International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

Intrusion Filtration System (IFS) - Implementation of Security Model

Marlapalli Krishna, V Shariff, Bandlamudi S B P Rani, S K Chaitanya Rudraraju, Soni Lanka

Abstract: ***Different algorithms of data mining used to filter the traffic data of network and to alert the intrusions. The proposed IFS shall be incorporated with antivirus and IDS to improve the filtration process. In previous paper we discussed the basic structure of Intrusion Filtration System. The IFS is a enhancement tool for computer system to protect the circulation of corrupted file in Network. The tool can be implemented in individual system to protect the system as well the network and internet communication. The tool will generate the Token Security Code (TSC) tokens and embed with the filtered file to tag them as safe to use. The filtration system experiment is done on DARPA dataset KDD99 (1999 DARPA). The coding part of Intrusion Filtration System (IFS) designed here will combine the algorithm of Binary Decision Tree (BDT) and Pattern Counting Algorithm (PCA). The TSC code will be checked every time the file is used whether it is opened work in system or to send through email or through using USB.***

Keywords: PCA, IFS, Binary Data Tree, Token Security Code (TSC), Pattern Counting Algorithm, Network Security.

I. INTRODUCTION

Denning's presented the story of Intrusion Detection Systems (IDS) in 1981 [3,4,5]. IDS are developed to present accurate, extended and adaptive technology for network security [7,18]. Typically Intrusion Detection Systems are used to identity intrusions in system. For this filtering process a wide ranges of Intrusion detection systems are used. The functioning of IDS is based on their nature of implementation. And based on that IDS [1,2] may be classified into Host based, Pattern based, Network based and Anomaly based.

Based upon basic structure of tagging filtered files for user, in this paper we proposed a network security technique using intrusion filtration system for reducing the risks caused to vulnerabilities in the network or single alone system. The main theme of the model is explained in two sub headings-

New model of Intrusion filtration System [12] – In this section the primitives on which the model is developed and the architecture introduction is explained.

TSC code generation and tagging filtered file for use[6] - Presents in depth explanation of how the model is being developed and explains the usage of a variety of components that are used in construction of the model.

Depending on type of data they filter and database versions available with them, the nature of systems will vary from system to system. Fig.1 depicts the General Process of IDS.

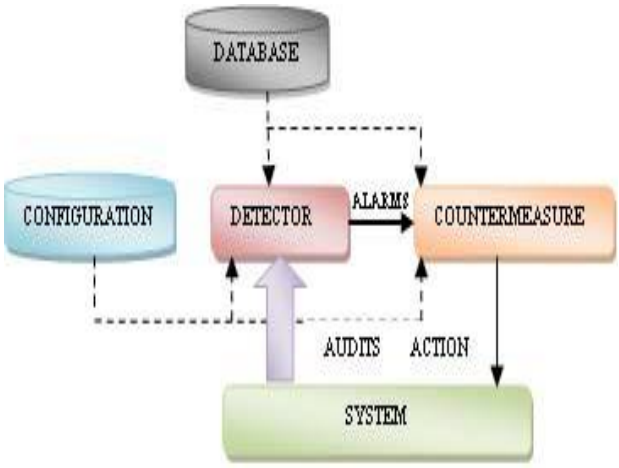

Fig.1 General Process of IDS

II. PROPOSED MODEL

II.I. PROPOSED MODEL OF IFS FOR NETWORK SECURITY

The proposed model "Intrusion Filtration System" for Computer files is being built upon these components and the basic information about the model is given below:

- A low cost security model build by using existing security components in OS.
- The Model has distinctive collection of a variety of security components to achieve a superior level of security on the Computer.
- After scanning the various antivirus products generate log files which we will used for creating Token Security Code(TSC) to tag the files and generate TSC log file. The security model explained here can be used for any Operating System.

Intrusion Filtration Systems proposed here will filter the data and tag the file with TSC code. Fig.2 explains the working process of IFS.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Dr. Marlapalli Krishna, Professor, Department of CSE, Sir C R Reddy College of Engineering, India. (marlapallikrishna@gmail.com).
V Shariff, Assistant Professor, Department of CSE, Sir C R Reddy College of Engineering, India. (shariff.v@gmail.com).
Bandlamudi S B P Rani, Obtained M.Tech from Andhra Univrsity., India. (bsbprani.425@gmail.com).
S K Chaitanya Rudraraju, Assistant Professor, Department of CSE, Sir C R Reddy College of Engineering, India. (skc.rudraraju@gmail.com).
Soni Lanka, Computer Sciences, Faculty of Science, Universiti Brunei Darussalam, Gadong, Brunei Darussalam. (karri.sony@gmail.com).

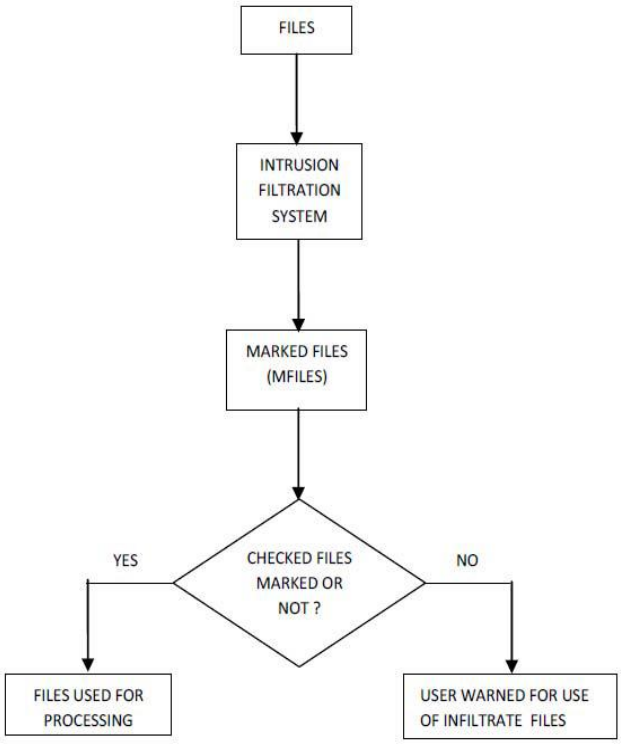

Fig.2 Intrusion Filtration System.

- The TSC log work as an Index to cross check for files whether it was tagged file with TSC code or not. The TSC log store File Name, File path, File Size and TSC associated with the file.
- The all four attributes stored in TSC log play important role and are parameters to filter the file in IFS. The TSC log is a text file and stored as system file.
- The Token Security code will use encryption method to provide better security.
- The IFS will be implemented as and security tool like other application tools. It will an extension tool for security.
- The antivirus products scan files shows the log for corrupted and uncorrupted files. They correct the corrupted files. The IFS will not work on intrusion detection [8,9] rather it work on filtered scanned files by tagging them with TSC and warn user if they are using corrupted files so that name Intrusion Filtration system [13,14].
- An antivirus service security component provides the security to this model. By doing this even when security is compromised at any level the will be shielded by the operating system security components.

II.II. TSC GENERATION AND TAGGING FILTERED FILE FOR USE

The TSC will be differ for all tagged files and it will be generated randomly consisting of a group of random characters. No two files will be tagged with same token security code. The length of the TSC will be differ in length and collection of characters. To generate TSC code total 62 characters from combination of A-Z, a-z and 0-9 and additional 3 to 4 character of file extension extracted from respective file going to be tagged, shall passed as a parameter to TSC code generation function [10,11].

The length of the TSC code is not fixed. The TSC length will be same for files of Folder or Directory mentioned in path but may vary for files of folder and Directory of different path. TSC is a secure and safe code because it will be generated randomly in a specific length, with randomly selected characters out of the collection, so it's really difficult to copy and pretend. Thus the tagged file can be separated easily on the basis of TSC. The TSC will be embedded to the file as a string.

The TSC may be placed anywhere in the file. The IFS tool requires higher end programming because it will interact directly with system files and has to interact with different applications files. The backend programming must be done using different API's by looking the various categories of extensions of files.

The provision of absorbing a new kind of files extension and importing related API's and packages shall be properly dealt in the programmer side when coding for IFS. While processing a single file TSC has to be managed twice for one file - First when embedding the TSC in file stream and second when TSC has to be checked with TSC Log before it shall be used. The flow chart of generating process of TSC is explained in next section and is shown in Fig.3.

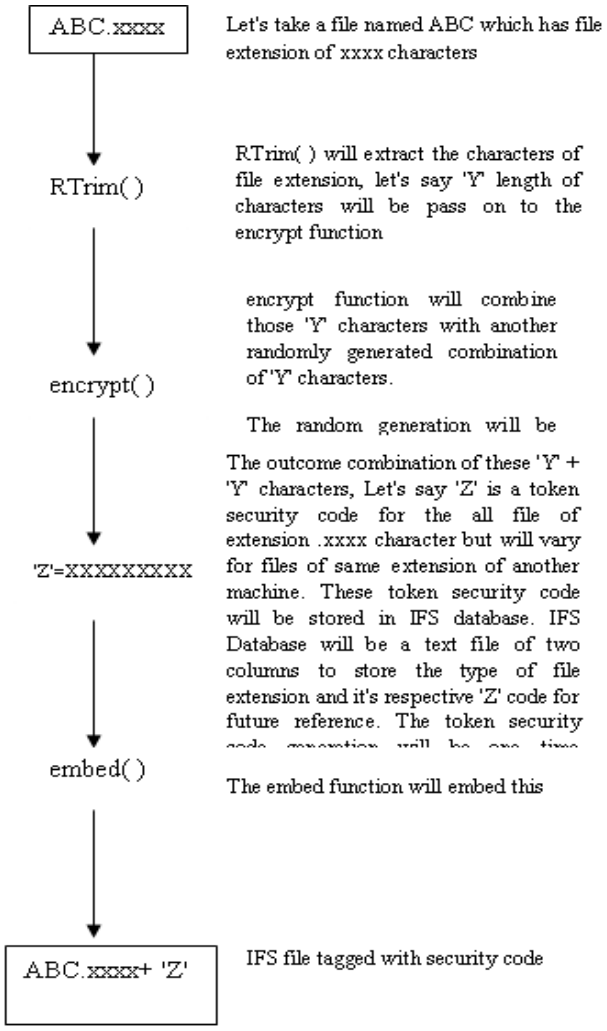

Fig.3 TSC Generation and Tagging Process

II.III. EMBEDDING TSC CODE IN FILE

The TSC will be embedded in file using buffer reader. The TSC will be embedded as string of random collection of alphanumeric characters and combination of file extension. The extension of file used here will provide extra plus point to generate a unique TSC for file. The model proposed here will read entries of all files from scan log. The location of log files may change as per the IFS installed. We will discuss all three CASES-

CASE 1: In general file directories are exclusively mentioned at a time of installation of operating system. The list of available files and folders will be read, their extension will be filtered, and TSC code will be generated and embedded to the end of every file available inside the specified path. The default TSCLOG file can be created at C drive for storing the details.

CASE 2: In case of Antivirus or with the IDS, the log file depends on the product installed and shall be read from their. The variety of Log files are maintained by the scanning software's depending upon the system and its components installed.

The log files storage location may vary depending on the OS, version and service type. Microsoft antivirus stores variety of log files –

- Client Logs
- Site Server Logs
- Wake On LAN Log Files
- Management Point Logs
- Out of Band Management Log Files
- Fallback status point log
- Network Access Protection Log Files
- Software Update Point Log Files
- Desired Configuration Management Log Files
- Mobile Device Management Log Files
- Operating System Deployment Log Files
- WSUS Server Log Files
- Software Updates Client Computer Log Files
- Windows Update Agent Log File
- Power Management Log Files

In case of Microsoft we have to work with Fsinvprovider.log (in all SMS 2003 Service Packs it was renamed as FileSystemFile.log), Windows Management Instrumentation (WMI) provider for software inventory and file collection.

In case of Norton Antivirus, the log file can be read from history of files can output can be stored in text file by using following-

Open Norton
click on "History"
choose "Scan Results"

Use cmd move to the path of this folder: C:\<Somewhere>\Norton Antivirus\Engine\<Version_Number>

Use this comand to scan a file or a folder: Navw32.exe <path to scan>

This comand will make you a log file: MCVI32.exe /export <log path> /category <category number>

In McAfee products the log file are located in different locations based on the Operating system installed.

For Windows 7 and later:

The log files are located in C:\ProgramData\Mcafee\Managed VirusScan\Logs

For Windows XP, Vista and earlier:

The log files are located in C:\Documents and Settings\All Users\ApplicationData\McAfee\Managed VirusScan\Logs.

Available log files include the following:

- myAgent.log
- myNotices.log
- myUninstall.log
- myUpdate.log
- myInstall.log

In latest, specific software tools are also available to maintain the log files. For example SpaceObServer can enable us to export the details of scan in customized format (Fig.4). Few log tracking software names mentioned below -

- Logentries
- DxSoft
- File Viewer Plus
- techradar.pro
- Microsoft System Center Configuration Manager 2007.

Fig.4. Software tools to observe Log files

II.IV. CHECKING OF TSC IN FILES

In IFS when user initiate a request for accessing a file, before it get opened for work the availability of tag TSC will checked with TSC log. The Filename received from user to open shall be passed to the searchTSC( ) method to first check the name of file in TSC log, after than if file name found in TSC log the data stream of file will be checked for TSC tag as a String. If both filename and TSC found and matched for respective TSC log of file, the user allowed to access for file [15].

CASE 1 - DATA ACCESSED IN SAME SYSTEM BY USER

In this case the on selection of file by user to open it through thread generated by user process, the details will be cross check in TSC log and if found, the file will be simply open without any intervention of IFS. If the entry of file going to access not found in TSC log, user of that file will be warned with message that the file is not safe for use.

In case user agreed to still access the file will be allowed for user access [16].

CASE 2 - DATA ACCESS THROUGH REMOVAL OF PORTS FROM SYSTEM AND VICE-VERSA

Here in this case before shifting data, the selected content of file will be buffered and stream of buffer will be checked for TSC code.

To find the TSC pattern the TSC code is searched in the data stream of the file.

The file is allowed to copy in removable disk only when the founded TSC code in the file stream is equal to the TSC log.

Suppose if TSC code is not founded then the user is notified for unfiltered file access. And also he will get a warning for the verification whether he desires to access such type of files. The files will be copied to the removable disks if the user wishes to access such files.

In reverse process prior to copy of file in the system data coming from port is checked fpr TSC code in the data stream of file name. The copying process is accomplished only when TSC code is found otherwise the process is roll backed to its original state and a caution message be publicized to the user for access of unfiltered file [17].

CASE 3 - DATA ACCESS FROM INTERNET TO SYSTEM

In this whenever a user downloads data from Internet the following process of steps will be followed.

- The data will be downloaded into the default folder.
- The content of downloaded file is intended for a scan by IFS.
- The scanned file is tagged with TSC if data is found clean and uncorrupted.
- A caution message is raised to user for malicious content if the scanned data found to be corrupted. And user was recommended to remove the file or folder.

III. IMPLEMENTATION OF IFS

The Intrusion Filtration system process in following steps -

Step 1 - The antivirus invoked by IFS to scan the computer files.

Step 2 - The log file will be fetched and the list is separated of safe files and unsafe files.

Step 3 - TSC code generator creates TSC by using randomization method. TSC code will be a random generated code, combination of A-Z, a-z, 0-9 and the extensions of respective files. TSC code will be unique. No two TSC code will be same.

Step 4 - The TSC code will be tagged to the scanned safe files and tagged as TSC file. A TSC log will be generated to store the details of tagged file for future use. File name, File size, File path and embedded TSC code details is stored in TSC log.

Step 5 - Whenever any new file stored in system, the process from Step 1 to Step 4 will be executed before TSC log update.

Following are the screen shots of model programming code-

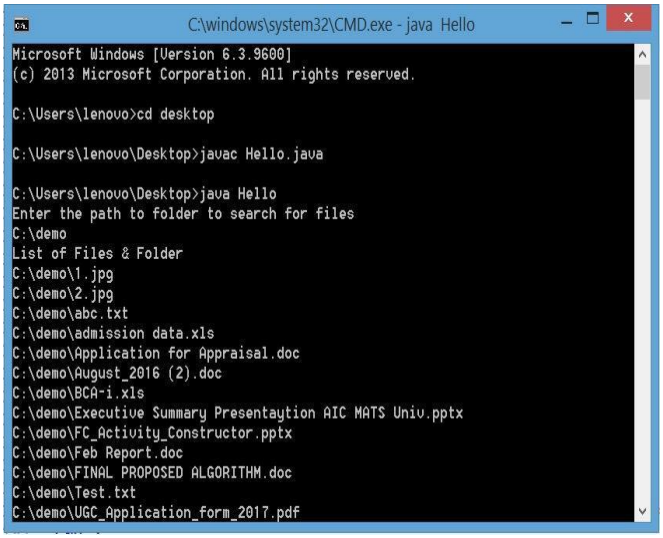

Fig.5. Listing of F files from Directory

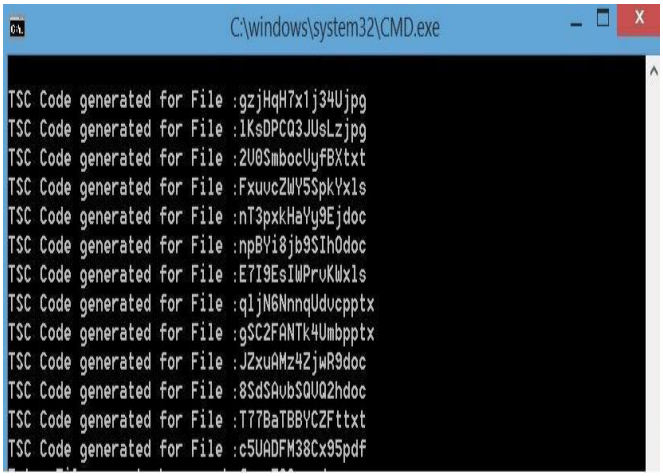

Fig.6. FigGeneration.7.erationofTokenof TSCSecurityfor FilesCode (TSC)

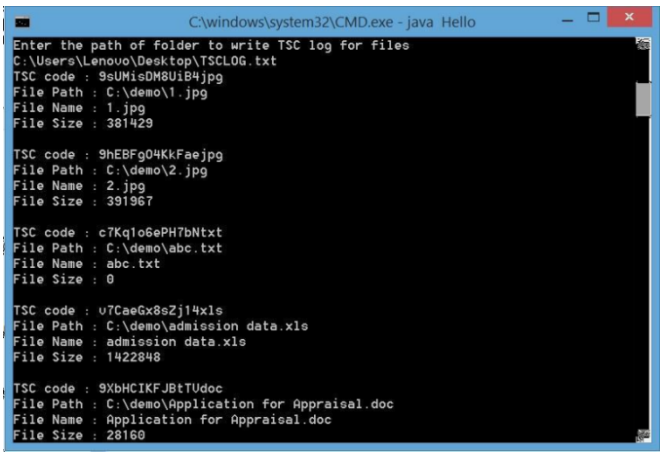

Fig.7. TSC Log File entry.

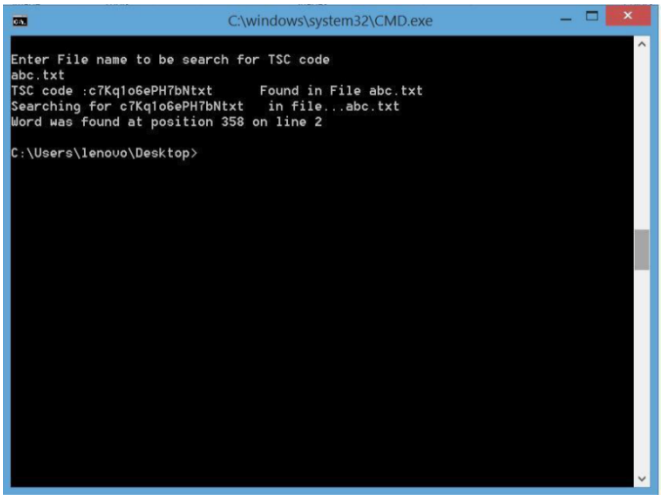

Fig.8. Checking TSC in File

III.I. SECURITY LEVEL I - TSC CHECK

- When user select any file for access, on select event a process to check whether the file is TSCfile, get executed.
- TSC code will be checked with the TSCLOG.
- If TSC code found in the file, the user can access the file in normal procedure.
- In case if file is not found in TSC log a warning message is to be shown to the User that file is not a TSC tagged file.

III.II. SECURITY LEVEL II - FILE SIZE CHANGES THROUGH SYSTEM GENERATED THREAD ( )

When file accessed by user thread and any changes made to the file the entry will be updated of TSC logfile. The file entry will be updated after file go through the step 1 to 4.

- When file accessed by system generated call( ) by any application tools without user generated process thread, while updating the log if any changes found in the file size a new entry will be made in TSC log.
- When user tried to access such modified file in same location, A message will shown to user that it was modified by system generated thread and option are given to the user whether they want to access the previously stored TSC file and discard the entry at TSC log of this system thread generated file and pool out from safe files. The change in file size is notable because file size is stored in bytes.

III.III. SECURITY LEVEL III - FILE PATH CHANGES THROUGH SYSTEM GENERATED THREAD ( )

- When file accessed by user thread and any changes made to the file path will be updated of TSC log file. The file entry will be dated after file go through the step 1 to 4.
- When file accessed by system generated call( ) by any application tools without user generated process thread, while updating the log if any changes found in the file path a new entry will be made in TSC log.
- When user tried to access such modified file in same location, A message will shown to user that it was modified by system generated thread and option are given to the user whether they want to access the previously stored TSC file and discard the entry at TSC. log of this system thread generated file and pool it out from safe files. The change in file path is notable because file path is stored.

The system can be used in both Client machine & Server machines and implemented even in offline mode. IFS is a Intrusion Prevention System (IPS) and will restrict the user from accessing the files which were corrupted. The IFS is platform independent and simple to implement. Because of its automatic update of TSC log through the system, no specific additional maintenance is needed.

IV. ADVNTAGES OF IFS

The concept of IFS is based on working the uncorrupted files. We are by using IFS neither trying to detect Intrusion nor focusing on identified intrusions. The focus is to use scanned and filtered files so that the corrupted file should not get in channels of network and hence to create a safe environment. In comparison for cost efficiency the IFS won't require big space and so the cost effective. If implemented with operating system the IFS will be very effective tool to create a safe environment of working. It has less maintenance requirements. Once installed it will work like other features of operating system without creating complications.

IV.I. ADVANTAGES OVER ANTIVIRUS

The Antivirus software designed to track, quarantine and remove corrupted files from system. The viruses are playing very smartly and now days designed in such a way so that they travel easily to one computer to another across the Internet. The network virus programs are deliberately designed to infect the user or system files and thus to create a damage to the data. IFS and Antivirus both will be self initiator to work with but IFS is not a replacement of Antivirus software rather it is a tool which will extend the efficiency of antivirus software hence the performance of system.

IV.II. ADVANTAGES OVER IDS

IDS works on algorithms to detect the intruders through various methods as explained in the chapter I and Chapter II, whereas IFS works with filtered file. The working performance and cost of implementation is comparatively very less.

IDS need more monitoring and intervention for processing in comparison with IFS. IFS will be a self initiated tool which will work all across the duration till the computer is in on condition without requiring any intervention once it was installed.

V. LIMITATION OF IFS

The following are the limitations of IFS

- The performance of IFS will be limited to the capacity and performance of available antivirus or IDS in computer system.
- The strong the antivirus protection, better the performance of IFS.
- The frequent up gradation is required to cater the diversity of new file extension.

- The Antivirus or IDS changes may need path setting and environment variable settings to be changed to extract the Log files of system.
- The financial implication will be one time only at the time of emergence at professional level
- Up gradation packages may require financial implications if charged by subscriber company.
- The IFS implementation can be done as a patch tool of antivirus, IDS, default utility program with operating system or separate utility program.
- The higher end programming implementation is required to be integrated with OS.

VI. CONCLUSION

With the increased usage of internet, the hackers are inventing new threats almost on every day. To provide some extent of security IFS focus on circulation of filtered files and by not using the corrupted files. IFS provide the network security by stopping the circulation of ruined files through removal disks and through internet as attachment. We tried here to explain all aspects and discuss its performance. The different types of IDS are explained here with all their advantages. After deploying firewall technology in network the IDS are also becoming next logical step for many organizations at the network perimeter. By proposing IFS we are trying to avoid the use of corrupted files and subsequently their distribution in the network.

VII. FUTURE WORK

The model proposed here requires higher end programming in order to get implemented in operating system. The code done here to show the processing of IFS is working with Text files only. To start the IFS all initial API packages must be implemented in back end programming so that different files can be accessed regardless of their type i.e. extension of file, TSC can be easily embedded and traced whenever required. Thus the actual implementation part of this research work is still left. Although it can be offered as utility program also but implementation with OS as an compulsory feature will be the best option to create a safe environment for user to work.

REFERENCES

1. Rita Dewanjee “Intrusion Filtration System(IFS)- mapping Network Security in new way” , IEEE, 26 June 2017, 10.1109/ SCOPES.2016.7955883,978-1-5090-4620-1, http://ieeexplore.ieee.org /abstract/ document/7955883/
2. Rita Dewanjee, Dr Ranjana Vyas, " A Study on IDS (Intrusion Detection System) and Introduction of IFS (Intrusion Filtration System)", Computing and Network Sustainability, Lecture Notes in Networks and Systems book series (LNNS, volume 12), Springer, Singapore, 06 July 2017, pp 119-126, 978-981-10-3935-5.
3. Kothapalli Chaitanya Deepthi, Dasari Ashok and Dr M Krishna. “A multi Ability CP-ABE access control scheme for public cloud storage”, International conference on computer vision and machine learning, IOP Conf. Series: Journal of Physics: Conf. Series 1228 (2019).
4. V Pranav, P Satish Kumar and Dr M Krishna. “Performance study of cloud computing for scientific applications”, International conference on computer vision and machine learning, IOP Conf. Series: Journal of Physics: Conf. Series 1228 (2019).
5. M.Ghassemian: Analysis of an Anomaly-based Intrusion Detection System for Wireless Sensor Networks. In: *International Journal of Computer Applications (0975 – 8887), Volume 28– No.7,* August 2011.
6. K Purna Prakash , Dr M Krishna and M Satya Vijaya. “Data productive collaborative filtering using deep learning based recommender model”, International conference on computer vision and machine learning, IOP Conf. Series: Journal of Physics: Conf. Series 1228 (2019).
7. Krishna M., Chaitanya D. K., Soni L., Bandlamudi S.B.P.R., Karri., R.R.: (2019), "Independent and Distributed Access to Encrypted Cloud Databases". In: Omar S., Haji Suhaili W., Phon-Amnuaisuk S. (eds) Computational Intelligence in Information Systems. CIIS 2018. Advances in Intelligent Systems and Computing, vol 888. pp 107-116, Springer Nature. DOI: 10.1007/978-3-030-03302-6_10.
8. Sri Krishna Chaitanya Rudraraju, Nakka. Desai, M. Krishna and Bandlamudi S. B. P Rani. “Data Mining In Cloud Computing: A Review”, Journal of Advanced Research in Dynamical and Control Systems, pp: 1198-1207, Vol-9, Issue-18, 2017.
9. V. Jyothsna, A.Rangampet, V. V. Rama Prasad: A Review of Anomaly based Intrusion Detection Systems, International Journal of Computer Applications 28(7):26-35, August 2011.
10. M. Krishna et al., “Alignment Establish Representative Data Uploading and Private Data Principle Test in Cloud”, International Journal of Research in Electronics and Computer Engineering (IJRECE), pp: 132-135, Vol.5, Issue.4, Oct-2017.
11. Y Leela Sandhya Rani , M.Krishna and Shaik Nusrath Jahan “Closeness: An Advanced and Effective Measure for Data Publishing”, International Journal of Research in Electronics and Computer Engineering (IJRECE), pp: 184-189, Vol.5, Issue.4, Oct-2017.
12. Evaluating-intrusion-detection-systems-and-comparison-of-intrusion-detection-techniques-in-detecting, http://www.intechopen.com.
13. Manda Pradeep Chandra, Marlapalli Krishna and Prathipati Ratna Kumar. “Better Message Transmission Solution in Steganography”, International Journal for Research on Electronics and Computer Science, pp:5500-5504, Vol.07, Issue.2, Nov-2016.
14. Bandlamudi S B P Rani, Dr. A. Yesubabu and M. Krishna. “Data Encryption Using Square Grid Transposition”, International Journal & Magazine of Engineering Technology, Management and Research, 2(11), pp: 71-75, Nov-2015.
15. G. Jacob Víctor , S. Rao Meda, V CH Venkaiah: False Positives in Intrusion Detection Systems. In http://www.academia.edu, 2010.
16. K Koteswara Chari and M Krishna. “An Efficient Scalable Data Sharing in Cloud Storage Using Key Aggregate Encryption”, International Journal of Science Engineering and Advance Technology, 3(11), pp: 945-946, Nov-2015.
17. D Paul Joseph, M Krishna and K Arun. “Cognitive Analytics and Comparison of Symmetric and Asymmetric Cryptography Algorithms”, International Journal of Research Studies in Computer Science and Engineering (IJRSCSE), 2(3), pp: 63-68., Mar-2015.
18. Kaur, S. Kaur: Comparative Analysis of Anomaly Based and Signature Based Intrusion Detection Systems Using PHAD and Snort. In: Proceeding of Security and Privacy Symposium, Feb 28 to March 2, 2013.