Proposing OMVDPM – Offline Macro Virus Detection and Prevention Mechanism

Inderpal Singh[1], Sheetal[2]
Department of Computer Science & Engg[1, 2]
CKD Institute of Management and Technology, Taran[1]
Sri Sai College of Engg and Technology, Manawala (Amritsar) [2] Punjab (India)

ABSTRACT
This paper discussed about different types of viruses along with its symptoms, causes as well as side-effects and correspondingly proposes a new designed methodology named ***OMVDPM*** (offline macro virus detection and prevention mechanism) on the time of MS-Word document accessing. The complete functioning of this new designed methodology is work under main two steps viz. at first detect macro virus in word document and in second step provide prevention from macro virus. This new designed methodology utilizes the concept of log files for continuous monitoring of the details of that specific MS-Word document as like the date of creation of document, time as well as space consumed and the working of this new designed methodology is totally based on automatic randomly generated encrypted digital signature on the time of MS- Word document saving. The more interesting feature of this new designed methodology is every time a log file is created when document will be accessed by that specific user (i.e. who is owner of the document) and it provides latest details of that specific file with automatic updated time, date and space consumed. The main focus of this paper is to reduce the growth of macro virus in MS Word document on the time of document accessing and provide offline ***encrypted digital signature*** security of document at saving mode.

Keywords
Macro Virus, Resident Virus, Log Files, Computer, Offline Security, Digital Signature, MS-Word document.

1. INTRODUCTION
Computer viruses [10] [14] are omnipresent as like air in digital world. The use of computer in digital word in increases day by day because of the dependency of the humans on machine increases [3]. As computer professionals collected data in their surveys, malwares or viruses are the most dangerous threat [13] for our computer world. Once malware enter into the system then it starts to find vulnerabilities within the operating system and after that perform unwanted operation in the system [17] Now a days, there are several types of malwares [14] [24][25][26] exists as shown in figure.1 and figure.2.

The most important type of malware is virus. The classification of virus is further divided into three portions viz. add on, shell and intrusive code [6]. Each category has its own method during spreading. For handling these three different types of virus classification computer security professionals developed several different anti-virus software's [1] and mechanisms. It was the only reason authors said, it is a kind of big contest between virus creators and anti-virus developers. As increases the usage of computers the growth of viruses attacks will be increases and shapes its results in the form of cyber-crime.

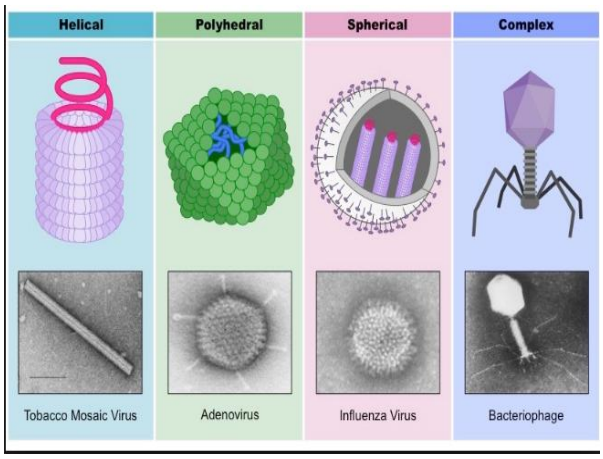

Fig.1 Types of Viruses [25]

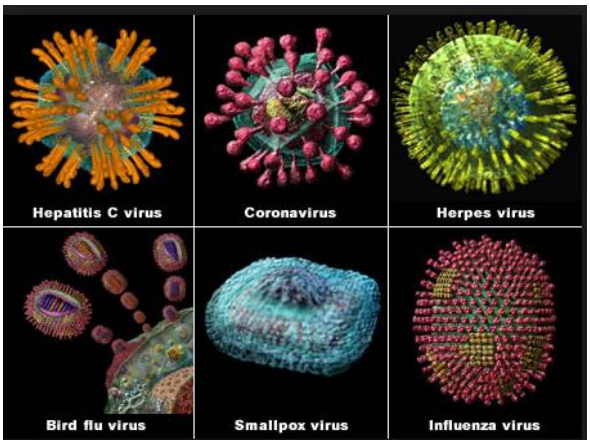

Fig.2 Types of Computer Viruses [26]

Cyber-criminals main function is to launch and spread virus [23] over the network and steal or alter information. They uses several ways to spread their viruses and the most common methods are email medium [19][20] and Wi-Fi hotspots by utilizing metamorphic techniques [11]. The main function of metamorphic technique is to infect the internal structure of the application. By utilizes these two common methods cyber criminals will easily spread viruses in different user accounts. This increased growth of cybercrime over network gives birth to computer forensics [16]. Alternatively, anti-virus software developers [1] designed new strategies for virus detection methods [7] as an example most commonly virus bypass detector tool is used by anti-virus software developers for detecting malicious programs. The latest idea

used by the researchers is usage of computer immune system whose main function is to provide protection by their own. It performs self and non-self-monitoring against viruses [8]**.**As authors surveyed every year thousands of viruses are found by utilizing traditional approaches but these are not enough or sufficient to detect infected files. So to provide prevention [5] from different types of viruses [2] [5] authors suggested to study every virus individually deeply as like their features [12], operations [4] along with their overall structure [21][3]. So that prevention will be provided in advance in future. Different types of viruses with its origin and examples are discussed in table.1 given below:

Table.1: Virus Summary with its causes and example [2] [5] [14].

S.NO	*Type of the Virus*	*Origin/Root Cause of Virus*	*Example*
1	Macro[9]	Payload send in email inbox	MS-Word
2	Zombie[9]	Email Inbox	GMAIL SPAM folder
3	Browser Hijacker	Web browser	Bing and Fox tab search
4	File Infector[22]	Host file	.exe file
5	Resident	RAM	Memory space wastage
6	Web Scripting[22]	Warning message alert created by web browser	Report attack site & file extension like(.vbs,.com,.pif,.bat)
7	Space Filler	Hard Disk	Message length increase and space wastage
8	Logic Bomb	Host(Standalone program)	Congratulations you are the only winner of one crore.
9	NTFS	Stack data structure	Buffer Overflow
10	Melissa[9]	E-Mail attachment	MS-Word/MS-Outlook
11	Conflicker	Pen Drive/Removable drives	Collect financial information through database
12	Boot Sector	Hard Disk	MS-DOS

This research paper target is to find the factors which leads the virus attacks among personnel computer users.In this research paper, authors discussed about macro virus where the function of macro virus[13][14] is to distrub the content of microsoft word by applying infection and correspondingly it performs sequence of actions automatically when file is accessed by that authenticated user. As authors surveyed, such type of macro virus is mostly spreaded through email MS-Word document attachments in enterprises. Here,authors designed a new methodology named "OMVDPM" is termed as offline macro virus detection and prevention Mechanism. The function of this new designed methodology is at first to detect virus and after that provide prevention from that dectected virus as shown in fig.3:

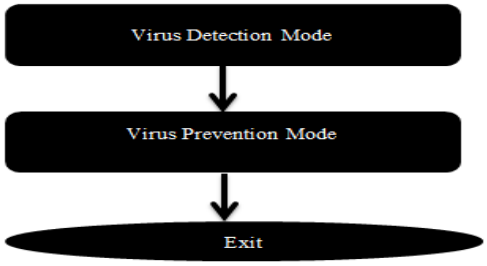

Fig.3: A Roadmap for OMVDPM.

As information collected from literature survey, manual digital signature is applied for providing offline security to MS-word document user. Once manually digital signature [7] [15] [18] is applied then alteration will not be possible. This new designed methodology provides automatic randomly generated encrypted digital signature while clicking on file save button as shown in fig.4:

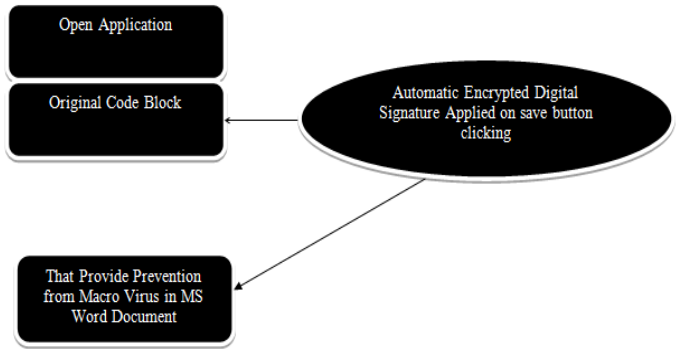

Fig.4: OMVDPM- A New designed Mechanism.

One more interesting feature of this new designed methodology is every time when user accesses the same file again and again then a separate encrypted digital signature is created for more tighten the security form the macro virus. This new designed methodology utilizes the concept of log files for continuous monitoring of the details of MS-Word document as like the date of creation of document, time, type of content saved as well as space consumed as shown in User Accessing File Cycle(UAFC) that can be diagrammatically represented in fig.5:

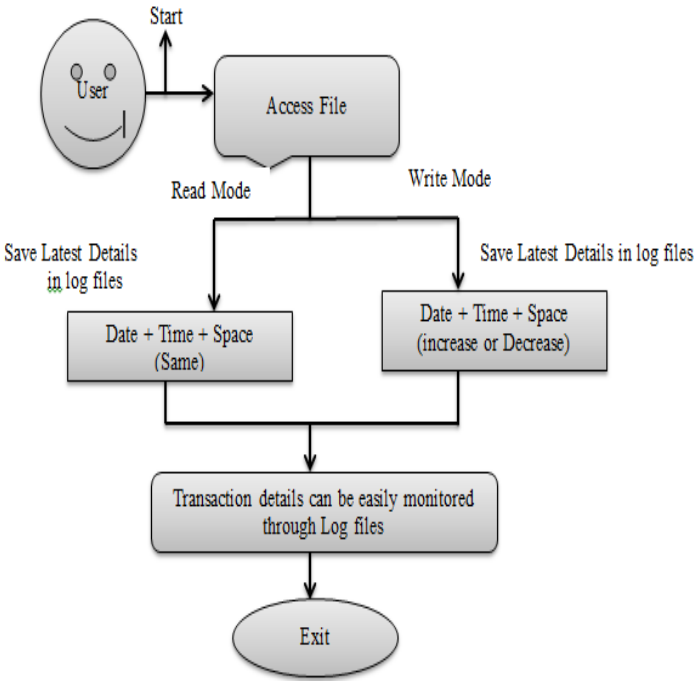

Fig.5: User Accessing File Cycle (UAFC).

The major function of User Accessing File Cycle is to provide latest updates like date, space consumed and time through log files. And the working of this new designed methodology is only based on automatic randomly generated encrypted digital signature on the time of MS- Word document saving. In addition, it has one more feature that is every time a new automatic encrypted digital signature is created on the click of

save button at the accessing of that specific MS-Word document. This proposed methodology may help to reduce macros in word document that is actually a major threat for the well-being applications usage.

2. RESEARCH DESIGN

Fig. 6:A path to provide offline security from Macro Virus.

3. A ROADMAP FOR EXISTING SCENARIO (MS-WORD PROCESSING)

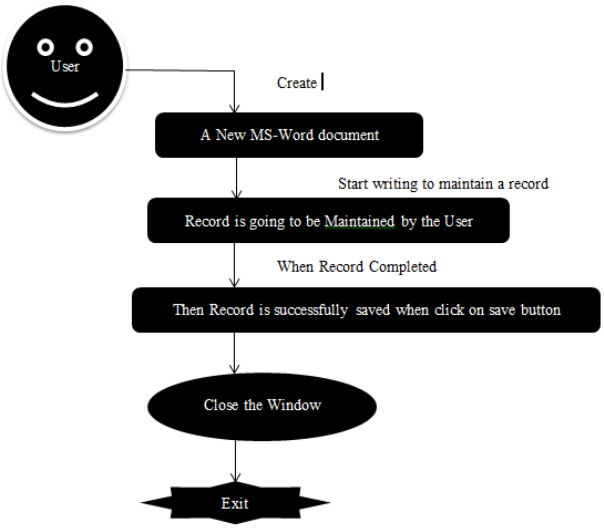

Fig. 7: Steps enabled for Creating a Microsoft Word Document.

4. A ROADMAP FOR PROPOSED OMVDPM (Offline Macro Virus Detection and Prevention Mechanism)

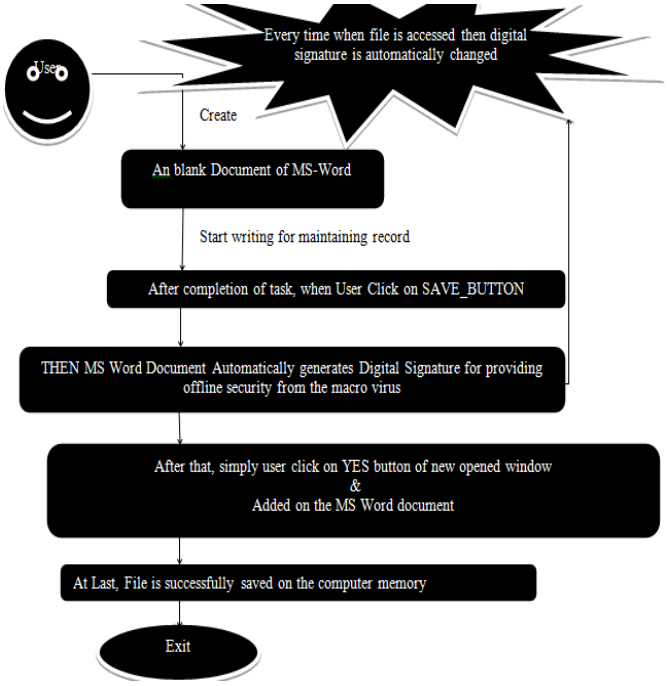

Fig 8: Steps Enabled for designing OMVDPM(Offline Macro Virus Detection and Prevention Mechanism).

5. CONCLUSIONS

Different types of viruses are reviewed with their symptoms and causes are analyzed in this paper. Macro virus may considerably be reduced by developing the procedure named OMVD & PM (Offline Macro Virus detection & prevention Mechanism) is designed in this procedure. The complete working of this new designed methodology is based on automatic randomly generated ***encrypted digital signature*** every time that is on the time of document (i.e. MS Word) saving. The major benefit to utilize this new designed methodology is continuous monitoring of log files. The main significance to utilize log file is to give the complete details of transactions processing as like date of document created, type of document, time of document processing as well as space consumed by that specific file etc. This new designed methodology provides a secure and an efficient way to access MS WORD document. In this way, this new designed methodology may help for enhancing home computer/personnel computer security from macro and resident viruses and correspondingly provide a better quality of service (QOS) by authors.

6. REFERENCES

[1] Zaqaibeh belal & Jebril.H Iqbal, September 2008. Computer virus strategies and detection method, International journal of open problems in computation math.

[2] Ibrahim suhaimi & masrram Maslin, January 2016. Evolution of computer virus concealment & anti-virus techniques: A short survey, International journal of computer science.

[3] Patil.V Bhaskar & Joshi, May 2013. Computer virus: Their problems and major attacks in real life, International journal of peer to peer network trends and technology.

[4] Spafford.H Engine, 1994.Computer viruses as artificial life, Journal of artificial life, MIT Press.

[5] MIS Unit, the impact of computer virus attacks and its preventive mechanisms among personnel computer users, south eastern University, Sri Lanka.

[6] Zanero Stefano & serazzi giuseappe, 2001.Computer virus propagation models, IEIIFCNR Institute.

[7] Malavade N. Vinayak, Bhuvad S Shrinivas, March 2014. Study and comparison of computer viruses, International journal of advanced research in computer science and software engg.

[8] Bag by KURT, Taking computer virus detection to a new level, University of Auckland, New Zealand.

[9] Gong Weibo, Towsley Don, Email Virus propagation modeling and analysis, Technical report TR-CSE-03-04.

[10] Martin Alexandra, Koi Yaw Godfred, 2012. The economic impact on computer virus- A Case of Gauna, Journal of emerging trends in computing and information sciences.

[11] Dey Kumar Bhabesh, Charan Singer Mahindra, Mishra Lokesh, May 2012. The new age of computer viruses and their detection, International journal of network security and its applications.

[12] Kharat Vilas & Gore Sharad, December 2011. Computer viruses in UNIX Environment- A Case study, International journal of computer engg and Science.

[13] Joshi.J Milind & patil V. Bhaskar, 2011. The working and problems of computer virus in enterprise areas, International journal of computer science an Information technology.

[14] Singhal, 2014. Computer viruses in India- A Questionnaire Survey, International journal of computer applications, National conference on innovations and recent trends in engg and technology.

[15] Saharan ravi & Chaudhary ravi raj, 2011.Feature detection approach from viruses through mining, Journal of global research in computer science.

[16] Lai.Y.K, Kwan K.W, The rules of time on NTFS file System, University of hongkong.

[17] Pathak K.M, Keller M.J, October 2014. Protection of smart phone, personnel computer and other similar devices from virus infections, International journal of innovative research in computer and communication engg.

[18] Herawan Tutu & sharif MD Azmir, July 2013.On analysis and effectiveness of signature based in detecting metamorphic virus, International journal of security and its applications.

[19] Gong Weibo, Towsley Don & Zon C Cliff, Modeling and simulation study of the propagation & defense of internet email worm, University of central Florida.

[20] Liu Jun Ding Hua Qing, Computer virus propagation model based on variable propagation rate, International journal of advanced science and technology.

[21] Rasheed Frheem Muhammad, March 2012. Modeling virus propagation in peer to peer network, International journal of computer science.

[22] Sarvanam.V, Rajeshwari.S, January 2013. Security issues in protecting computers & maintenance, Journal of global research in Computer science.

[23] Toyoizumi Hiroshi, Performance evaluation of defence strategies against computer virus, University of Aizu.

[24] Bajaj Chetna & Khari MANJU,July 2014.Detecting Computer Virus, International journal of advanced research in computer engg and technology.

[25] Virus Classification [Image - Online] http://ib.bioninja.com.au/standard-level/topic-5-evolution-and-biodi/53-classification-of-biodiv/virus-classification.html

[26] What Are The Types of Computer Viruses? [Image - Online] http://www.codercaste.com/2009/09/30/what-are-the-types-of-computer-viruses/