IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 14, Issue 5, May 2024, ||Series -1|| PP 37-43

Keyloggers and Data Visualization on Keyloggers: rootkit malware

Jarajana Ravikumar[1], G Rajasekharam[2], Ch. Kodanda Ramu[3]
[1]*M.Tech Scholar(CSE) in Department of Computer Science and Engineering,*
[2]*Associate Professor, Head of the Department, Department of Computer Science and Engineering,*
[3]*Associate Professor, Miracle educational society group of institutions, Miracle City, Bhogapuram, Vizianagaram, India*

Abstract: compared to past generations, modern civilization is much more reliant on electronics. This dependence has benefits and drawbacks. Although there are several advantages, one disadvantage being susceptible to rogue software can quickly overshadow them all. One such spyware is a keylogger. Previously, the main focus was merely on recording a user's keystrokes, but today they are renowned for adding a wide range of functionality. Keyloggers are a type of rootkit malware. These keyloggers are used to steal private information secretly, and because they operate entirely in stealth mode, it is difficult to identify them. Keyloggers are used in everything from Microsoft products to the computers and servers used by your workplace. In rare circumstances, your mate may have installed a keylogger on your laptop or phone to support their accusations of adultery. The keylogger can capture all actions associated with the emphasis placed on console keys or movement of the working environment. One of the main causes of the keyloggers' explosive development is that programs operating in user space can track every keystroke that a system's users' type. Keyloggers represent a serious risk to both personal and professional activities such online banking, email communication, and system database. A password is a phrase or word that is used to protect access to a website. An application, a network, documents, and data on a computer system can all be accessed with a password. A password should typically be comprised of something challenging to decipher so that it may be kept private. We can use our keylogger tool to approve that password.

Index Terms – Keylogger, stealth, Keystroke, System, E-mail.

I. INTRODUCTION

The internet's forerunner, Arpanet, celebrated its 50th birthday in 2019. From 1969, there have been over 4 billion internet users, and there are far more devices connected to IP addresses than there are people. Internet usage is increasing tremendously, but so are the security risks. One of the main causes of security breaches is still installing malicious software over the internet. Malware, also referred to as malicious software, is a program that aims to carry out unwanted and disorderly actions in a computer system without the user's consent. Malware encompasses items like viruses, worms, Trojan horses, keyloggers, and spyware, among others. All of these malwares have been and still are a serious hazard to everyone in the world. Keyloggers are the main topic of discussion in this exposition. Keyloggers are the main topic of discussion in this exposition. They are installed on a device with the specific intent of tracking the user. In the past, keyloggers were just used to record keystrokes and communicate them to the attacker, but as technology has improved, keyloggers have added a variety of new features, including the ability to activate the microphone and webcam and take screenshots, etc. Keyloggers can be used for both legal and illegal objectives [1].

Because of their stealth nature, keyloggers are becoming more prevalent. They operate in stealth mode, making them difficult for antivirus software to identify. Keyloggers can be avoided, nevertheless, by taking certain precautions. Applications for prevention, such as firewalls and anti-malware, must be downloaded. Updating security fixes on a regular basis. The use of licensed software and the downloading of applications from reliable sources are both required. Checking the CPU and RAM use of the computer on a regular basis is another simple method for finding undesirable software. Python is used to write the keylogger's proposed algorithm. The functionality for screen capture is included, along with tools for obtaining computer information, clipboard contents, turning on the microphone, and gathering Chrome data. The information is gathered, forwarded to the attacker through email, and is completely undetectable. These keyloggers also are for legitimate purposes like parental monitoring, forensic etc. are described in Table 1.

TABLE 1

Legitimate	**Illegitimate**
1. IT troubleshooting	1. Stalk a non-consenting person
2. Computer product development	2. Steal a spouse’s online account info
3. Business server monitoring	3. Intercept and steal personal info
4. Employee surveillance	
5. Parental supervision of kids	
6. Tracking of a spouse	

II. RELATED WORK

Here, are few significant studies are presented to emphasize the importance of key loggers for system monitoring. Keyloggers have existed since the middle of the 1970s. The "Selectric bug" was a typewriter-targeting programme developed by the Soviet Union. Keyloggers have greatly improved since then. In the past ten years, improvements have been seen in both efficiency and usability. Keyloggers, as the name suggests, can only provide information if keystrokes are recorded. A huge problem was brought about with the 2012 introduction of Windows 8 with a touchpad personalized keyboard. S. Moses investigates how keyloggers can record inputs from a virtual keyboard in " Keylogging malware and the Touch Interfaces." Additionally, examples of how different keyloggers react to it are provided. A. Bhardwaj suggests in that the keyloggers should be classified according to two factors: the execution location and the functions provided. Additionally, the keylogger can be software- or hardware-based.

The detection of keyloggers is another area that is developing as new keyloggers are being released. E. Ladakis proposed a sneaky keylogger with such a revolutionary technique in 2013, looking into the world of graphics processors as an alternative for hosting an environment for the keylogger to operate. Since smart phones have already become a necessity in our life, banking services are now available through smartphone platforms. Because it makes the financial procedure simple, users are growing more at ease with the application. A. Kuncoro draws attention to the security risks that these mobile applications with key loggers provide in. analyses security software.

III. WHAT ARE KEYLOGGERS

Keyloggers are a type of software or hardware device that records and tracks all keystrokes made on a computer or mobile device. While tracking a user's keyboard activity is the main goal of keyloggers, they increasingly have capabilities that go beyond that. They can watch practically everything that runs on a computer. Some keyloggers, also referred to as "screen scrapers," enable visual tracking of a target machine by periodically collecting screenshots of the screen. The collected photos can then be used to gather insightful data about the user. Advanced keyloggers can keep an eye on activities like Internet access, file functions, cut, copy and paste. Keyloggers are frequently used to monitor user behavior and record information like personally identifying information and other confidential or delicate data. Keyloggers are different from other types of adware or spyware, including Trojan horses and worms. These are cautiously and accurately created to perform their jobs without drawing the attention of users, sharing available resources with allowed applications, remain unnoticed also on computer for required period of time, and without interfering with users' normal activities. Despite organizations having anti-virus software, anti-spyware, and firewalls, examples of business spyware relying on keystrokes tracking have also shown a significant rise [2].

The development of keylogger incidents was highlighted in the 2006 Websense Web@ Work Report. Keyloggers monitor a wide range of computer-based activities. Keyloggers record and transmit victim keystrokes and other operating system actions to locally or globally available CDs. Most of the time, keyloggers transmit the intruders the keystroke records. Software keyloggers monitor systems in the targeted operating system that record keystroke information, store it on a disk drive or in remote spot, and transfer it to the hacker who put the keylogger there. Commercial software keyloggers are widely available over the Internet, whereas hackers either make or employ parasite keyloggers.

Keyloggers have been used in various actual life instances. Keyloggers for gadgets may be tracked using both Windows and operating system-specific methods. A Microsoft text called WM KEYDOWN is generated whenever a user presses a key on the WOS by the OS system's key driver. This text is moved in the automated message queue. The WOS will then add this message to the thread's message queue for the application that is connected to the computer's active window [3]. The threads that check this queue send the message to the session function of the active window. There are four basic approaches for creating keylogger systems: Keyboard State Table, Windows Keyboard Hook, Kernel-Based Keyboard Filter Driver, and Innovative. Keyloggers for computers offer the following features:

A. Any keystroke made by the user; Mouse (clicks and motions).
B. Titles of opened or centered windows.
C. regular or in response to an incident, screenshots of screens.
D. Utilization statistics and running programmes.
E. Internet usage (pages viewed and time spent on each page).
F. File system operations (create, rename, change, access, and delete), and file system operations.
G. Emails delivered, returned, and even unread.

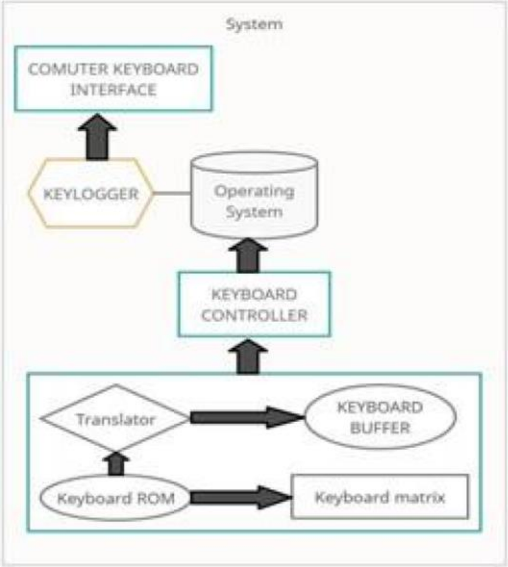


Figure 1: Block diagram of Keylogger working

IV. KEYLOGGER IN FUNCTION

Keyloggers can be used for a variety of requirements by multiple users, including the departments of government, military, and law enforcement organizations, information security professionals, staff members, managers, guardians, educators, and spouses. The most of keyloggers are utilized for unlawful purposes including identity theft and the collecting of private information. Intrusion detection, police forensic investigations, parental supervision, workplace surveillance and monitoring, and catastrophe recovery are just a few examples of acceptable uses. Some functions are described in table no. 2 below [4].

TABLE 2

Functions	Description
Keystroke Logging	Records individual keystrokes on the keyboard.
Stealth Operation	Operates discreetly to avoid user detection.
Data Encryption	Secures logged data using encryption methods.
Remote Delivery	Can be installed and controlled remotely.
Bypassing Security	Evades detection by antivirus software.
Log File Management	Organizes and manages log files efficiently.
Exfiltration	Transfers logged data to external locations.

Throughout this article, we'll demonstrate how keyloggers are used and how they pose a major risk to PCs. Keylogging and keyboard capture are other names for keystroke logging. This could involve writing down keystrokes on a keyboard. It's usually performed secretly to make sure that the user or anyone using the keyboard, is unaware that their actions are being watched. The person running the logging programme can then obtain data.

V. PROPOSED METHODALOGY

The proposed methodology in this research is programmed in the Python language. The software is intended only for one victim, not for many. A victim may receive the malware via email or by employing additional hardware, such as a pen drive or hard drive. The following features are included:

- Every keypress, even those using special characters, will be recorded.
- Access to the clipboard of the victims.
- Images of the victims' screens.
- Use of the microphone.
- Computer details: RAM and OS.
- IP and MAC addresses for the network.
- Information gathering for Chrome history.
- The files are automatically removed from the user's PC when the information [5].

The files are automatically removed from the user's PC when the information is collected and provided through email to the attacker system. Functional Prerequisites:

- SMTP servers
- Email storage
- Internet access

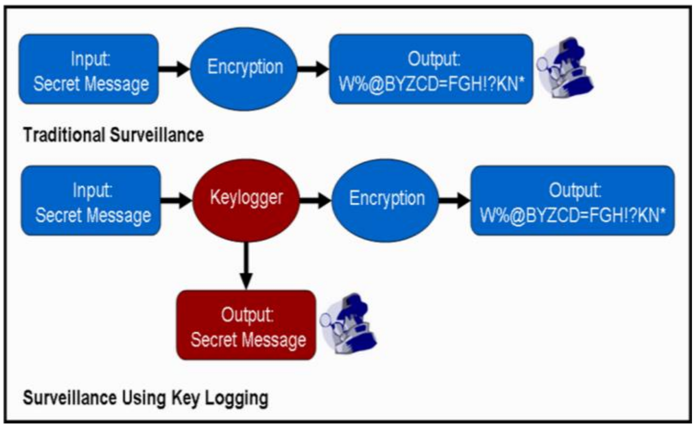


***Figure 2:** Keylogger methodology*

Malicious applications known as software keyloggers are launched on a desktop or smartphone to record every keystroke made there. A broad description of the how software keyloggers operate is provided below:

- Delivery: The keylogger is sent to the target computer by the assailant. This may be accomplished via a variety of techniques, including corrupted downloads, email attachments, or direct physical connection to the device.

- Installation: The keylogger must be set up on the target machine when it is supplied. The attacker may mislead the victim into deploying the keylogger through social engineering techniques, or they may utilize a system vulnerability to install it regardless of the victim's awareness.
- Persistence: The keylogger must be set up to launch automatically at system startup and remain active in the background. This allows a keylogger to monitor the keystrokes in stealth mode.

- Keystroke recording: Once activated, the keylogger starts to record every keystroke performed here on system, containing username, credentials, credit card details, and other sensitive data. Other information could also be recorded, such contents of the clipboard and website visits.

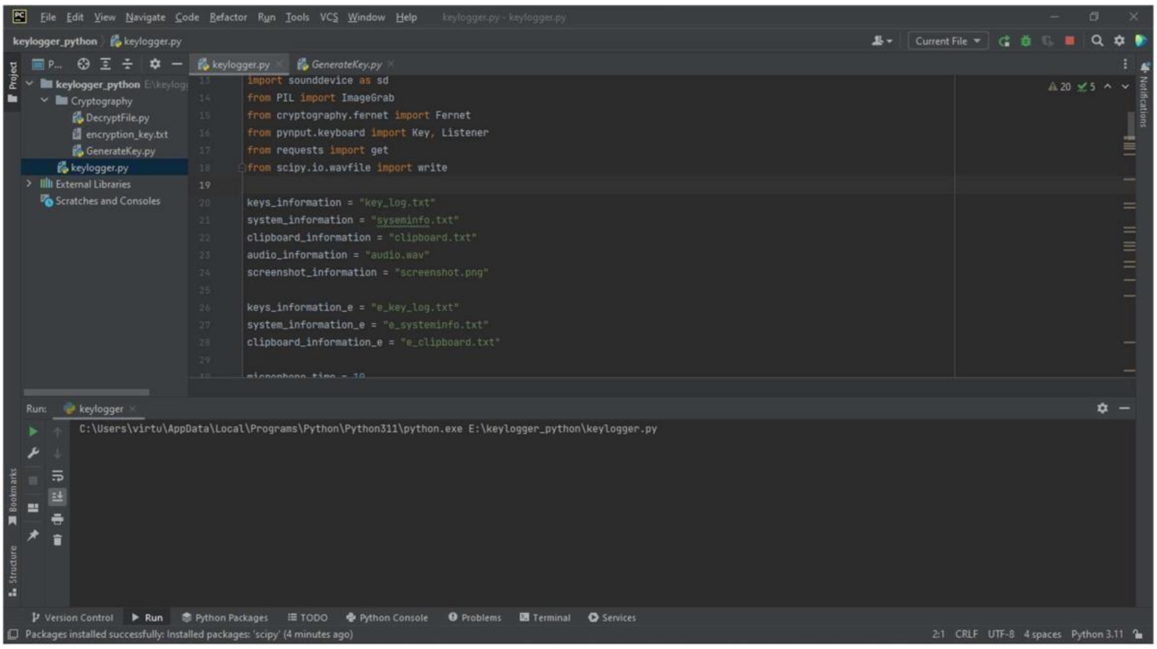
- Data transfer information: The recorded information is usually transferred to a remote host under the attacker's control. Several techniques, including email, FTP, and employing a command and controlling (C&C) servers to receive the data, can be used to do this.

- Covering tracks: The assailant may take action to hide their footprints and prevent being discovered. This can be done by erasing the keylogger out from system, encrypting the data that was stolen, or erasing the keylogger's activity records remotely.

Install anti-malware programs, keep your system updated with security updates, and exercise caution while viewing e - mail attachments or installing software from dubious sources to prevent falling prey to a software keylogger assault. Even if an attacker can install a keylogger onto your device, employing two-factor verification and strong authentication can make it more challenging for them to collect your login information [6].

VI. TESTING AND ANALYSIS

In this experiment, the attacker executes the code (shown in figure 2) to get the information from the victim system which is recorded by the keylogger in stealth mode without the user knowledge, the information is transmitted to the attacker system at certain amount of time as we have set 60 seconds in the execution code, the keyloggers will be transferring the collected information to the attacker system through email every 60 seconds in stealth mode.



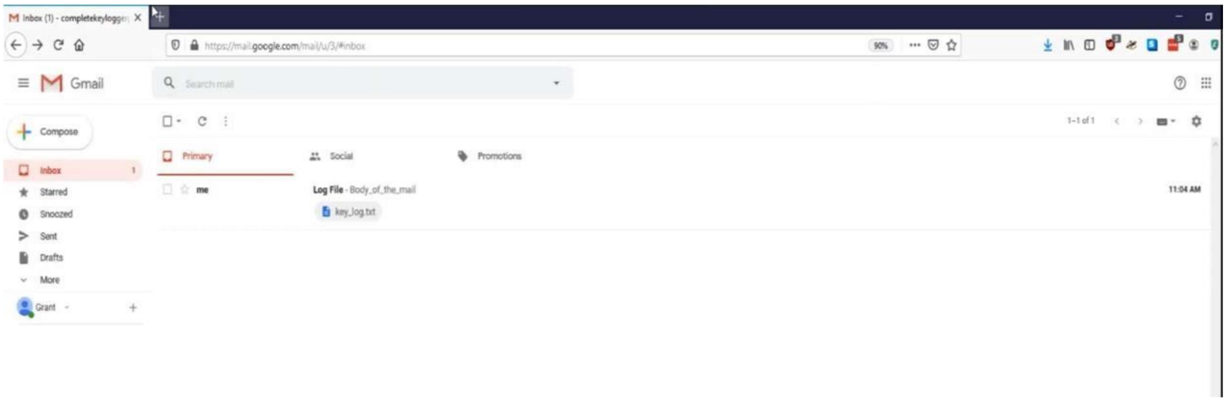
```
import sounddevice as sd
from PIL import ImageGrab
from cryptography.fernet import Fernet
from pynput.keyboard import Key, Listener
from requests import get
from scipy.io.wavfile import write

keys_information = "key_log.txt"
system_information = "syseminfo.txt"
clipboard_information = "clipboard.txt"
audio_information = "audio.wav"
screenshot_information = "screenshot.png"

keys_information_e = "e_key_log.txt"
system_information_e = "e_systeminfo.txt"
clipboard_information_e = "e_clipboard.txt"

microphone_time = 10
```

```
C:\Users\virtu\AppData\Local\Programs\Python\Python311\python.exe E:\keylogger_python\keylogger.py
```

Packages installed successfully: Installed packages: 'scipy' (4 minutes ago)

Figure 3: Keylogger code execution

We can see that as soon as the user begins entering their information on the Facebook signup screen, every keystroke they make is logged. Once a certain time has passed, a mail with keystrokes and mail attachments is sent. This presents a risk since the password that the user types are easily visible to the attacker [7].



me Log File - Body_of_the_mail 11:04 AM
key_log.txt

Figure 4: Email sent by the keylogger.

VII.MEASURES FOR SOFTWARE SECURITY

Keylogger detection procedures are required to secure organizational or individual personal data. Internet users ought to be able to recognize the existence of installed keyloggers on their devices, a few illustrations of wide metrics:

a. Antivirus, antispyware, anti-keylogger, and anti-virus software alerts
b. A few keys don't function correctly.
c. A character doesn't immediately show up on the screen once a key is tapped.
d. Not all button presses are successful.
e. Drag-and-drop actions as well as double clicks behave strangely [8].

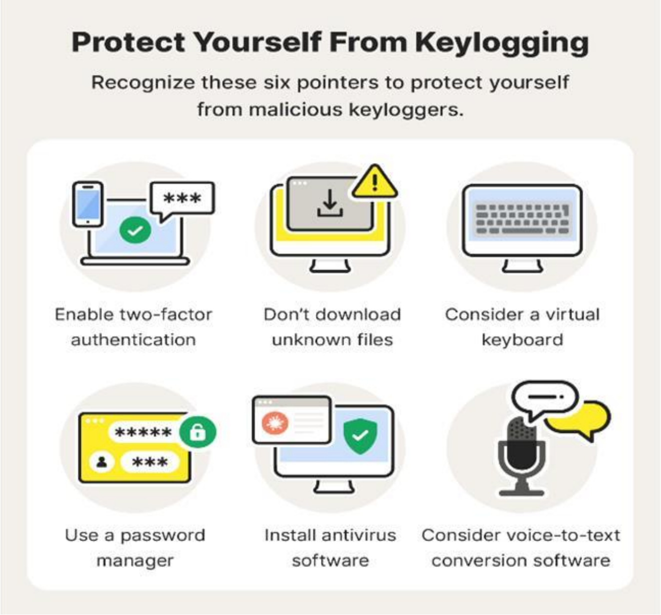

Protect Yourself From Keylogging
Recognize these six pointers to protect yourself from malicious keyloggers.
***
Enable two-factor authentication
Don't download unknown files
Consider a virtual keyboard
*****
***
Use a password manager
Install antivirus software
Consider voice-to-text conversion software

Figure 5: Prevention against Keyloggers

When any of these symptoms appear, however after rebooting a machine, it is likely a keylogger is still present in the OS. When typing in personal information via a keyboard, users should constantly be aware of keylogger dangers. Digital keyboards are utilized to input personal details into apps like online banking and shopping, however they do not completely safeguard users' private information. It ought to be disregarded that some very advanced keyloggers could take snapshots to reveal private information depending on click of the mouse. The following actions might be conducted in addition:

- Be cautious whenever using the device.
- Don't ever leave people unattended with your machine.
- Be always aware of keylogger signals and surveillance system activity.
- Use the phone's keyboard.
- Keep your software upgrades current.
- Download software only from reliable websites [9].

VIII. CONCLUSION

An effective tool for keeping an eye on user behavior on devices like computers and smartphones is a keylogger, to sum up. It can assist firms in safeguarding confidential data and ensuring that staff members are abiding by protocol. People can use keyloggers to keep an eye on their behavior or the behavior of others at their homes or places of employment. However, it's crucial to keep in mind that keylogging should only ever be done lawfully and ethically since doing so might have major repercussions. Keyloggers are useful instruments that may be used for a variety of applications. Although certain keylogger algorithms are legal, many (perhaps even most) keyloggers are utilized unlawfully. Keylogger exploits are not prevented by standard device interaction safety procedures on computer systems. Human-to-machine interactions must be considered to prevent keylogger invasions. It is anticipated that keylogger dangers will increase with time. Users need to be aware of this significant danger when using computers and take precautions to avoid it. Sadly, despite the existence of papers, material, and sites concerning keyloggers, there is insufficient information, particularly regarding new risks. The most effective strategy to lower security risks is to use a comprehensive security solution that protects against a wide range of threats [10].

REFERENCES

[1]. Y. Balakrishnan and R. P N, “An analysis on Keylogger Attack and Detection based on Machine Learning,” 2023.

[2]. Dave, “How Keyloggers Work and How to Defeat Them”, IEEE Access, 2021. **[3]** https://www.researchgate.net/publication/267777154_Malware_Analysis.

[3]. Rai, S., Choubey, V., Suryansh, & Garg, P. (2022). A Systematic Review of Encryption and Keylogging for Computer System Security. Proceedings - 2022 5th International Conference on Computational Intelligence and Communication Technologies, CCICT 2022, July, 157–163.

[4]. Disha H. Parekh, Nehal Adhvaryu, Vishal Dahiya (2020). Keystroke Logging: Integrating Natural Language Processing Technique to Analyse Log Data. International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue- 3, January 2020.

[5]. 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.

[6]. Tuscano, Ashley, and Thomas Shane Koshy. "Types of Keyloggers Technologies–Survey." ICCCE 2020. Springer, Singapore, 2021. 11-22.

[7]. Singh, Arjun, and Pushpa Choudhary. "Keylogger detection and prevention." Journal of Physics: Conference Series. Vol. 2007. No. IOP Publishing, 2021.

[8]. Tove, M. (2022). What Are Keyloggers and How Can You Protect Yourself?

[9]. https://iopscience.iop.org/article/10.1088/1742- 6596/2007/1/012005/pdf

Authors

JARAJANA RAVIKUMAR Holds a B.Tech Degree in Computer Science & Engineering from Aditya Institute of Technology & Management,Tekkali,Srikakulam. He presently Pursuing **M.Tech (CSE)** in Department of Computer Science and Engineering from Miracle Educational Society group of Institutions,Visakhapatnam. Area of interest include Python,Compiler Design,Cryptography,FLAT,Web Technologies, Web Programming .

G Rajasekharam is working as Associate Professor, Head of the Department, Department of Computer Science and Engineering, Miracle educational society group of institutions, Miracle City, Bhogapuram, Vizianagaram, India.

Ch. Kodanda Ramu, M. Tech, (Ph.D) is working as Associate Professor, Department of Computer Science and Engineering, Miracle educational society group of institutions, Miracle City, Bhogapuram, Vizianagaram, India.