Global Scientific JOURNALS

GSJ: Volume 9, Issue 4, April 2021, Online: ISSN 2320-9186
www.globalscientificjournal.com

WAYS OF COMBATING RANSOMWARE ATTACK IN THIS GLOBAL VILLAGE USING PREEMPTIVE APPROACH.

Ifeose Justin N.
Department of Computer Science
Delta State Polytechnic Ozoro
Delta State, Nigeria

Ike Mgbeafulike
Department of Computer Science
Chukwuemeka Odumegwu Ojukwu University
Uli
Anambra State, Nigeria

Key words: Ransomware, Phishing, Cryptovirology, Ransom, Bitcoin, Cryptoviral Extortion, Cryptocurrency.

Abstract

The world recently has been faced with different magnitude of attacks by ransomware malware increasingly by the day. This has rendered both individuals and organizations incapacitated, majorly in the field of computer and information technology. There is no infallible solution for protecting against ransomware as the malware code uses metamorphic and polymorphic algorithms to generate different versions, thereby evading signature detection. Ransomware also uses domain generator algorithms (DGA) to generate new domains for the command and control server (C&C), they constantly exploit new vulnerabilities; hence, for an individual or organization to protect itself, an adaptive security architecture is required for constant monitoring of the system to detect new ransomware infection at an early stage and blocked it before encryption of the files are done. This approach is a defense in depth approach that supplements the network defenses such as patch management, antivirus software, intrusion detection, firewalls, and content filtering. A framework for implementing the preempt and preventive security architecture model using open source software is presented, and the proposed framework is tested against the WannaCry and Petya Ransomware. The proposed framework was successfully able to alert of the ransomware attack and, it was even possible to prevent the ransomware from executing on the victim host.

1.0 INTRODUCTION

Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system so that it is not difficult for a knowledgeable person to reverse, more advanced Malware uses a technique called cryptoviral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. In a properly implemented cryptoviral extortion attack, recovering the files without the decryption key is an intractable problem, and difficult to trace digital currencies such as Ukash and Cryptocurrency are used for the ransoms, making tracing and prosecuting the perpetrators difficult. (Mimoso, 2016).

Ransomware is a subset of Malware in which the data on a victim's computer is locked -- typically by encryption, and payment is demanded before the ransomed data is decrypted and access is returned to the victim. The motive for ransomware attacks is usually monetary, and, unlike other types of attacks, the victim is usually notified that an exploit has occurred and is given instructions on how to recover from the attack. Payment is often demanded in a virtual currency, such as Bitcoin, to not know the cybercriminal's identity. (Lutkevich et al., 2019)

Lutkevich et al. (2019) add that ransomware malware can be spread through malicious email attachments, infected software apps, infected external storage devices, and compromised websites. Attackers have also used remote desktop protocol and other approaches that do not rely on any form of user interaction.

Lutkevich et al. (2019) reveal that ransomware kits on the deep web have allowed cybercriminals to purchase and use software tools to create ransomware with specific capabilities. They can then generate this Malware for their distribution, with ransoms paid to their Bitcoin accounts. As with much of the rest of the IT world, it is now possible for those with little or no technical background to order inexpensive ransomware as a service (RaaS) and launch attacks with minimal effort. In one RaaS scenario, the provider collects the ransom payments and takes a percentage before distributing the proceeds to the service user.

Lutkevich et al. (2019) assert that encryption ransomware is one of the most effective forms of ransomware today. As mentioned above, an attacker gains access to and encrypts the victim's data, asking for ransom payment to unlock the files. Attackers use complex encryption algorithms to encrypt all data saved on the device. A note is usually left on the inflicted system with information about retrieving the encrypted data after payment. Compared to screen lockers, encryption ransomware puts the victim's data in more immediate danger, and there is no guarantee of the data returning to the victim after negotiation. In both cases, the victim may receive a pop-up message or email ransom note warning that if the demanded sum is not paid by a specific date, the private key required to unlock the device or decrypt files will be destroyed.

1.1 STATEMENT OF THE PROBLEM

The damages caused by ransomware Malware to computer users around the globe can be very disturbing. The challenges faced by users whose systems are under attack from such Malware is mentioned below:-

Loss of money: Huge sums of money are paid to the developers of the ransomware software by desperate computer users who need to have their data recovered

Time Waste: Projects files stored on a workplace computer system that have been compromised are usually lost to this attack, and a lot of time is wasted in redoing the file again.

System Damage: The process of encrypting the files by the ransomware uses system resources that may overload it and cause dame to the operating system.

Update Failure: Antivirus failure to update will render them unable to detect the ransomware virus when they begin to attack the computer system.

Loss of data: Valuable data is lost to the ransomware as it encrypts the most commonly used files used by the computer user.

Hard Drive Damage: The creation of multiple encryption files on the system hard drive will lead to the hard disk's corruption, causing damage to the unit and preventing smooth storage of files.

1.2 OBJECTIVES OF THE STUDY

This research aimed to develop an Anti-malware Model for the Protection of the Computer System from File Encryption associated Ransomware. After the completion of this research work, the following will be achieved:

i. To identify users' problems when attacked by ransomware with a bid to develop a system to curtail it.

ii. Develop a system that will scan the Hard Disk drive of PC files and store information on their access data.

iii. To create a system that will monitor the files stored on the Hard Disk and check for any change in their properties such as file access date, file name, file size, and file existence on the hard disc drive.

iv. To report any detected activity on any file to the system users, which could be as a result of ransomware encrypting the files.

v. To prevent any further action of the suspected ransomware in order to protect the files in the system.

vi. To test the system to ensure that it achieves the set-out aim of the research.

1.3 OPERATIONAL MODE OF RANSOMWARE

According to Johansen (2019), The idea behind ransomware, a form of malicious software, is simple: Lock and encrypt a victim’s computer or device data, then demand a ransom to restore access.

In most cases, the victim must pay the cybercriminal within a set amount of time or risk losing access forever. And since malware attacks are often deployed by cyber thieves, paying the ransom doesn't ensure access will be restored. Ransomware holds your personal files hostage, keeping you from your documents, photos, and financial information. Those files are still on your computer, but the Malware has encrypted your device, making the data stored on your computer or mobile device inaccessible. While the idea behind ransomware may be simple, fighting back when you're the victim of a malicious ransomware attack can be more complex. And if the attackers do not give you the decryption key, you may be unable to regain access to your data or device. Knowing the types of ransomware out there, along with some of the dos and don'ts surrounding these attacks, can go a long way toward helping protect yourself from becoming a victim of Ransomware (Johansen, 2019)

According to Barak (2017), most ransomware is delivered via email that appears to be legitimate, enticing you to click a link or download an attachment that delivers the malicious software. Ransomware is also delivered via drive-by-download attacks on compromised or malicious websites. Some ransomware attacks have even been sent using social media messaging. Generic ransomware is rarely individually targeted, but rather a “shotgun” approach where attackers acquire lists of emails or compromised websites and blast out ransomware.

Given the number of attackers out there, it will be likely that if you get hit multiple times, it will be by a different attacker.

Whether or not the ransom is paid, keep in mind that attackers will always try extracting useful data from a compromised machine. Assume all sensitive data on the machine was compromised, which could include usernames & passwords for internal or web resources, payment information, email addresses of contacts, and more (Barak, 2017)

2.0 REVIEW OF RELATED WORKS

Malone et al. (2011), in *Hardware Performance Counters a Cost-Effective Way for Integrity Checking of Programs,* proposed using hardware performance counters to detect malicious program modifications at load time and runtime by acting as dynamic integrity checkers. The main benefit of this is that it incurs almost no hardware cost since they are built into most processors. The authors claim that hardware performance counters are very efficient at detecting program modifications. The biggest limitation to the research in (Malone et al., 2011) is that they tested their approach on programs running solo instead of in a dynamic environment where multiple programs are running simultaneously. Also, this only serves to protect benign programs and does nothing to detect standalone Malware, Given that ransomware is generally standalone. Demme et al. (2013), in 'On the Feasibility of Online Malware Detection with Performance Counter', proposed that this approach would require significant modification before it could expand its capabilities. (Tang et al., 2014). continue previous works on hardware performance counters and use them to detect anomaly-based Malware by looking at micro-architectural execution patterns. The author's approach goes beyond that of recent works in behavior-based malware detection to detect a much wider range of Malware to include zero-day by using machine learning to establish a baseline of benign program executions and use them to detect deviations, and the detector can be used in complement to existing signature-based detections.

Because the approach of using hardware performance counters for malware detection is a relatively new idea, it is still far from production-ready. It is prone to a high false-positive rate, and it also requires baselines for every individual program on a computer to detect anomalies in the benign programs themselves in the event they are exploited or are under attack. This does not do much for standalone malware detection.

The feasibility of building a malware detector in hardware using data from existing hardware performance counters is examined by (Demme et al., 2013). In this paper, the authors find that they can detect multiple variations of Malware within families with ease given a small control set. They also propose modifications in hardware that allow the malware detector to run smoothly beneath the system software, which is a great improvement and fewer buggies than existing software-based antivirus solutions. When used in combination with software-based antivirus, the authors claim that their approach advances state-of-the-art in online malware detection. This paper provides a lot of solid insight and can serve as a foundation for many future works. As with anyone who develops malware-fighting solutions, the author's voice concern over the potential for malware authors to once again adapt their programs to combat even hardware-based approaches such as the one discussed in their paper, but on the other hand, it is good to see the hardware community finally join the fight against Malware because it forces malware authors to step into a new arena in which they lose the advantage they have had over the anti-malware developers in the software arena since Brain was first discovered.

Kharraz et al. (2015), in Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attack*s*, view the evolution of ransomware in the wild from 2006-2014 and determine that the sophisticated destructive capabilities of most ransomware families lack growth despite the improvements of encryption, deletion and communications techniques in general. They insist that stopping advanced ransomware attacks is not as complex as commonly believed and that defenses involving file system monitoring can be practical and effective because ransomware generates file system requests much differently than benign programs. While the file system monitoring approach is indeed practical, as evidenced by my own research, it alone is not enough due to the overwhelming percentage of ransomware samples analyzed by the authors that produced some amount of data loss before being detected. Other than that, their analysis of the destructiveness of ransomware is thorough and was very useful in developing my approach to combating ransomware.

Kharraz et al.(2016) take this work even further in ‘A Large-Scale, Automated Approach to Detecting Ransomware ‘ by focusing on the difference between ransomware and other existing families of Malware. In the malware arena, ransomware stands alone compared to all the rest, which is why nearly all generic malware detection systems are losing the fight against ransomware. The authors create a dynamic analysis system called UNVEIL, which is designed to detect ransomware specifically and is to be used in combination with other malware detection systems. UNVEIL essentially generates a honeypot environment and detects ransomware as soon as it interacts with the user's data. UNVEIL also monitors the desktop to detect any ransomware-like behavior, such as a lock screen preventing the user from accessing their files. The authors boast that UNVEIL significantly improves upon state of the art by demonstrating its capability to identify known evasive ransomware currently immune to detection by existing antivirus systems. This paper really improves upon state of the art given a zero false-positive rate from over 13,000 samples and detects superficial and sophisticated and zero-day ransomware attacks. One limitation of the paper is ransomware's potential to detect the artificially generated environment to avoid it. While it certainly raises the bar of difficulty for the ransomware author to circumvent, it is not infeasible. The other limitation is that most ransomware samples still incur some amount of data loss before detection.

In ‘PayBreak: Defense against Cryptographic Ransomware, ′ Kolodenker et al. (2017) proposed a new system, PayBreak, to combat ransomware and prevent any data loss effectively. It does this by essentially creating a key escrow inaccessible to ransomware that holds every key securely used in encryption, allowing the decryption of any files encrypted by ransomware. PayBreak demonstrates the ability to restore all files lost to twelve different ransomware families, and it does so with negligible performance overhead. While complete data recovery or complete prevention of data loss is the ideal result of combating Ransomware, PayBreak only manages to effectively work with only 60% of all ransomware families, leaving eight common families of ransomware that can decimate a user’s system to go uninhibited. PayBreak also lacks basic robustness allowing it to be evaded simply by ransomware authors rolling back to older versions of crypto libraries or through basic obfuscation and evasion techniques, as stated by the authors themselves. Their approach was essentially just a proof-of-concept, and it is uncertain whether the authors will pursue any future work on PayBreak or not.

3.0 PROPOSED SYSTEM AND IMPLEMENTATION

This system is designed specifically for the detection of ransomware activities on the system. It will be used to monitor changes in the files of any selected folder in order to detect if any sudden change in the file properties occurs, which could signal that the files are being encrypted.

3.1.1 HIGH-LEVEL MODEL OF THE NEW SYSTEM

The High-Level Model of the proposed system is illustrated in the figure below.

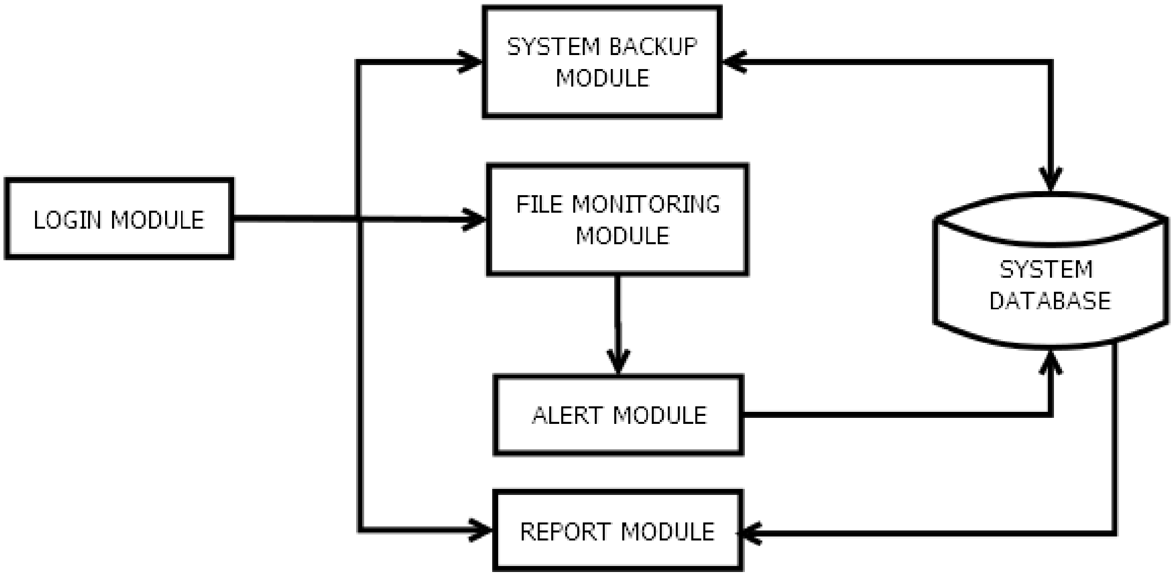

Figure 1

3.1.2 MAIN MENU

The main menu of the proposed system is presented in the figure below.

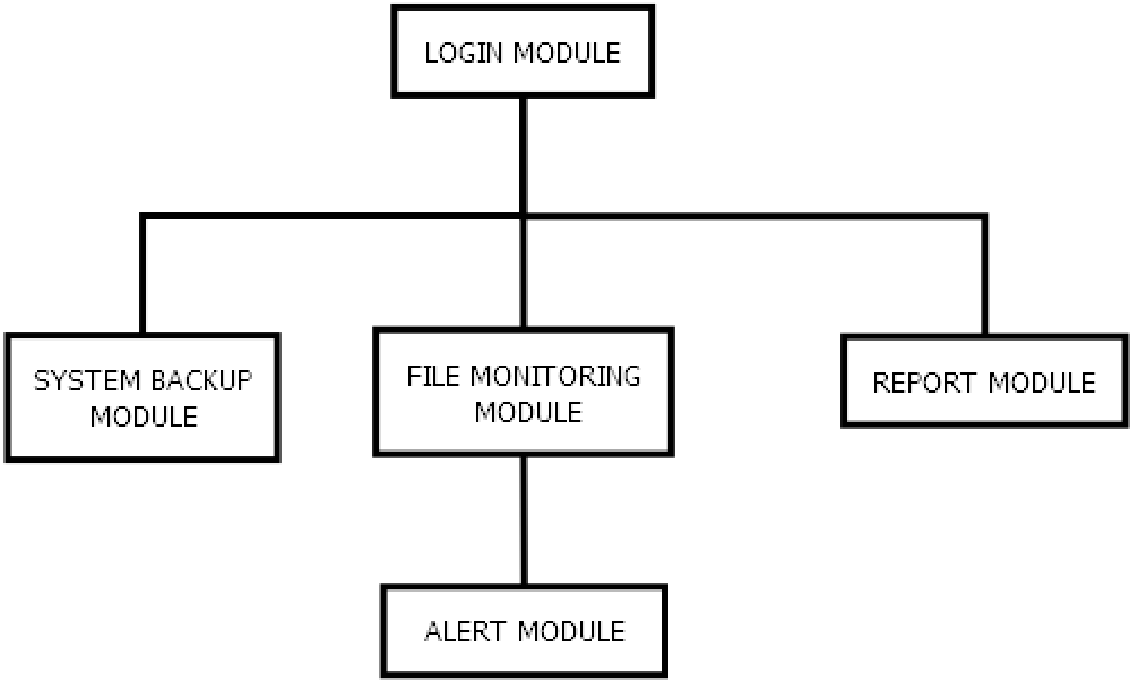

Figure 2

3.1.3 PROGRAM MODULE SPECIFICATION

The modules of the proposed system are presented below.

1. Login Module
2. Select Folder Module
3. View Report Module
4. Monitor Files Module
5. System Alert Module

3.1.4 ALGORITHM

The algorithm for the file monitoring process to be used by the proposed system is shown below:

1. Start

2. fetch the Folder to be monitored

3.Copy the files in the folder to a backup location

4. Copy the file properties to the database

5. Check the database for change in a file property

6. If change prompt user to confirm change source

7. If change source confirmed, then enter report and go to step 5

8. If the change source is not confirmed, lock down the system

9. End

3.1.5 USE CASE DIAGRAM

Below is the use case diagram of the proposed system.

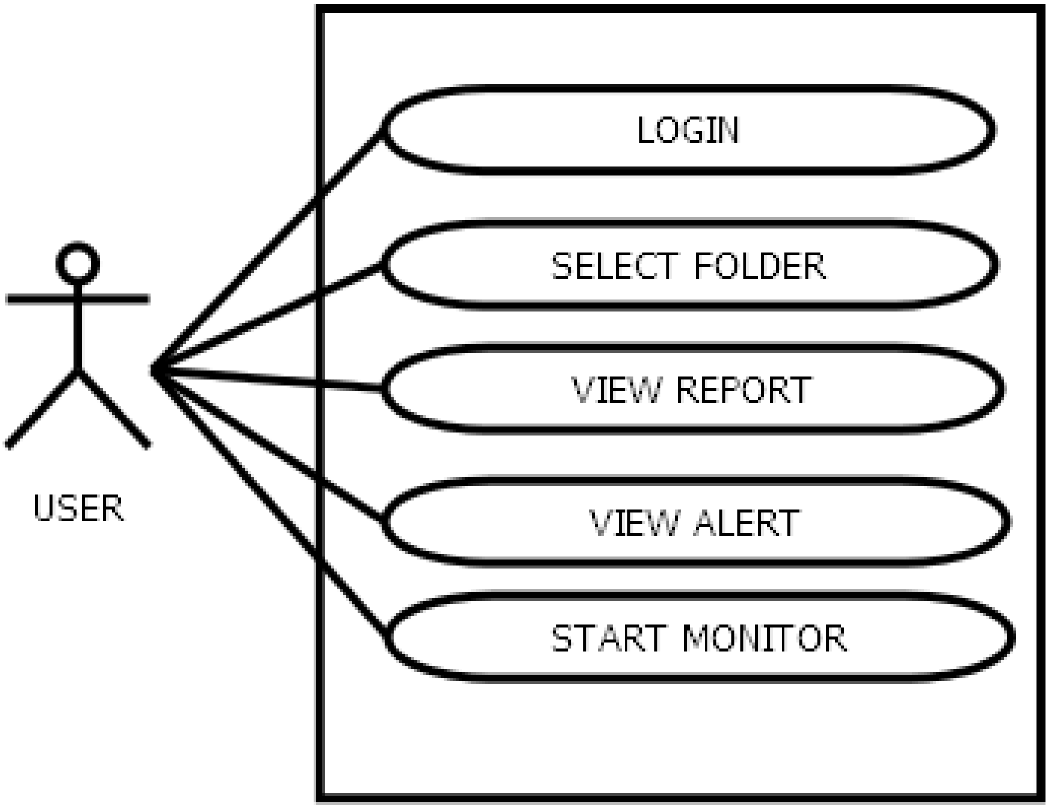

Figure. 3

3.1.5 DATA DICTIONARY

The data dictionary that will be used is listed in the table below.

DATA	TYPE
Username	String
Password	String
Name	String
Folder	String
Filename	String
Filesize	String

FileCreate	String
FileModified	String
FileAccesses	String
Report	String

3.1.6 FLOWCHART

The flowchart of the operations for the users of the system is displayed below:

User Operation Flowchart:-

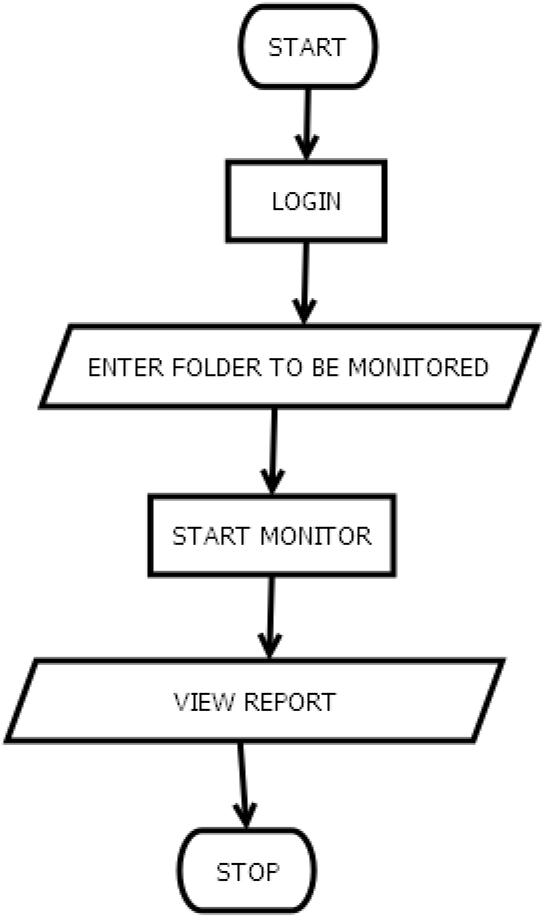

Figure. 4

System Operation Flowchart:-

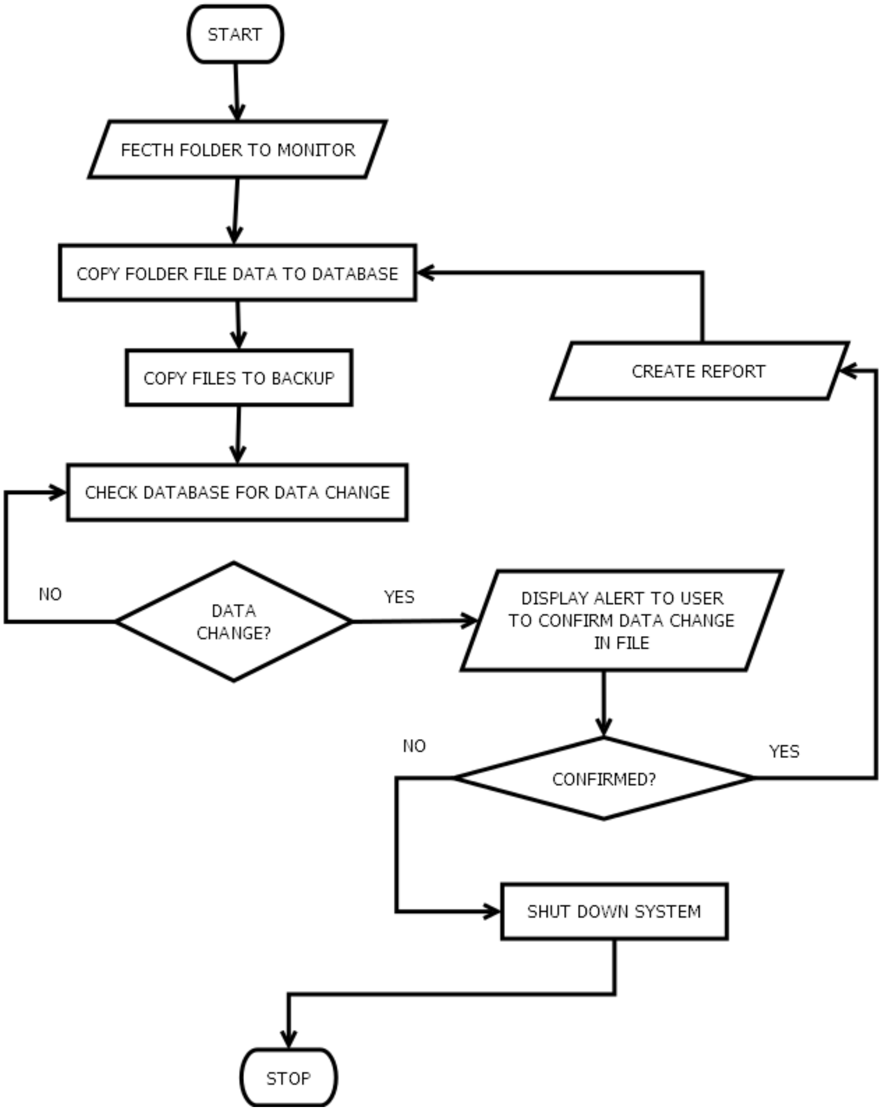
START
FECTH FOLDER TO MONITOR
COPY FOLDER FILE DATA TO DATABASE
CREATE REPORT
COPY FILES TO BACKUP
CHECK DATABASE FOR DATA CHANGE
NO
DATA CHANGE?
YES
DISPLAY ALERT TO USER TO CONFIRM DATA CHANGE IN FILE
NO
CONFIRMED?
YES
SHUT DOWN SYSTEM
STOP

Figure 5 Systems Flowchart

4.0 RESULTS AND DISCUSSION

The actual test result was done by choosing a folder on the system containing files that were to be monitored. The folder was monitored for changes by the system.

A file in the folder was changed by being renamed, and the software captured the event and sent a prompt asking the user to select options based on whether they were aware of the action on the file. The expected result was for the system to protect the files of the user as well as alert them to the danger of a possible attack on their system by malicious ransomware software. The system used a model that was able to monitor the chosen files and have them backed up as a proactive measure against attacks from ransomware malware. This way, the information of the user is safe as this is the only way that the file can be prevented from attack and protected without having to pay the ransom, as if their files get encrypted by the ransomware application, it will be impossible to decrypt.

5.0 **CONCLUSION**

Once attacked by ransomware, it is nearly impossible to undo the malicious software changes. Thus the best method of combating the problem is to use a preemptive approach to tackling the problem to detect the ransomware activity before it begins to damage the files on the PC. With this application, it is hoped that many computer users will be saved from the heartache of losing their precious data to internet criminally obsessed scaveng**ers.** This led to developing an Anti-malware Model for the Protection of the Computer System from File encryption-based ransomware. The system was developed and tested and was found to work as was expected by the researcher.

REFERENCES

Lutkevich, Ben; Richardson, Robert (2019) "ransomware" [online] TechTarget Available From <https://searchsecurity.techtarget.com/definition/ransomware>

Mimoso, Michael (2016). "Petya Ransomware Master File Table Encryption". threatpost.com. Available From <https://threatpost.com/petya-ransomware-encrypts-master-file-table/117024/>(28 March 2016)

Mitre Finch (2016) "STAFF ALLOCATION IS THE SOLUTION TO FRUITFUL STRATEGIC MANAGEMENT" [online] Available From <https://mitrefinch.com/blog/staff-allocation-solution-fruitful-strategic-management/>(14 October 2016)

D. Jay (2018) "Top 10 Reasons- Why You Need Effective Resource Allocation" [online] Available From <https://blog.orangescrum.com/2018/12/top-10-reasons-why-you-need-effective-resource-allocation.html>

E. BRAUN (2017) " Importance of Effective Resource Allocation" Available From <https://www.eresourcescheduler.com/blog/resource-allocation-simple-way-schedule> (February 14, 2017)

MEHWISH MAJEED (2019) "Importance of Resource Allocation and Time Management in Project Management" [online] Available From <https://project-management.com/importance-of-resource-allocation-and-time-management-in-project-management/>

N.Gopalakrishnan., J.Karthik., S.Pravin Kumar (2011) "Ant Colony Optimization for Effective Bed Allocation & Job Scheduling in Hospitals" Proceedings of International

Conference on Biomedical Instrumentation, Engineering and Environmental Management(ICBEEM-11), July 2011, Tamil Nadu _ pp. 39-43.

Arjita Sharma, Niyati R Bhele, Snehal S Dhamale, Bharati Parkhe (2015) "A Proposed Scheme for Software Project Scheduling and Allocation with Event-Based Scheduler using Ant Colony Optimization" International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 4, Issue 1, January 2015

Monmarché Nicolas, Guinand Frédéric and Siarry Patrick (2010). Artificial Ants. Wiley-ISTE. ISBN 978-1-84821-194-0.

Software Project Scheduling and Allocation with Event-Based Scheduler using Ant Colony Optimization:

Marco Dorigo and Thomas Stültze, Ant Colony Optimization, p.12. 2004.

Waldner, Jean-Baptiste (2008). Nanocomputers and Swarm Intelligence. London: ISTE John Wiley & Sons. p. 225. ISBN 978-1-84704-002-2