

ISSN: 2366-1313

company's information. The most objective of keyloggers is to interfere within the chain of events that happen once a secret is ironed and once the information is displayed on the monitor as a result of a keystroke.

3. Real Time Working Of Keylogger Malware Analysis Authors: - Devashree Kataria, Manan Kalpesh Shah, S Bharath Raj, Priya G

The paper highlights the rise of malware, particularly focusing on keyloggers, as a significant concern. Keyloggers, in particular, have become increasingly problematic as most antivirus solutions struggle to detect them effectively, rendering them nearly undetectable. Antivirus software aims to prevent and remove malicious software by identifying and eliminating threats from a device. However, certain types of malwares, such as keyloggers, evade detection, posing a serious threat to user privacy and security. The paper introduces antivirus software as a defense mechanism designed to detect, prevent, and eliminate malicious software from devices. Despite its intended purpose, the focus here is on keyloggers, a specific type of malware that has become a significant concern due to its ability to evade detection by most antivirus solutions, making it extremely challenging to detect and remove them effectively.

III SYSTEM ANALYSIS

EXISTING SYSTEM

The existing systems include large number of varieties keylogger intrusion and detection systems.

Disadvantages

- Limited Detection.
- SystemResource Consumption.
- AdaptabilityofNewer Keyloggers.

PROPOSED SYSTEM

The proposed system that entirely overcomes the problems associated with previous keylogger intrusion and detection is a complex task due to the evolving nature of cyber security threats. Hence our projects proposed system will be our take on keylogger intrusion and detection, using the knowledge of cyber security gained during our engineering.

Advantages

- Real-time Monitoring and Alerts

ISSN: 2366-1313

- Continuous Updates and Patch Management
- Regular Security Audits and Penetration Testing

IV IMPLEMENTATION

Architecture:

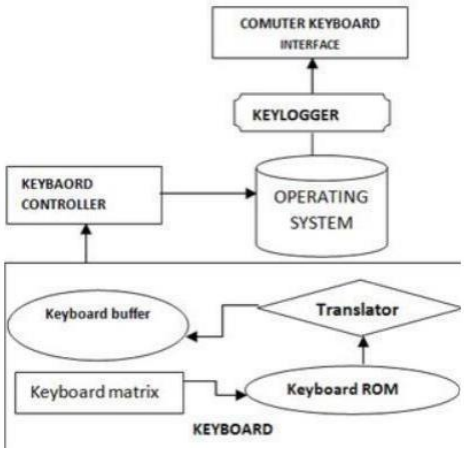


Fig: 1. Architectures of the system model

Keyloggers are hardware or software tools that capture characters sent from the keyboard to an attached computer. They have both lawful/ethical and unlawful/unethical applications. Lawful applications include:

- Quality assurance testers analyzing sources of system errors;
- Developers and analysts studying user interaction with systems
- Employee monitoring and Law enforcement or private investigators looking for evidence of an ongoing crime or inappropriate behavior.

On the other side of the line between lawful and unlawful use, cybercriminals use keylogging technology to capture identities, confidential intellectual property, passwords, and any other marketable information.

Keyloggers fall into four categories: software, hardware, wireless intercept, and acoustic. Although they differ in how they are implemented and how information is captured, these 51 four keystroke logging technologies have one thing in common. They store capture information in a log file. When software or hardware keyloggers are used, the log files are stored on the compromised machine. Remote capture technologies (i.e., wireless intercept and acoustic) typically store keystroke data on the collection device. Software Keyloggers Software keyloggers capture keystroke information as it passes between the computer keyboard interface and the OS. They are implemented as traditional applications or kernel-based. In almost all malicious instances of this type of keylogger, users participated in some way in the software's installation. Keylogging

ISSN: 2366-1313

applications use a hooking mechanism (e.g., SetWindowsHookEx ()) to capture keyboard data. Most kernel-based keyloggers are replacement keyboard device drivers. A portion of the logger resides in the OS kernel and receives data directly from the keyboard interface. A hardware keylogger is essentially a circuit located somewhere between the keyboard and the computer. Devices placed in line with the keyboard cable are the most popular means of deployment. The keylogger is connected directly to the PC and the keyboard to the keylogger. Another method is to install a keylogger circuit into a standard keyboard. This has the advantage of no physical evidence of user monitoring. Laptops present a special challenge. External keyloggers are not an option unless the portable computer never leaves its docking station, and an external keyboard is used. So devices must be installed in the laptop. Figure 6 is an example of a mini-PCI hardware keylogger. the keylogger is connected directly to the PC and the keyboard to the keylogger. Another method is to install a keylogger circuit into a standard keyboard. This has the advantage of no physical evidence of user monitoring. Laptops present a special challenge. External keyloggers are not an option unless the portable computer never leaves its docking station, and an external keyboard is used. So, devices must be installed in the laptop. The advantage of using a hardware keylogger is its invisibility to anti-malware software; although security aware users can easily see them. A disadvantage, at least for non-Bluetooth- accessible devices, is the need for physical access to retrieve information.

Before jumping into the mysteries of keylogging, we should understand how keyboards work and how they interface with systems.

How Keyboards Work:

A keyboard consists of a matrix of circuits overlaid with keys. This matrix of circuits, known as a key matrix, can differ between keyboard manufacturers. See Figure 1. However, the key codes that are sent through the keyboard interface to a specific operating system are always the same.

Fig 2. Keyboard Matrix

ISSN: 2366-1313

When the user presses a key, a circuit closes in the Key Matrix. The Keyboard Processor detects this event and captures the circuit location. Using a table stored in keyboard ROM, the processor translates the circuit location to a character or control code. Control codes are typically CTRL- or ALT-combinations. The keyboard's memory buffer temporarily stores the translated character or control code and then sends it to the computer's keyboard interface. The computer's keyboard controller receives the incoming keyboard data and forwards it to the operating system. A keyboard driver is typically used to manage this part of the process. The operating system processes the keyboard input based on the current state of the OS and applications. A keyboard interfaces with a computer via either a cable or a wireless connection. Common cable connections include the old PS2 standard and today's more common USB connector. A popular wireless connection uses a 27 MHz signal with a range of about six feet. This 50 type of connection is found in Microsoft and Logitech wireless keyboards. For solutions that require greater range, more robust wireless connections are available. These long-range connections can reach about 100.

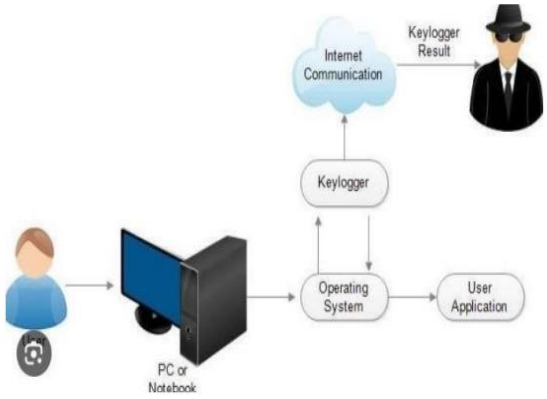


Fig 3: Systemworking

MODULES

1. **Input Module**

- Implementation of a simple Keylogger:
- Capture all the keystrokes

2. **Processing Module**

- Logging the keystrokes bysending it to the email.

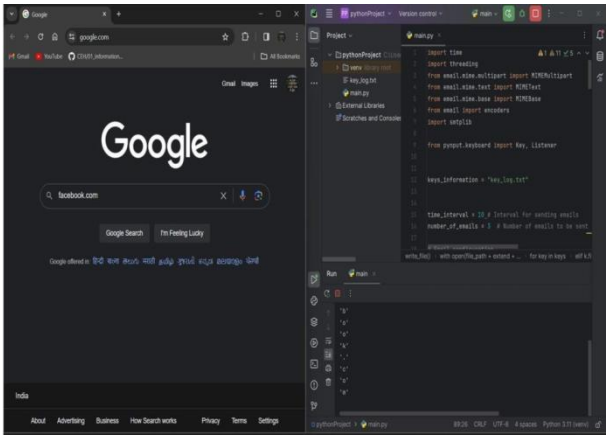
3. **Output Module**

- Detecting the keylogger.

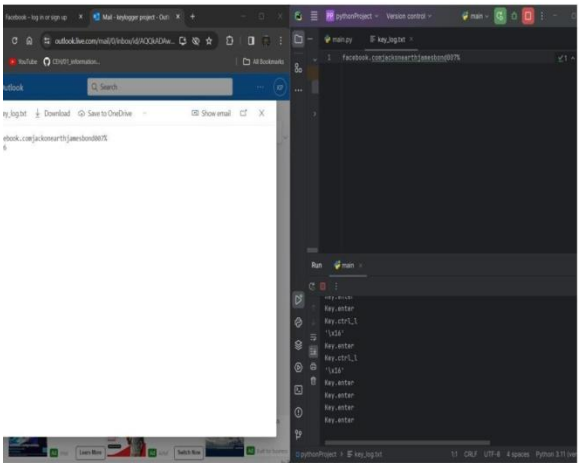
V RESULT AND DISCUSSION

Starting the Keylogger and logging the key

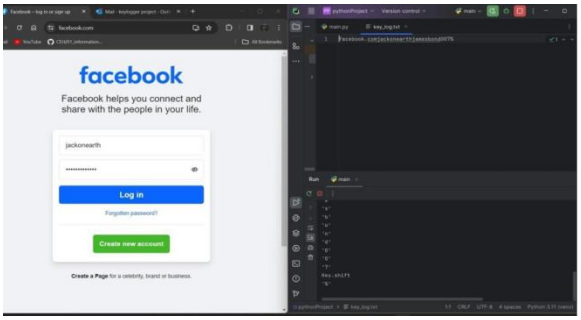
ISSN: 2366-1313



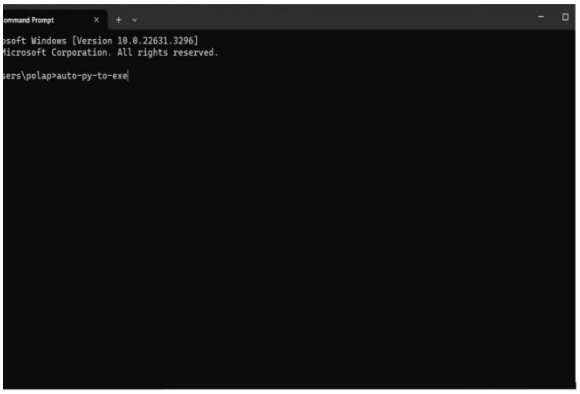
Entering data into the field



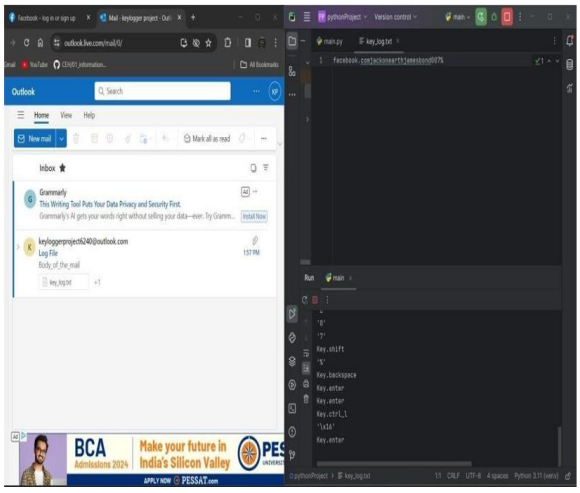
Installing pyinstaller and opening auto-py-to-exe



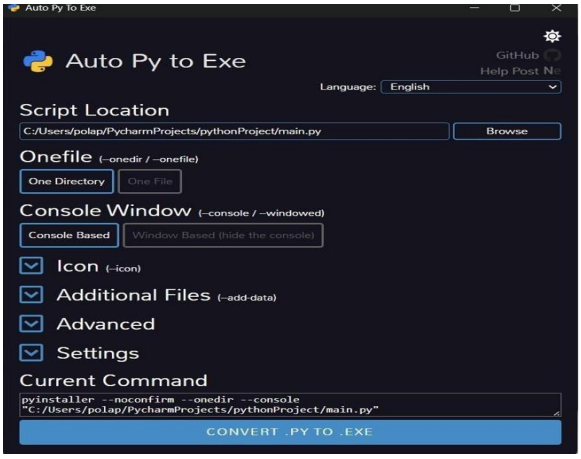
Receiving email ofthe logged Keys



Browsing the python script and converting the executable

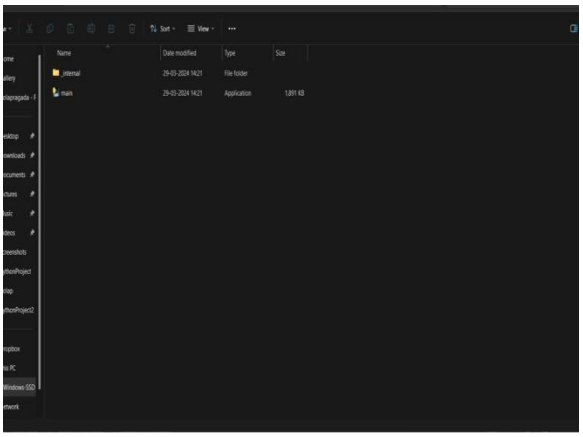


Checking the received log document



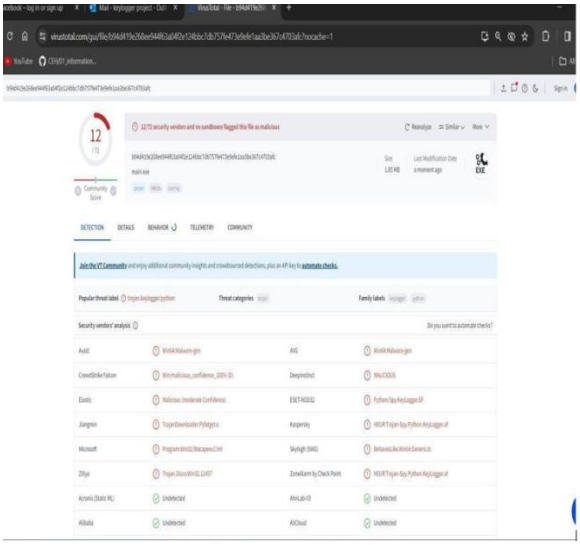
ISSN: 2366-1313

Running the executable



Uploading the executable in virustotal

Virustotal flagging the device as a keylogger



VI CONCLUSION

In conclusion, this project was completely for our understanding of the topic of Keyloggers Intrusion and Detection. The proliferation of keyloggers represents a significant threat to the security and privacy of individuals, businesses, and governments worldwide. Their ability to operate covertly and evade detection poses formidable challenges to cyber security professionals tasked with safeguarding sensitive information in an increasingly interconnected digital ecosystem.

FUTURE ENHANCEMENT

However, through ongoing research, technological innovation, and collaborative efforts across industry sectors, significant strides have been made in understanding keylogger intrusion methods and developing effective detection and mitigation strategies. By leveraging a combination of advanced security technologies, user education, and proactive security practices, organizations can bolster their defenses against keyloggerrelated threats and mitigate the risk of data compromise and financial loss. Nevertheless, vigilance remains paramount in the ongoing battle against this pernicious form of cybercrime.

VII REFERENCES

1. Ahmed, Yahye Abukar, et al. "Survey of Keylogger technologies." International

journal of computer science and telecommunications 5.2 (2014).

2. AISHWARYA, SANKHLA, J. O. H. N. SONIA K, and S. SUMUKH. "The Implementation and Detection of Keyloggers in a System." (2018).
3. Bhardwaj, Akashdeep, and Sam Goundar. "Keyloggers: silent cyber security weapons." Network Security 2020.2 (2020): 14-19.
4. Blåfield, Toni. Different types of keyloggers: Mitigation and risk relevancy in modern society. BS thesis. 2020.
5. Constantin, Lucian. "Attack Campaign Uses Keylogger to Hijack Key Business Email Accounts." PCWorld, 17 Mar. 2016, www.pcworld.com/article/420141/attack-campaign-useskeyloggertohijack-key-business-email-accounts.html.
6. Mallikarajunan, KME Narasima, et al. "Detection of spyware in software using virtual environment." 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI). IEEE, 2019.
7. Tuli, Preeti, and Priyanka Sahu. "System monitoring and security using keylogger." International Journal of Computer Science and Mobile Computing 2.3 (2013): 106-111.
8. Tuscano, Ashley, andThomas ShaneKoshy. "Types of Keyloggers Technologies–Survey." ICCCE 2020. Springer, Singapore, 2021. 11-22.
9. Singh, Arjun, and Pushpa Choudhary. "Keylogger detection and prevention." Journal of Physics: Conference Series. Vol. 2007. No. 1. IOP Publishing, 2021.
10. Prasadu Peddi (2015) "A review of the academic achievement of students utilising large-scale data analysis", ISSN: 2057-5688, Vol 7, Issue 1, pp: 28-35.
11. Rockikz, Abdou. "How to Make a Keylogger in Python." Python Code, 4 Aug. 2019, https://www.thepythoncode.com/article/write-a-keylogger-python.
12. Prasadu Peddi (2015) "A machine learning method intended to predict a student's academic achievement", ISSN: 2366-1313, Vol 1, issue 2, pp:23-37.

AUTHORS

Mrs.S.Spandana, Sr Assistant Professor Dept. of CSE-Cyber Security,Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301.

Email: sspandana.cse@gcet.edu.in

ISSN: 2366-1313

Mrs.Dr.G.Kalyani, AssociateProfessor Dept. of CSE-Cyber Security,Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301.
Email: Soujenya.voggu@gmail.com

Miss.Polapragada. Sai Prerana, Dept. of CSE-Cyber Security, Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301.
Email: polapragada.prerana@gmail.com

Miss. Solapur. Ruchitha, Dept. of CSE-Cyber Security,Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301.
Email: solapur.ruchitha63srdt@gmail.com