Send Orders for Reprints to reprints@benthamscience.ae

The Network Security Management System Design Against the New Virus Invasion

Liu Yinfeng*

Xi'an International University, Shaanxi, Xi'an 710077, China

Abstract: The virus and virus defense technology is always against each other and mutual development. In this regard, there have been various improved methods, such as dynamic detection, behavior analysis based on virtual machine technology, virus detection based on artificial intelligence technology, virus defense multi engine virus defense system and so on. The new virus defense architecture through fingerprint information to estimate user files are hidden virus risk, there will be a thorough analysis of the key part of risk file upload to the server virus defense. Information of fingerprint algorithm proposed in this paper for a new virus defense architecture, the removal of some commonly used algorithm complexity of fingerprint information, to a certain extent at the expense of fingerprint low collision rate and uniformity, the solving process to simplify the information of fingerprint algorithm, get faster convergence speed. The algorithm proposed in this paper is more prominent in processing large numbers of files at the request of the detection performance advantages.

Keywords: Message fingerprint, virus defense, virus detect.

1. INTRODUCTION

In today's world, the Internet has penetrated every corner of people's life and work, the development of computer network technology makes the Internet coverage of the yen interest widely, the impact on people's life, work and social order is normal. At the same time, viruses and other network security threats are becoming more and more serious, has brought huge economic losses. According to Computer Economics report, the global annual economic losses that caused by the virus is $10000000000. According to the Federal Bureau of investigation American (FBI) and Computer Security Association (CSI) released a research report [1], in the event of all computer system security attack, the number of virus attacks and the direct economic losses have topped the list. In China, computer virus defense situation is equally grim. According to Ministry of Public Information Network Security Supervision Bureau report shows that 54% of the surveyed units of information network security incidents occurred, the computer virus security about 84% of the total number of pieces. One part of computer virus attacks bring very significant benefits. According to [2] cnBeta.com reported in April 6, 2011, currently has formed a larger group of virus control 80% of the virus download channel, and formed a clear division of labor, income diversification gray industrial chain, only the flow of income a year profit of about 150000000 yuan. Sidiroglou *et al.* proposed a security architecture for E-mail [3]. Effect of [4] Bergeron *et al.* detected sequence API function calls to the virus, API as a key node in the control flow of the program to generate a graph, dangerous system call sequences and then test whether the graph contains exceeds a threshold value. In the field of intelligent virus defense, IBM, Tesauro and Kephart *et al.* discussed how to detect the nerve the network is applied to virus in [5], experiments show that, the neural network can be well applied to the boot virus detection. Arnold *et al.* Then this result is applied to virus detection [6]. Schultz *et al.* Windows32 environment to apply data mining methods to virus defense field [7], the use of executable code fragment, API call, DLL library and sequence of characters such as feature vector, the detection methods of different virus test. Kolter *et al.* Try to machine learning algorithm is applied to virus detection [8], experiments show that the detection effect is better than the single classifier using the integrated classifier.

In the field of Cloud Antivirus, Jon Oberheide [9] and Evan Cooke *et al.* [10]. of virus defense strategy under the cloud computing environment, analyzed the reason of Cloud Antivirus concept and practice. In the field of polymorphic virus detection, Christodorescu *et al.* Research on related technologies of [11] against the deformation of the virus, by introducing a virus automata to handle the virus code contained in the junk code and abnormal jump instruction, at the same time mark placeholder register, if the virus detection program generated automata and language intersect, that is abnormal detection program. Szappanos proposed a [12] Code normalization to detect polymorphic viruses, the technology gap in the removal of polymorphic virus code symbols, garbage code, take command, and then generate the virus specific characteristics of the code, but the essence is still the signature scanning technology based. This refers to a Bloodhound technology used to detect polymorphism virus scanner, heuristic using a static and a dynamic, the dynamic scanner by an expert system to collect program is running in the process of CPU information, the behavior sequencing of polymorphic virus after decryption. A method of integrity

1874-4443/15

through the test operation to prevent virus intrusion, to run the program signed using a signature tool, used to prevent the virus on the ELF format files of the infection. This paper presents a novel virus defense architecture. The new structure will be the main function of virus detection from the user's computer virus defense is transferred to the server, thus greatly alleviate the serious occupation of virus defense system of user's computer resources, improve the user's computer virus defense system usability and user experience. This paper proposes a new information of fingerprint algorithm is efficient. In the field of virus defense, because the user file size is too large, the risk of collision exists commonly used information in fingerprint fingerprint algorithm, may cause widespread influence. In the new virus defense architecture, user information fingerprint file just as judging user file filtering conditions need to upload the dismantling. Fingerprint the consequences of a collision is just a small amount increased network traffic and server load, does not affect the result of testing the user file security, the influence on the performance of the whole system is very small. Therefore, some complex characteristics of common information of fingerprint algorithm, such as avalanche effect, distribution of fingerprint check, in this specific application domain no longer has a very important practical significance.

2. TRADITIONAL VIRUS DEFENSE ARCHITECTURE

The traditional virus defense architecture universal detection method based on virus characteristic code. The so-called virus characteristic code, refers to the virus in an executable code fragment is special, can be used to accurately identify the type and name of the virus. In poisoned detection, the virus signature database of each feature code, retrieve its existence in a test file, so as to determine whether the detected file contains the character code corresponding to the virus.

2.1. Traditional Virus Defense Architecture Server

The traditional virus defense architecture in the server process as shown in Fig. (**1**), on the server side, after the collected samples of the virus file, firstly preprocessed file after file, get the shelling, and then analyze the sample virus. And different client, server resources are relatively abundant, can use more complex virus analysis technology. Then extract the characteristics of the virus code, add to the number of virus defense dig library server.

Through the statistical analysis of the virus database, so that the spread of the virus and the epidemic distribution, early warning of the recent high incidence of virus in order to. For a wide range of spread, causing serious harm to the virus, can the server launched antivirus.

2.2. Traditional Virus Defense Architecture are Faced with the Problem

From the above analysis of the traditional virus defense architecture of the client and the server is introduced, the traditional virus defense architecture is client - server architecture of light. The main function of the realization of viruses are present in the client, the client maintains a large database, the client can realize intelligent virus detection technology of all kinds of advanced. The traditional virus defense architecture is more and more difficult to deal with the virus emerge in an endless stream, partly because of the large number of viruses, rapidly evolving; on the other hand is because the traditional virus defense architecture itself has limitations: the virus detection is implemented on the client, and the client computing and storage resources are very limited, virus detection require storage and high strength a large number of computing resources, it will seriously affect the normal use of the user's computer.

3. THE NEW VIRUS DEFENSE ARCHITECTURE

The main focus of the design of new virus defense architecture is based on the existing problems of traditional virus defense structure improvement. The basic idea is the traditional virus detection function of virus defense architecture focused on the client to the server, so as to effectively alleviate the pressure on resources utilization of the user's computer, server and powerful computing ability and storage resources are relatively rich overall improve virus defense ability.

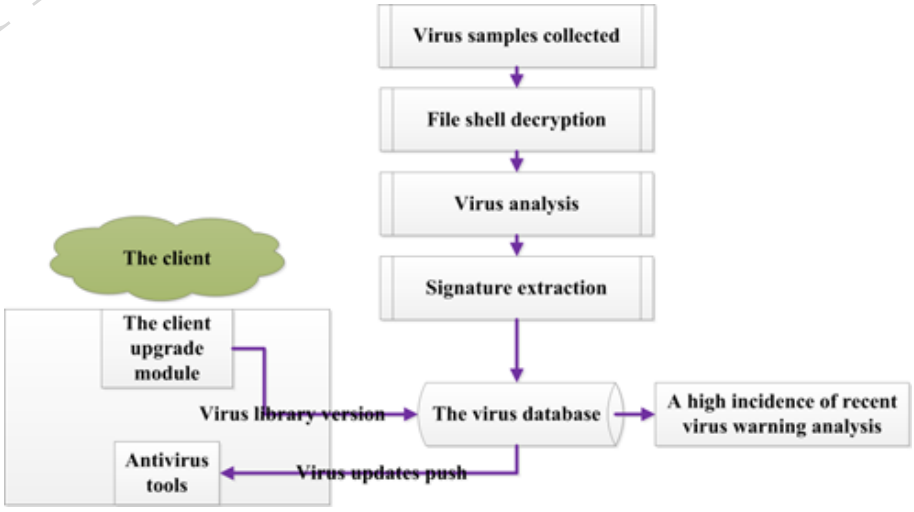

Fig. (1). The flow chart of the traditional virus defense architecture server side.

Since the new virus defense architecture will be the main function of virus detection is transferred to the server, the user will need to upload files to the server for virus detection. Therefore, the new virus defense architecture mainly faces two difficulties: (1) the protection of user privacy documents. (2) the massive user files for virus detection will cause a huge network traffic and server load. Do not solve these two problems, a new virus defense structure is difficult to have the practical application value.

Consider the design of a new type of virus defense architecture how to reduce network traffic and server load, mainly reflected in the following 4 points:

A) Boundary defense module

Computer operating system originally installed in the user should be safe, in the installation of anti-virus system will also be full scan to file system of the user's computer, so it can be considered in the initial conditions, the user system is safe. Therefore, virus defense system does not need to always detect virus of all the files in the file system, only need to modify the contents of virus defense in the file system to be modified, so as to ensure the security of the system, and reduces the unnecessary virus defense spending.

B) The recent high incidence of virus database

The new virus defense architecture will be completely virus character codes stored in the server, stored on the user's computer in a recent high incidence of virus database. According to the principle of locality, accounting for 20% of the total number of the virus in virus virus attacks accounted for 80%, so the recent high incidence of virus database resources only for complete virus signature database is 20%, but the virus hit rate can reach 80%. This design, hand to ease the use of the user's computer virus defense architecture resources, improving the efficiency in the use of user's computer resources; on the other hand, 80% of the virus can be in the local user computer is detected, greatly reducing the virus defense architecture of network traffic and server load.

C) fingerprint algorithm using information efficiently

In the new framework, considering the risk brought by touch the fingerprint, fingerprint information file is not directly based on the judgement of the security document, but the document information of fingerprint as a filter, filter out the credibility of good to upload to the server to conduct a thorough analysis of virus defense documents.

D) specification document decomposition Not all user files are uploaded to the server for virus defense to virus detection, virus defense structure according to the new file specification dismantling dismantling key parts may contain viruses of different types of users in the file upload.

3.1. New Virus Defense Architecture Design for the Client

The basic design of a new type of virus defense architecture the client as shown in Fig. (**2**), when the user of a computer's file system received from outside the credibility of unknown file, such as the user to download or copy files through the USB interface, virus defense system boundary defense drive will perceive the user behavior, and then sent to the virus defense system message start the process, virus defense. To file for each new user credibility and unknown in the file system, driven by the border defense cooperation and file scanning module, select a file from the virus detection, according to the following steps:

A) access to the user computer local recent high incidence of virus database, file signature matching. If you can match, including the recent high incidence of virus in the file, to step f); if not, the recent high incidence of virus, that the file is not included, but also the need to further examine, turn the steps of B).

B) depending on the type of file, in accordance with the dismantling of the user file specification dismantling dismantling, and virus detection related documents critical section. Step C).

C) For information on file fingerprint key section, will detect the fingerprint information is uploaded to the server, virus defense. Virus defense server receives the information of fingerprint, fingerprint detection risk file access, user query is a dangerous file. If the information is recorded in the file fingerprint dangerous virus defense server fingerprint database, indicating the presence of dangerous user file, further testing is needed, to step d); if the information is not recorded in the fingerprint anti-virus server, the file security, turn the steps of G).

D) virus defense server will return the results to the user computer fingerprint detection. The client file upload to the critical section virus defense server for further testing, to step e).

E) virus defense server receives the file key section, followed by various virus detection engine of client files for virus detection. If the file does not contain a virus, to step g); if the file containing the virus, virus defense server update dangerous file fingerprint database, and the steps of F).

F) determine the user file containing the virus, ill file processing module for virus file processing, such as virus file cleanup, quarantine and backup etc..

G) determine the user file security.

3.2. New Virus Defense Architecture Design on the Server

New virus defense architecture server-side basic design as shown in Fig. (**3**), In the new virus defense architecture of the server, to collect samples collected by the mechanism of virus samples, the samples after pretreatment to the virus detection engine cluster processing, after a series of virus detection module detection, feedback analysis results to the user. If analyzed in server file contains a virus, you need to make a series of updates to the database server:

A) file fingerprint extraction dangerous file, add to the risk of virus defense server file fingerprint database.

B) extracted from the virus feature code added to the features of the virus, virus defense server code library.

C) for a period of time the virus for statistical analysis, the recent high incidence of virus database updates.

D) for particularly harmful, especially wide virus, to specific analysis, the timely introduction of targeted killing kit.

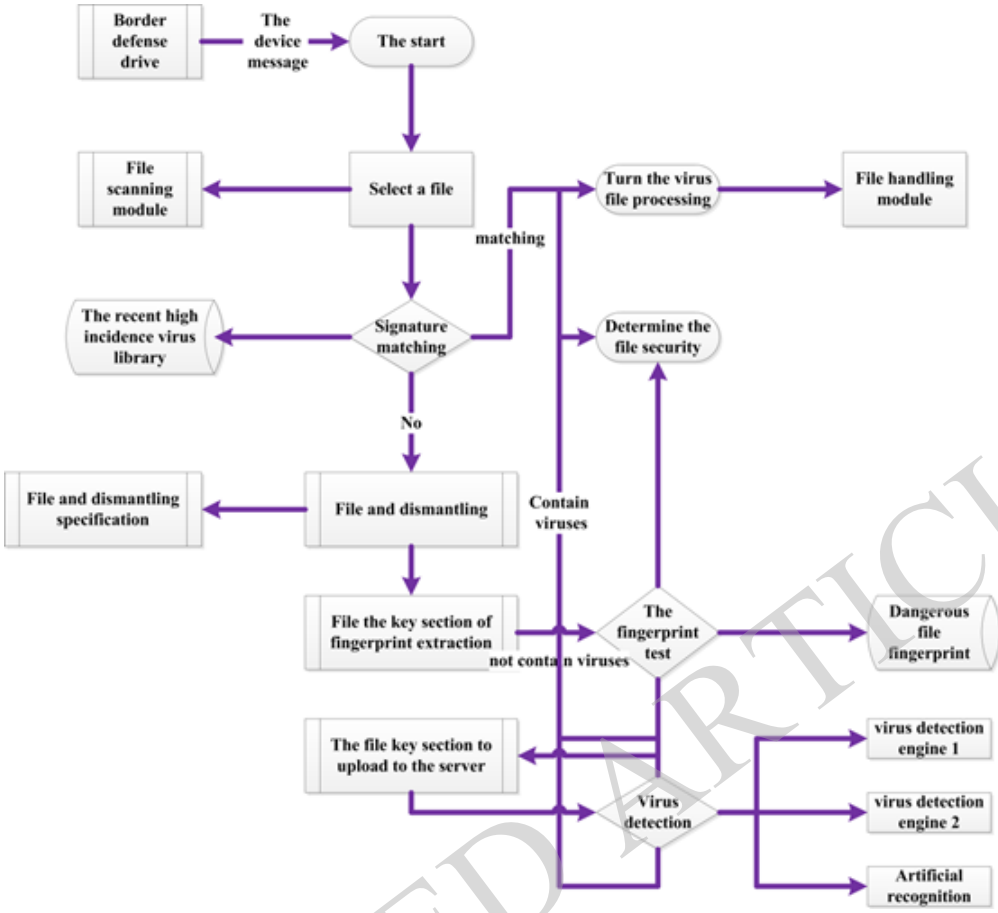

Fig. (2). new virus defense architecture client design.

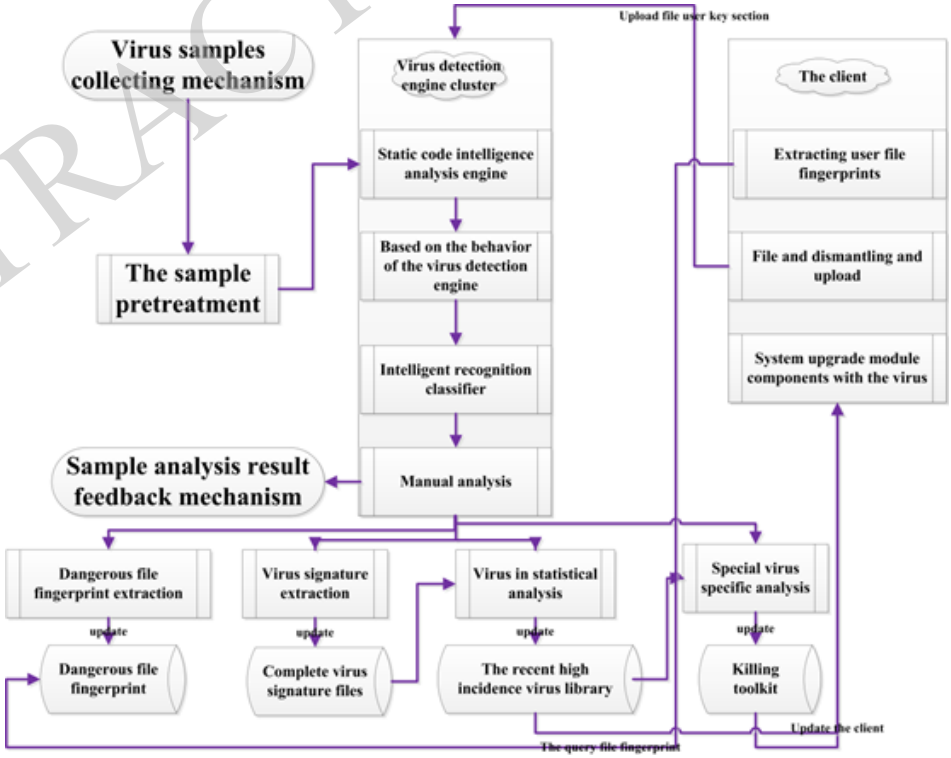

Fig. (3). New virus defense architecture design on the server.

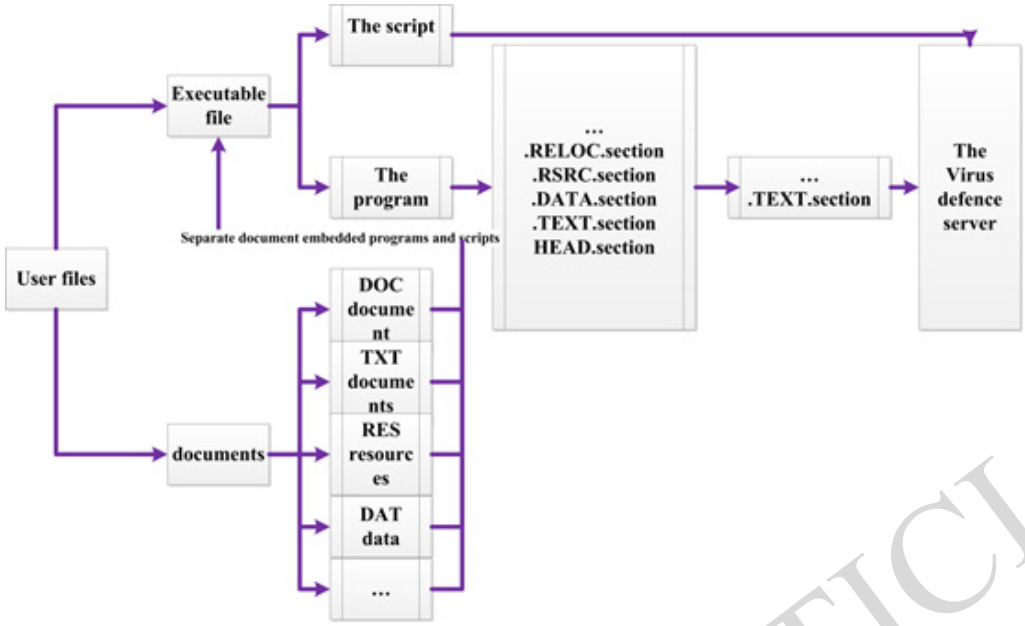

Fig. (4). Windows platform user file classification and dismantling upload the schematic diagram.

After the recent high incidence of virus database updates and designed to kill kit on the server side, the need for timely update will be pushed to the client.

3.3. File and Dismantling Specification

User file type is various, huge quantity. Direct all users to upload files to the server will have unimaginable virus defense of network traffic and server load. File specification is to define how the dismantling dismantling the user file and virus detection key part related to upload to the server.

Not all users are likely to contain the virus file. User profiles can be divided into executable files and documents in two categories. Executable files can be divided into two kinds of scripts and programs, program code segment, data segment by segment, resources, relocation table, export symbols section of code, which only contains executable procedures of the user's system implementation, data segment, the resource section section does not contain malicious operation. Therefore only need to disassemble the code uploaded to the server for virus detection, virus defense. The document, after the separation of the programs and scripts embedded in the document, containing only the user data information and does not contain the user operation, does not contain the virus. In the Windows operating system platform for the user the most widely used as an example, users upload file classification and recycling as shown in Fig. (**4**):

4. NEW VIRUS DEFENSE ARCHITECTURE ANALYSIS OF THE RESOURCE USAGE

4.1. New Virus Defense Architecture Model of the Resource Usage

The new virus defense architecture resource occupation diagram as shown in Fig. (**5**), Fig. (**5**) shows, the new virus server provides virus defense services according to a certain sequence for each client, the server provides services to the I client, server resources are occupied by each module for the I client to upload the file, so the model can be converted to a typical resource allocation problem, a large number of research results of network control theory and energy efficient network can be applied to the field.

4.2. The New Virus Defense Architecture Resource Usage

$t_{\max} = \max(t_1, t_2, ..., t_m)$ is the bottleneck of assembly line, the client n service time of $\sum_{i=1}^{n} k_i$ a user file content:

$$T = t_1 + t_2 + ... + t_m + \sum_{i=1}^{n} k_i - 1 \cdot \max(t_1, t_2 .. t_m) \quad (1)$$

In practical application, the order of magnitude of m is less than 103, the number of n is 1010, the order of k_i is 106, $\sum_{i=1}^{n} k_i$ is much larger than that of m; (3.4), then the formula of:

$$T \approx t_{\max} \cdot \sum_{i=1}^{n} k_i \quad (2)$$

New virus defense architecture the server footprint as follows:

$$RT'_s \approx (r_s + r_1 + r_2 + ... + r_m) \cdot T = (r_s + \sum_{j=1}^{m} r_j) \cdot t_{\max} \cdot \sum_{i=1}^{n} k_i \quad (3)$$

New virus defense architecture in the ith the footprint of clients are as follows:

$$RT'_i = (r_c + r_0) \cdot r_i \cdot t_0 \quad (4)$$

The total footprint for the new virus defense architecture:

$$RT'_t = RT'_s + \sum_{i=1}^{n} RT'_i = (r_s + \sum_{j=1}^{m} r_j) \cdot t_{\max} \cdot \sum_{i=1}^{n} k_i + \sum_{i=1}^{n} k_i \cdot t_0 \cdot (r_c + r_0) \quad (5)$$

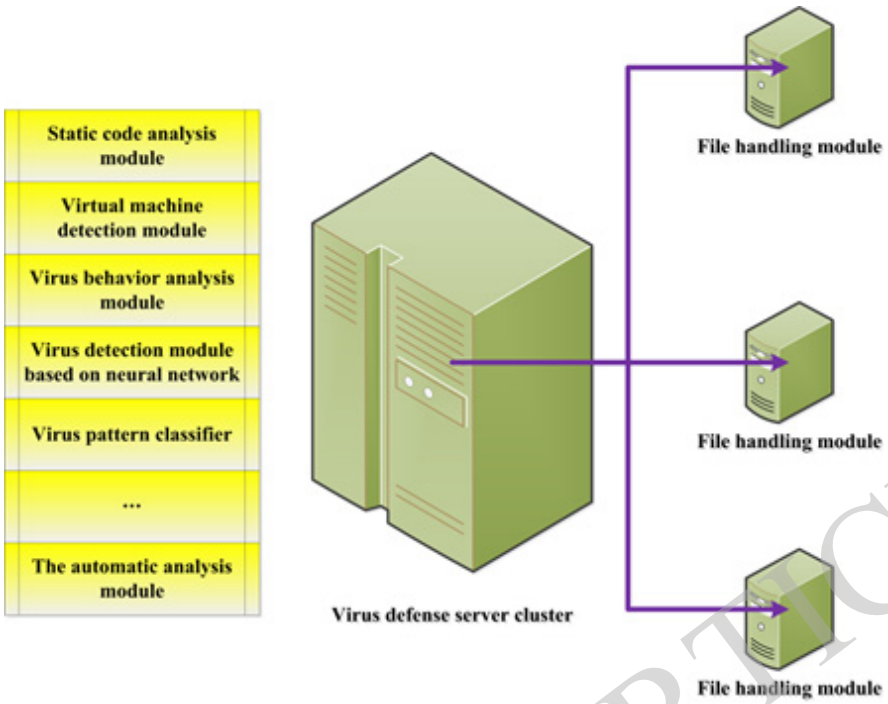

Fig. (5). New virus defense architecture resource usage.

The traditional virus defense architecture resources usage and new virus defense architecture resource consumption number of death level is $O(n \cdot k_i \cdot m \cdot r_j \cdot t_j)$. This shows that in the sea to provide better disease defense services at the same time, the new virus defense architecture does not lead to greater consumption of resources.

Network virus defense system of a large scale, but the energy consumption problem of virus defense system study is less. Because in the traditional virus defense architecture, core modules are concentrated in the client, the user of a computer implementation of energy-saving strategy is not easy. The new virus defense architecture the client resources transferred to the server cluster, on the one hand the release of user's computer resources, improve the usability of the user of a computer system; on the other hand, is conducive to the implementation of energy saving strategy in large centralized server.

CONCLUSION

With the development of computer network is more and more extensive influence on people's life and work, computer viruses and other network security threats has intensified. Virus defense situation increasingly severe yen, against the virus to countries around the world have brought huge economic losses. On the one hand, the number of computer virus is very large, but every year to grow at a faster rate. On the other hand, the computer virus has evolved more difficult to find and remove.

Signature detection of traditional virus defense architecture based on has been widely used, because before this is the most simple and effective way. Retrieval and virus characteristic code fragments in the executable code by virus, virus defense system can accurately identify the type of virus, and then be removed.

But today, the traditional virus defense architecture has been difficult to continue. With the development of technology, hackers generally deformation of viruses by software encryption technology, the automation tool capable of mass production of virus, resulting in 2006 after a surge in the number of viruses, and the growth rate increased year by year. One of the disadvantages of the traditional virus defense architecture features of the virus is dependent on the client's code base, but the virus signature database limit the size of the user's computer has close bearing. The drawbacks of the computing ability of computer user two is insufficient, need to support the intelligent detection of virus, resulting in the ability to detect the virus defense system of the traditional lack of virus. The traditional virus defense system not only caused unbearable burden to the processor and memory the user's computer, and the ability of the virus to the defense can not meet the needs of the situation.

In order to solve the above problem, this paper analyzes the design of traditional virus defense architecture, points out the defects of the traditional virus defense architecture is the most important virus were detected in the user's computer, causing virus defense required resources are severely constrained. Aiming at the defects of the traditional virus defense architecture and various improvements in the presence of. This paper presents a new type of virus defense architecture, the main function of virus detection, virus defense is transferred to the server, to ensure that there is sufficient resources for advanced intelligent computer virus detection; the key part of the user uploaded files will have the necessary in-depth and comprehensive analysis, rather than directly according to the information of fingerprint files to determine whether a file security; comprehensive use of a variety of strategies, because users upload files to reduce network and server load; at the same time, the problem of user privacy protection are discussed, and puts forward some suggestions from the perspective of technology.

In the new virus defense architecture, no longer as the only file fingerprint identification document, but as a file security query ID, is essentially a judge whether need to filter users to upload files to the server of the virus defense. In this application, some complex characteristics information of fingerprint algorithm commonly used in such as fingerprint, fingerprint distribution uniformity in the process of operation avalanche effect will no longer have very important practical significance, fingerprint collision consequences may not only is necessary to upload user files uploaded to the server for the detection of virus defense detection of the file security, does not affect the results. Therefore, this paper proposes a merge hash algorithm, simplify the process of solving the information of fingerprint, the fingerprint uniqueness of sacrifice and low collision rate, improve the efficiency of the fingerprint solution, in order to better cope with the new virus defense architecture to handle massive amounts of user files. The experimental results show that, the merge hash algorithm does have the speed upgrade, but because of the impact of document processing and other aspects of the promotion effect as it were.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

[1] B. Stephenson, and B. Sikdar, "A quasi-species model for the propagation and containment of polymorphic worms," IEEE *Transactions on Computers*, vol. 58, no. 9, pp. 1289-1302, 2009.

[2] S. Paul, and B. K. Mishra, "Selection of next generation anti-virus against virus attacks in networks using AHP," *International Journal of Computer Network and Information Security*, vol. 2, pp. 29-35, 2013.

[3] J. Dean, and S. Ghemawat, "Map Reduce: simplified data processing on large clusters," *Communications of the ACM,* vol. 51, no.1, pp. 107-113, 2008.

[4] S. Ghemawat, F. H. Gobiof, and S. T. Leung, "The google file system," *ACM SIGOPS Operating Systems Review*, vol. 37, no. 5, pp. 29-43, 2003.

[5] F. Chang, J. Dean, and S. Ghemawat, "Big table: A distributed storage system for structured data," *ACM Transactions on Computer Systems*, vol. 26, no. 2, pp. 10-18, 2008.

[6] S. Sidiroglou, J. Ioanidis, A. D. Keromytis, and S. J. Stolfo "An email worm vaccine architecture," *Proceedings ofthe 1st Information Security Practice and Experience Conference*, pp. 97-108, 2005.

[7] J. Bergeron, M. Debbabi, J. Desharnais, and M. Erhioui, "Static detection of malicious code in executable programs," *In Symposium on Requirements Engineering for Information Security*, pp. 1-8, 2001.

[8] G. Tesauro, J. Kephart, and G. Sorkin, "Neural networks for computer virus recognition," *IEEE Expert*, vol. 197, no. 11, pp. 5-6, 1996.

[9] W. Arnold, and G. Tesauro, "Automatically generated Win32 heuristic virus detection," *Proceedings of the International Virus Bulletin Conference* 2000.

[10] M. Q. Schultz, E. Eskin, and E. Zadok, "MEF: Malicious Email Filter, A Unix mail filter that detects malicious windows executables," In: *Proceedings of USENIX Annual Technical Conference*, pp. 245-252, 2001.

[11] J. Z. Kolter, and M. A. Maloof, "*Learning to detect malicious executablcs in the wild*," New York: ACM Press, pp. 470-478, 2004.

[12] J. Oberheide, E. Cooker, and F. Jahanian, "CloudAV: N-Version Antivirus in the Network Cloud," *Proceedings of Network and Distributed System Security Symposium, San Diego*, CA, 2004.

Received: May 26, 2015 Revised: July 14, 2015 Accepted: August 10, 2015