Detecting And Preventing Of Malware Spread

S.Kayathri, S.Ramya, S.Meena

Abstract: This article is one of the web application in cloud domain used to find the malware in server. The hackers and virus writers try to attack the computers connected to the internet. To detect the malware spread the user can fix the sensor in the server system it can scan the system continuously. If any error or malware occurred in the client side it can make the intimation for the admin. With the help of server, admin give the alert to the user to detect the malware. The user will get the intimation about the time and folder where the malware is occurred. By using this application the user can easily find out the malware so they can store their information safely. It provides more Authentications for the user. The sensor is used to scan the malware in the system. The scanning process is visible for the admin. So the user can know the sensor report and the timing of malware attack.

Keyword: Hackers, Malware, Spread, Sensor

1. INTRODUCTION
The main objective is to detect the malware spread. The user can fix the sensor in the server system it can scan the system continuously. If any error or malware occurred in the client side it can make the intimation for the admin. With the help of server, admin give the alert to the user to detect the malware. The user will get the intimation about the time and folder where the malware is occurred. By using this application the user can easily find out the malware so they can store their information safely. It provides more Authentications for the user. The sensor is used to scan the malware in the system. The scanning process is visible for the admin.

2. EXISTING SYSTEM
The existing system of malware spread fall is used to detect the particular system alone. The user can install the anti scanning process is visible for the admin. So the user can know the sensor report and the timing of malware attack.

2.1.1 Disadvantages
- The sensor scanned only the small files
- It cannot detect all the malware
- It can scan the single system alone

3. PROPOSED SYSTEM
In proposed system is used to detect the malware spread the user can fix the sensor in the server system. It can scan the system continuously. If any error or malware occurred it can make the intimation about the time and folder where the malware is occurred. It provides more Authentications for the user. This might be act as a better awareness for the person who drives.

3.1.1 Advantages
- Using this the user can easily find the malware
- The sensor can scan all the files
- It can find the attacked files
- The malware attacked time was intimate to the admin

4. PROBLEM DEFINITION
Now a day’s all the people are using systems and they can upload and share the files using internet connection at the time many malwares are attacked to the system to avoid that virus in the system can fix the sensor to scan the system continuously. At the time of scanning if any error or malware occurred it give intimation to both the user and admin. But in olden days the antivirus can scan the singles system alone. If any big files are attacked by malware it cannot scan. It can scan only the small files. To avoid this method the sensor based system was useful to find the malware. In this project user can login and registration facility to access the details.

5. OVERVIEW
The main objective of this article is to detect the malware spread. The user can fix the sensor in the server system it can scan the system continuously. If any error or malware occurred in the client side it can make the intimation for the admin. With the help of server, admin give the alert to the user to detect the malware. The user will get the intimation about the time and folder where the malware is occurred. By using this application the user can easily find out the malware so they can store their information safely. It provides more authentications for the user. The sensor is used to scan the malware in the system. The scanning process is visible for the admin.

6. MODULE DESCRIPTION
Sensing and Alert Sending
In this module if the admin can click the start button it can starts sensing continuously. After the completion of sensing if any malware can attack in the system it can give the alert to the server. Server can get the alert from the sensor.

---

Mrs. S. Kayathri, Assistant Professor/MCA, M. Kumaraasamy College of Engineering, Karur, Tamilnadu. E-mail: kayathris.mca@mkce.ac.in

Mrs. S. Ramya, Assistant Professor/MCA, M.Kumarasamy College of Engineering, Karur, Tamilnadu. E-mail: ginjas.mca@mkce.ac.in

Ms. S.Meena, Assistant Professor/MCA, M. Kumaraasamy College of Engineering, Karur, Tamilnadu. E-mail: meenas.mca@mkce.a.c.in

---
Register
The user has to register their details for the first time. In this page the user can make the registration process by giving their detail like Name, Username, Password, Security key. Once the user registers the details, user gets a benefit of regular user to get an account, server provide page that allows them to enter some information (the desired username, a password, and security key) and based on that to create the account. This is the registration page. To build the user registration page as authorized pages.

Login
In the login module the regular user can login the page by giving the username and password. After completion of login page the user can upload their files by clicking the browse button and the user can choose the location of the file. The user can send the selected file.

Authentication Process
In the authentication process it can encrypt the file and check the incoming packets. Server can check the authentication is correct or not. If the admin can enter the wrong security key it cannot decrypt the file. After giving the correct key it can start the process.

Attacker Model
In the attacker model it contains two types one is inside attacker and another one is outside attacker. In the attacker mode the admin can give their security key, if the key is correct it can start the process otherwise it gives the alert of authentication is wrong after giving the correct key it can give the details about the malware. It can find the attackers and the arrival time of malware.

Outgoing Packets
After completion of authentication process, it can find the endangered malware attack and the affected sensor list.

Figure A 7.2 Authentication Process

Admin Login
In this module the admin can login the page by giving the username, password and security key. After that admin can do their process like, to check the file list where the malware attacked and also check the time of virus attacked.

8. SYSTEM ARCHITECTURE
9. INTEGRATION TESTING
It is mainly used to integrate the all the software components combined together. It is done by after unit testing and before validation. Integrate the speed setting, speed ranging module. Based on that generate the SMS alert.

10. UNIT TESTING
Unit testing is used to check the test cases and program logic. It is used to check all the individual modules functioning properly and check the input and output values. Each and every module code flows validated. Before the integration check all the individual modules. This is the basic structural testing used in business processing and system configuration. It is used in accurately check the entire individual unit and expecting results. Unit testing is the small part of the application, it is applied in manually

11. FUNCTIONAL TESTING
Functional tests are mainly used to check the functionality of the sending message and receiving message. These two modules are integrated with android phone. Validate these two modules provide the systematic demonstration and customer requirement. Additionally this testing checks the data flow, business process, previous input and final output.

12. BLACK TESTING
Black Box Testing is testing the software, it check the external working of the each and every module. In this article external structure, workings, software problems are identified by the black box testing. In the black box testing check the software and hardware requirements of the document. It is mainly used to check the input and output behavior.

13. WHITE TESTING
This testing method is used to check the internal working of the coding. This testing method is mainly used to check the inner loop, structure, logic of the program. It is check all the major areas of the program.

14. CONCLUSION
The project is to detecting the malware spread. The user can fix the sensor in the server system it can scan the system continuously. If any error or malware occurred in the client side it can make the intimation for the admin. With the help of server, admin give the alert to the user to detect the malware. The user will get the intimation about the time and folder where the malware is occurred. By using this application the user can easily find out the malware so they can store their information safely. It provides more authentications for the user. The sensor is used to scan the malware in the system. The scanning process is visible for the admin.

15. REFERENCES