ISSN 2278-3091
Volume 10, No.2, March - April 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse1261022021.pdf
https://doi.org/10.30534/ijatcse/2021/1261022021

Comparison of Signature Based Techniques

Taha Nuzhat[1], Ammar Oad[2*], Mir Sajjad Hussain Talpur[1], Hina Rehman[1], Abida Luhrani[1], Akhtar Hussain Soomro[1], Raheel Sarwar[1], Shakir Hussain Talpur[1], Erum Saba Chang[1], Gaofeng Luo[2]
[1]Information Technology Centre, Sindh Agriculture University, TandoJam, Pakistan,
mirsajjadhussain@sau.edu.pk
[2]Faculty of Information Engineering, Shaoyang University, Shaoyang 422000, China,
ammar_2k309@yahoo.com

ABSTRACT

A huge amount of research is being done on web-based attacks, and as a result, many security mechanisms have been introduced. But, due to their very flexible nature, they are not as effective in the defense of attacks as they should be. Therefore, the proposed system designed an effective web security system that can detect attacks using digital attacks of signature. This system will be able to use modern signature-based technique for demonstrate information and it will be deployed on crest of the Visual Studio framework. An application layer attack, such as a Trojan attack, will be detected and protected by such a system. We are optimistic that such a system would work and demonstrate a better signature-based system, which will be compared to Avast.

Key words : Intrusion detection system, Structured query language (SQL), Cross Site Scripting

.

1. INTRODUCTION

Electronic business, electronic health and many other web implementations are constructed on the Internet. Many individuals use web applications; therefore, internet utilization is renowned. Many of these vulnerabilities and defenselessness are vulnerable to attack, such as XSS and SQL injection [1],[12] and Trojan horse attack. The current world has entered the information era with the development of computer networks, while the internet has become indispensable in life, work, and study. However, virus attacks have become increasingly popular because of the development and strengthening of the internet. Various attack methods greatly threat the proper security of human beings [13]. For many companies and individuals, Trojans have eventually become actual coercion for more than ten years. Statistics taken into custody contrary to network Security display that three sorts concerning significant protection events are frequently announced (i.e., deceit, infiltration, and malevolent code). Trojan horse exploits not only system vulnerability but also the system user's vigilance [14].

Trojans have been improved and ranges of sophisticated techniques have been integrated, which makes the detection processes much harder and longer than in the past. Lack of understanding and knowledge and proper procedures of the Trojan analysis have led to money loss, reduced productivity and tarnishing of the organization's reputation [1]. Many organizations and computer users have been facing problems because of the real threat of Trojan horses for more than a decade. There are three major security incidents mostly reported. These are malicious code, intrusion, and fraud, which are taken from the statistics of cyber security [2]. Although the Trojan research was started by [3]. Later than 11 years afterwards, research was conducted like [4],[5]. However, this works better by concentrating on hardware taxonomy and hardware detection techniques. During the past few years, many methods have been proposed for the detection of Trojan Horses. However, most of the methods are focused on hardware Trojans, worms, and malware. Few works have specifically targeted software Trojan Horses [6].

To detect Trojan theft activity used an algorithm which is based on timestamp-based data stream clustering [7]. In that research the clusters are used to compact communication facts stream knowledge based on the Trojan attack and extract the characteristics of clusters to detect the Trojan attack. This research is based upon experiments. lower false negative rate and 90% accuracy rate. However, theft capability is only the focus of this research work. Another detection method which is called Portable Executed (PE) file static attributes a new detection method which was presented by [8]. To analyze the static attribute in the Portable Executed (PE) file, an intelligent information processing technique is used. The test rate showed 63.90% result of the experiment. If the bigger volume of dataset is involved, the result of the experiment is improved.

Nowadays, there is so much information about vulnerabilities and exploitation in operating systems and applications, attacks, and defense technologies. Though information regarding these widely distributed and different defense technologies have been implemented, many organizations are constantly being attacked and exploited by malware such as worms and Trojans. Nowadays, computer network systems are more threatened by Trojans. This is

mostly true for Windows systems because there are large numbers of Trojan horses designed to enable attacks upon running Windows platforms [9],[10],[11]. Dissimilar defense appliances are less efficacious in opposition to the internet-based risk. Protection is needed to reduce the attacks of the application layer. The increase in the number of anti-virus making companies and the requirement for regular update of anti-malware software in computer systems is proof that a bigger effort is still needed in order to find a stable and lasting solution to the detection of attacks. Hence, we introduced a tactic at the application layer for diagnostic attacks. At the application layer, by utilizing this technique, the system will be proficient at identifying the attack. At the application layer, many kinds of attacks have been detected which are related to such types of attacks. The present protection system is particularly based on diagnosing the Trojans. Trojans are a dangerous threat to system protection. The Trojan is an authorized software which possesses toxic data. These attacks may be linked with games, photographs, MP4s or melody. The virus Trojan gets into the user's system when a movie, email or song is downloaded. In current research, an approach is utilized for detection of attacks which consists of signatures of attacks. For security purposes, present protection systems do not continually monitor and analyze network packets individually because of high false positive rates. These are ineffective in mitigating application layer attacks.

This research recognizes Trojan horse attacks in order to create the signatures of the Trojan attack's application layer. Analyze signature-based techniques with Avast and Kaspersky anti-virus software in sequence to determine the standards for selecting the best solution, as well as the designed technique.

2. LITERATURE REVIEW

2.1 PREVALENT IDS TO IDENTIFY COERCION

2.1.1 SIGNATURE BASED INTRUSION DETECTION SYSTEM

The Signature based detection technique is a traditional, uncomplicated, and well-organized method for detecting attacks. The Signature-based intrusion detection system provides solutions to count the increasing number of attacks on network resources. Signatures are typically a sequence of bytes within the malware code to detect that a program scanned is a malware or not [13]. A Signature based detection system is also known as string scanning and is thought to be the simplest form of scanning [14]. Signature based detection detects the attack by probing the particular sequence of bytes contained by an object to recognize a remarkably scrupulous version of the attack [15]. Furthermore, identified as sequence of character analysis, this is the uncomplicated shape of analysis. An attack is recognized through its sequence of bytes and which is known as an attack signature. Within accumulation, a hash value is one more kind based on signatures. A single value is the combination of a large amount of data with the help of procedure or mathematical function [16]. This technique scans the files for the attack's signature. Signature resembles the instruction pattern or specific string of bytes from an attack code. Signatures can be extracted by probing disassembled code of attack. Antivirus developers have to see the attack signature pattern from the attack code. If a new attack comes, then the developer has to analyze the infected file to come across its signatures. After collecting attack signatures, a signature database is created to aid in attack detection.

Signatures of before now known attacks are contained by the Signature Base System [17]. At the application layer and at the network layer, scrutinizing network transfer & server logs are able to be produced [18]. To remove the threats, signatures are worthless. It is difficult to advance a database which is messy & time overwhelming function in the direction of signature command which faces continuously growing context-based implementation. IDS deficiency invulnerability opposed to zero days & countenance hurdle about signatures by hand .

2.1.2 DATA MINING OR STATISTICAL BASE IDS

Although the framework employed in data mining is steeped in statistical technique (Xiao-Fang Wang et al., 2005). yet it is unable to deal with the issues as it fails to analyze malicious payloads. This is because it lacks semantics and therefore cannot take the contextual nature of the data into account and deals only with the character frequency[16].

2.1.3 ANOMALY BASED IDS

This system simply clarifies an abnormal activity as malicious by making it with a certain established profile [17]. On the contrary, the protection of data collection server in 2006 in the vicinity of SQL injection threats anomaly-based IDS was developed. Detection staging was minimized through that model in such research work. Though it is effective in pinpointing attacks, the false positive rate is equally elevated.

2.1.4 ONTOLOGY BASED DETECTION SYSTEM

The first and the foremost work was done by Under Coffer, Joshi, Pinkston in the paper "Modelling Computer Attacks: An Ontology for Intrusion Detection" [18]. Who defined the attacks, their location as well as their consequences? Around 4,000 classes were analyzed on the ontology base. The second study analyzed the relation between the master nodes and the child nodes through ontology [19]. Another study related to ontology supported outbound intrusion detection system. It actually involves the agent organization. The cells in this case work entirely on their own, thanks to the use of nonhierarchical agent structures [12]. The research employs a heterogeneous integrated intrusion detection system with Raw alarms [13]. Data processing makes use of ontology based intrusion detection systems by way of solving the

problem [14]. Ontologies of web resources for data integrity have expanded [15]. In the domain of the intrusion detection system at the network layer, sufficient research work has been done [16]. Although in a normal state of affairs, it is the statistical technique which is used to detect anomalies, but they too are found to be lacking and unable to deal with certain problems when the problems are created by the juxtaposition of various fragments[17]. This is because the techniques lack contextual nature. For data integrity of web sources, ontology has also been developed [18]. Ontologies for control access were also created [19]. In data processing, complicated attacks, ontology based detection systems are used, but they too are not able to deal with [20]. They take a better approach, but they are entitled to a scarcity as a result of this space-saving method of solving the problem and because it ignored internet-level attacks such as SQL attacks and XSS.

2.2 PREVALENT METHOD VS SUGGESTED METHOD

2.2.1 SECURE SPHERE

It protects against database breaches, enterprise data centers, worm infection, and service attacks, worms, data theft, and SQL injection detection.

2.2.2 DRAW BACK

There are two major drawbacks to the secure sphere. The first one is not being able to take into account the problems based on semantics and the other one is the high rate of zero-day attacks.

2.2.3 SNORT

This is able to detect protocols that are inversely flexible by analyzing IP traffic through the use of signature-based detection, content searching and also analyzing the data by matching it. Other pros of Snort include its integratibility with various applications and work at firewall level.

2.2.4 CONS

First and foremost, it is manual in nature, has the issue of flood alerting, and the security expect must be proficient in semantics.

2.2.5 AVAST ANTIVIRUS

Avast was founded in 1988. Avast is an anti-virus program that detects and removes attacks from your computer or removable storage device. Avast is free for non-commercial use, such as on a personal computer. Avast uses the method of detecting an attack through scanning or it can detect attacks online or when the user is surfing the internet. Scanning can be done in several ways. Avast can scan a system to detect an attack. There are different types of scanning. Avast can be used to detect an attack.

(1) Quick Scan (2) Full System Scan (3) Removable Media Scan (4) Select folder to scan

(5) Boot time Scan

2.2.6 QUICK SCAN

With the help of this option, we can quickly scan an entire system, detecting only the most vulnerable files. In this state, we can scan a system quickly.

2.2.7 FULL SYSTEM SCAN

With the help of this option. Avast can scan a full system, any drive of the system, particular folder, all hard drive and rootkits. All files are checked according to their content.

2.2.8 REMOVABLE MEDIA SCAN

In this scan option, Avast can remove all removable media that is currently attached to the computer. (for example, flash drive and hard drive).

2.2.9 CHOOSE A FOLDER TO SCAN

Completes a full scan of a specified folder. Scans only a specific folder or multiple folders.

2.2.10 BOOT TIME SCAN

It performs scanning at boot up time means at the time of starting of the computer. Avast can detect a virus. Avast can also detect an attack online when a user clicks on email to check email provided if a Trojan link is attached with a file, then Avast can detect an attack.

2.2.10 KASPERSKY ANTIVIRUS

Kaspersky is an Antivirus. Kaspersky was founded in 1997. It can detect attacks at running time or online when a user is surfing the internet and can detect attacks when access to the internet is not present or when the system is not connected with the internet. The following actions can be performed by Kaspersky antivirus when an attack is found.

(1) Disinfection (2) Delete (3) Skip (4) Block Access

With Kaspersky antivirus, one can detect the attack by scanning the whole system or a drive or a folder or a simple file. Kaspersky uses the signature-based technique. Through Kaspersky antivirus, one can scan the entire system. We can scan the whole drive or a particular folder. We can also scan a particular file. When the virus is found, Kaspersky can disinfect the file. Disinfection means before deletion of a virus it first backs up the file, then it will delete the attack.

Before disinfection, it makes a copy or backs up the object or file, then it deletes the attack. The second action which can be performed by Kaspersky is deletion of the whole file with an attached attack. Because if disinfection is not possible, then

Kaspersky can delete the file, because at this stage it will not copy or back up a file.

At this stage, it will just delete the whole file with an attached attack. It will not separate the attack from the file. The third action that can be done by Kaspersky is skipping the file. It will not perform another action. It will simply evict the file. Another action that can be performed by Kaspersky is the block access, which can be blocked to access the infected file or object. But it will not disinfect or delete the file. It will only log the information about the attack.

3. METHODOLOGY

The sole objective of this research is to upgrade the process that increases the protection of internet applications. In such a system, there is a security system for attack detection. Signature based technique is deployed here. Through this, the system can detect attacks using signature-based technique. The system utilizing signatures performs better in detection of HTTP requests and it would detect Trojan horse attacks based on the prevailing technique. The solution works on packet level check through understanding the nature of HTTP request. The request of the user http is observed in a prominent way that lowers the false positive rate. When a user sends a request, the analyzer tool parses the request and checks if the request is legitimate or not. Following that, condition patterns are checked and matched from knowledge, and the request is then changed to another security level of signatures. The user's behavior is analyzed to determine whether it is normal or abnormal, and whether the request carries any extension of the existing pattern in attack signatures, after which the system remains alert. Whereas the consistencies, attributes and classification of attacks are in a simple way. The given system will be manipulated in any organization's internal work as an antivirus program. Their entire request will be forwarded to the real server or the system will block it.

3.1 SYSTEM ARCHITECTURE

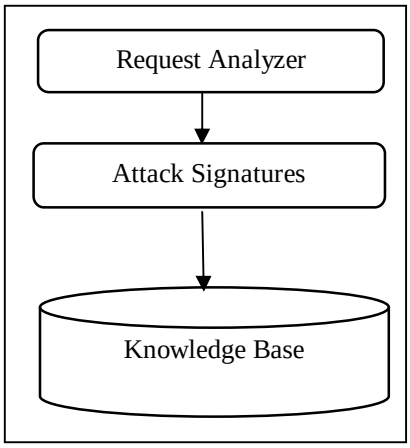

Figure 3.1: System Architecture

3.2 REQUEST ANALYZER

The 1st segment of the setup is request analyzer. The objective of Request Analyzer is to deconstruct the user request on the ground of signature edicts created by the knowledge Base and construct determination if the requisition is benevolent or spiteful. Later deconstructing the user requisition, it constructs determination if the requisition has the benevolent code or not. If requisition has malevolent code then fault is produced.

3.3 ATTACK SIGNATURES

The attack signatures as shown in figure iii-xi have many signature-based representations of malicious input, policies, and rules. The malicious content may be injected on web application usually injected from port 80. Some rules and policies can mitigate these attacks in efficient way.

1. The check of signatures, consistency and data format must be done .
2. Syntactic restriction must be performed on length, input value and on input field.
3. Extra check must be performed.

3.4 ERUDITION BASE SYSTEM

It includes information about attack encoding techniques, attack categories, system affected part, rules/polices for attack mitigation. Evaluator and Erudition base are foremost elements of the prototype as represented in Fig III-XI. Erudition Base is previously owned through to construct signature based on bashing & the evaluator which evaluates the data on the foundation of signature of attack. Evaluator constructs determination which secures data along with functional implementation is malevolent and also with that is not.

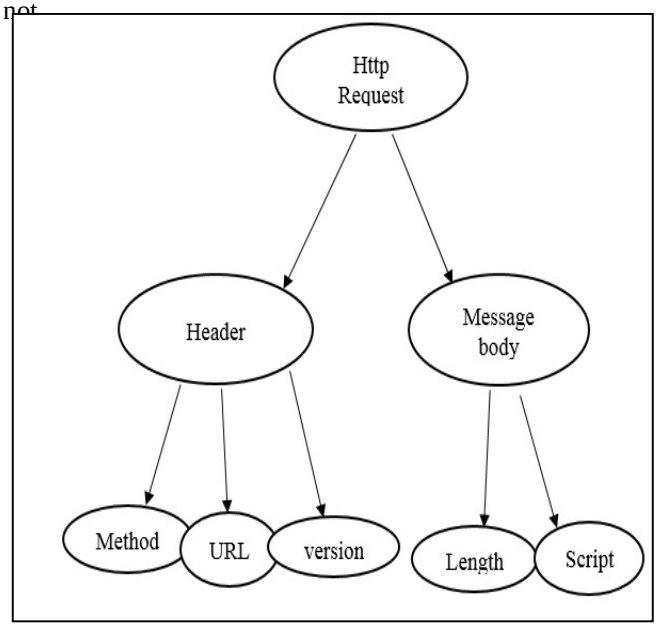

Figure 3.2: Http Signature Based Request

Figure 3.2 represents the requisition scenario. This scenario represents the interaction between web server & web browser. The requisition is pushed through web server. It approaches requisition into organization regarding query to receive knowledge in contrast aimed at erudition base. At that moment this consequently hurls answer especially for the web browser.

4. RESULTS

To aim at design and implement a signature-based detection technique implemented in software named "Trojan Detector", its result was compared with Avast and Kaspersky antivirus. The above-mentioned software will be compared in terms of time consumption, memory consumption and accuracy of the software online and offline.

All the given parameters are compared through these softwares individually with the following given file types and their sizes.

1 Images, Audios, Texts, Zips and Games.

2 10 MB, 20MB, 100 MB, 500MB and 1GB.

3 The system can scan different types and sizes of folders.

4 There are approximately 11 different types of Trojans available, the one that we have used is downloadable Trojan.

The accuracy of the system has been measured in terms of true positive, false positive , true negative and false negative.

True Positive:
It is a state in which there is an attack and system can also detect an attack.

False Positive:
It is a state in which there is no attack but system caan erroneously detect an attack.

True Negative:
It is a state in which there is no attack and the system cannot identify an attack.

False Negative:
It is a state in which there is an attack but the system cannot detect an attack.

The result was received through the use of Trojan detector and other antivirus on different machines of same specification.(Duel core).

For online Trojan detection a file was taken having Trojan virus and sent an email to someone and then Trojan detector was activated and downloaded that file and the Trojan detector detected the virus in that file. The number of Trojans that have been put in these files differently. In starting it scanned different file sizes by using Avast antivirus offline and then online, Scanned the documents through offline mode with 10MB folder which possessed 20 files and 8 viruses. Second one is 20MB folder which comprises of 40 files and 25 viruses. Third one folder is 100MB which consists of 60 files and 40 viruses .Fourth one folder is 500MB that contains 120 files and 80 viruses. And the fifth one which is the last folder that is of 1 GB has 170 files and 120 viruses. In the result found that the accuracy factors were true positive, false positive, true negative and false negative. When 10MB folder used then values are found 10, 6 ,5 and 7 .In the 20 MB folder then values are found 17,4,1 and 3.In the 100 MB folder then values are found 50,6 ,8 and 7.In the 500 MB folder then values are found 5 ,5 ,4 and 3 respectively.

Table 4.1: Accuracy of Avast by folder size

S.#	Folder Size	True Positive	False Positive	True Negative	False Negative
01	10 MB Total Number of files(20) virus(8)	10	6	5	7
02	20 MB Total Number of files (40) virus(25)	17	4	1	3
03	100 MB Total Number of files (60) virus (40)	50	6	8	7
04	500 MB Total Number of files (120) virus (80)	5	5	4	3
05	1 GB Total Number of files(170) virus (120)	1	2	7	1

After that files of different sizes were scanned by using Kaspersky antivirus offline and online, scanned the document through offline mode with 10MB folder which has 20 files and 8 viruses. Second one is 20MB folder which has 40 files and 25 viruses. Third folder is 100MB which has 60 files and 40 viruses. Fourth folder is 500MB which has 120 files and 80 viruses. And the fifth one which is the last folder which is of 1 GB and has 170 files and 120 viruses. In the result found that the accuracy factors were true positive, false positive, true negative and false negative. When10 MB folder used values are found 8,10,9 and 7.When 20 MB folder used values are

found 16,4, 3 and 7.When 100 MB folder used then values are found 28,2,4 and 15.When 500 MB folder used then values found 68,7,4 and 12.In the last when 1 GB folder used values are 99,1,4 and 15.

Table 4.2: Accuracy of Kaspersky by folder size

S. #	Folder Type	True Positive	False Positive	True Negative	False Negative
1	10 MB Total Number of files(20) virus(8)	8	10	9	7
2	20 MB Total Number of files (40) virus(25)	16	4	3	7
3	100 MB Total Number of files (60) virus (40)	28	2	4	15
4	500 MB Total Number of files (120) virus (80)	68	7	4	12
5	1 GB Total Number of files(170) virus (120)	99	1	4	15

Finally, the files of same sizes were scanned by using Trojan detector offline and online, the documents were scanned through offline mode with 10MB folder which has 20 files and 8 viruses. Second one is 20MB folder which has 40 files and 25 viruses. Third folder is 100MB which has 60 files and 40 viruses. Fourth folder is 500MB which has 120 files and 80 viruses. And the fifth folder which is the last folder which has 170 files and 120 viruses. In the result found that the accuracy factors were true positive, false positive, true negative and false negative. When 10MB folder used values are found 10,8,10 and 11. When 20MB folder used values are found 18, 7, 6 and 9. When 100MB folder used values are found 30, 5,7 and 21.When 500MB folder used values are found 78,6 ,5 and 20.When 1 GB folder used values are found 102, 9, 9 and 18.

Table 4.3: Accuracy of Trojan horse attack by folder size

S.#	Folder Type	True Positive	False Positive	True Negative	False Negative
01	10 MB Total Number of files(20) virus(8)	10	8	10	11
02	20 MB Total Number of files (40) virus(25)	18	7	6	9
03	100 MB Total Number of files (60) virus (40)	30	5	7	21
04	500 MB Total Number of files (120) virus (80)	78	6	5	20
05	1 GB Total Number of files(170) virus (120)	102	9	9	18

After that the number of Trojans that we have put in different way in these files. In the beginning different types of files were scanned by using Avast antivirus first through offline and then online mode. The documents were scanned in offline mode of type JPEG of size 10MB which contained 18 files and 15 viruses. Second folder of type songs of 10 MB which contained 24 files and 120 viruses. The third folder of type games of size 10MB which contained 12 files and 8 viruses. The fourth folder of type zip of size 10MB which contained 4 files and 2 viruses. In the result found that the accuracy factors are true positive, false positive, true negative and false negative. When the type of JPEG folder used values are found 9,8 ,6 and 8. When Songs file used values are found 20,1 ,4 and 5. When text files are used values found 30,5 ,2

and 10. When games file used values are found 70, 5, 5 and 10.When zip file used values are found 110,6 ,1 and 10.

Table 4.4: Accuracy of Avast by using different folder type

S.#	Folder Type	True Positive	False Positive	True Negative	False Negative
01	Jpeg Total Number of files (18) virus files(15) (10 MB)	9	8	6	8
02	Songs Total Number of files (24) virus files(20)(10 MB)	20	1	4	5
03	Text Files Total Number of files (72) virus files(57)(10 MB)	30	5	2	10
04	Games Total Number of files (12) virus files(8) (10 MB)	70	5	5	10
05	Zip Files Total Number of files (4) virus files(2) (10 MB)	110	6	1	10

After that different file types were scanned by using the Kaspersky antivirus offline and online mode .The document of different file types of JPEG were scanned which contained the 18 number of files and 15 number of viruses.

Table 4.5: Accuracy of Kaspersky by using different folder type.

S.#	Folder Type	True positive	False Negative	True Negative	False Positive
1	Jpeg Total Number of files (18) virus files(15)(10 MB)	13	10	7	6
2	Songs Total Number of files (24) virus files(20)(10 MB)	15	2	7	5
3	Text Files Total Number of files (72) virus files(57)(10 MB)	50	7	2	7
4	Games Total Number of files (12) virus files(8)(10 MB)	6	8	8	2
5	Zip Files Total Number of files (4) virus files(2)(10 MB)	1	5	0	1

Second folder of type songs which contained 24 files and 20 viruses. Third folder of type text which contained 72 number of files and 57 virus files. Fourth folder of type games which contained 12 files and 8 virus files. Fifth folder of type zip which contained 4 files and 8 virus files. In the result found that the accuracy factors are true positive, false positive, true negative and false negative .When the type of JPEG document values are found 13,10 ,7 and 6.When the songs type file used values are found 15,2,7 and 5.When text files used values are found 50, 7,2 and 7.When games type files used values are found 6,8,8 and 2.When the zip files used values are found 1,5,0 and 1. After that different file types were scanned by using the Trojan detector offline and online mode. The documents of different file types of JPEG were scanned which contained number of files 18 and the number of viruses are 15 files. Second folder of type songs which contained 24 number of files and 20 virus files. Third folder of type text which contained 72 number of files and 57 virus files. Fourth folder of type games which contained 12 number of files and 8 viruses file. Fifth folder of type zip which contained 4 number of files and 2 virus files. In the result found that the accuracy factors are true positive, false positive, true negative and false negative. When the type of JPEG files used values are found 12,10,3 and 9.When the songs file used values are found 16,3,1 and 4.When the text file used values are found 47,6 ,8 and 10.When the games file used values are found 6,2,1 and 5.When the zip file used values are found 1,5,1 and 3.

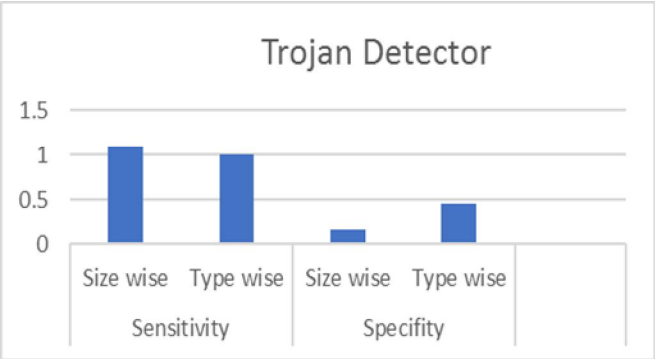

Figure 4.1: Accuracy of Trojan detector

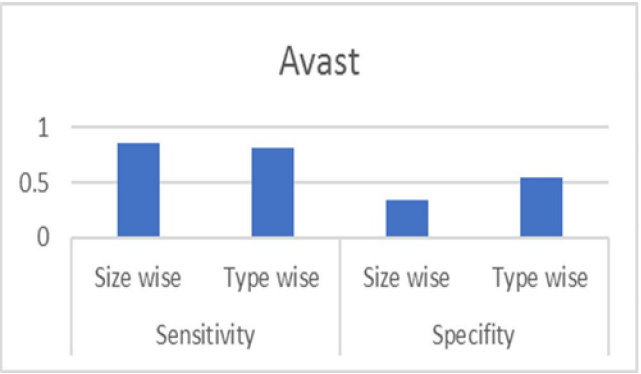

Figure 4.2: Accuracy of Avast

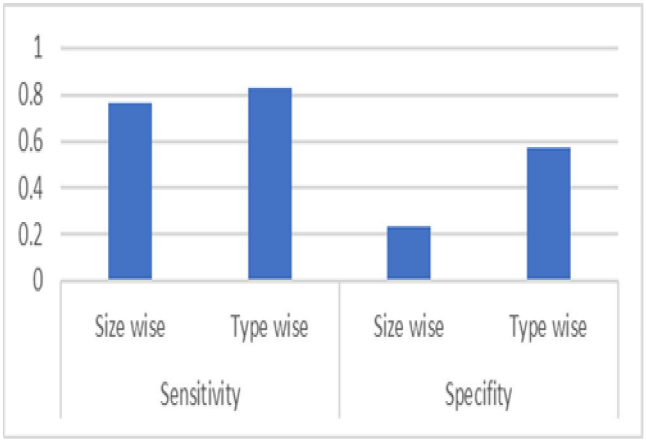

Figure 4.3: Accuracy of Kaspersky

Table 4.6: Accuracy of Trojan Detector by using different folder type Accuracy of Trojan Detector

S. #	Folder Type	True Positive	False Positive	True Negative	False Negative
01	Jpeg Total Number of files (18) virus files(15) (10 MB)	12	10	3	9
02	Songs Total Number of file (24) virus files(20)(10 MB)	16	3	1	4
03	Text Files Total Number of files (72) virus files(57)(10 MB)	47	6	8	10
04	Total Number of files (12) virus files(8)(10 MB)	6	2	1	5
05	Zip files number of files(4)virus files(2)	1	5	1	3

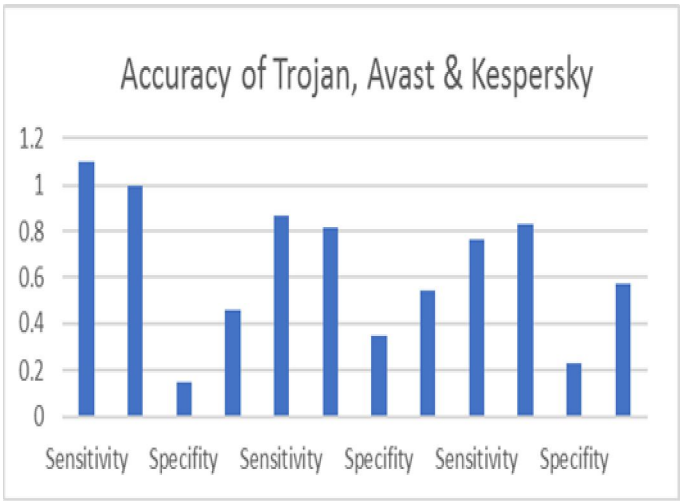

Figure 4.4: Accuracy of Trojan,avast and Kaspersky

Regarding sensitivity Trojan detector has greater sensitivity in both File Size Wise &File Type wise than Avast and Kaspersky. This proves that the accuracy of Trojan Detector is higher than Avast and Kaspersky.

Table 4.7: Time and Memory consumption of the Avast

File type and size	Avast			
	Offline		Online	
80 GB	Time	Memory	Time	Memory
	120 sec	9.4 MB	15 sec	7.88 MB

The result was received in terms of the memory consumption and time consumption of the system offline and online also. When Task Manager was used the memory consumption and time consumption of the system was found. Memory consumed by the Avast in offline mode is 9.4MB and in the online mode memory consumed by the Avast is 7.88MB. Time consumed by Avast is 120 seconds in offline mode and 15 seconds in online mode.

Table 4.8: Time and Memory consumption of Kaspersky

File type and size	Kaspersky				
	Offline			Online	
80 GB	Time	Memory		Time	Memory
	300 sec 146 MB			25 sec	36 MB

In online mode the Avast consumed 7.8MB that is less memory consumption as compared to Avast and Kaspersky and the Trojan detector consumes 19MB, that is average memory consumption as compared to Avast and Kaspersky and finally the Kaspersky consumes 36 Mb that is the highest level of memory consumption as compared to Avast and Kaspersky, it is proved that Kaspersky takes the highest amount of memory in online mode.

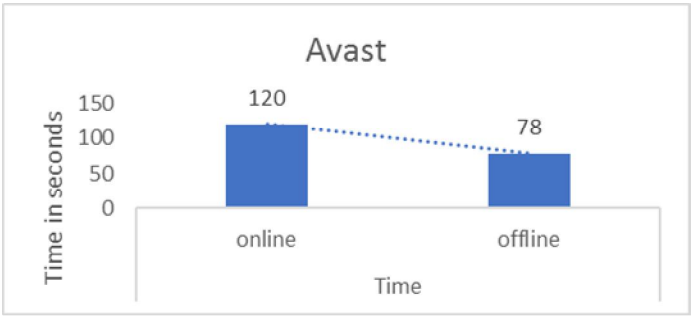

Figure 4.5: Time consumption of Avast

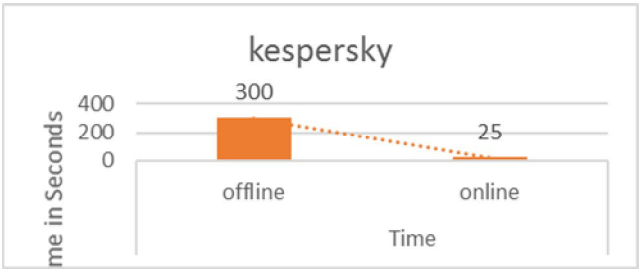

Figure 4.6: Kaspersky time consumption

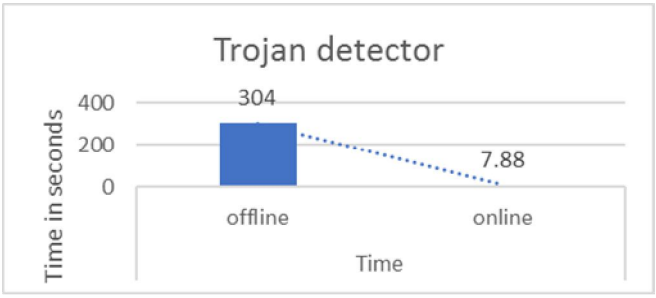

Figure 4.7: Trojan detector time consumption

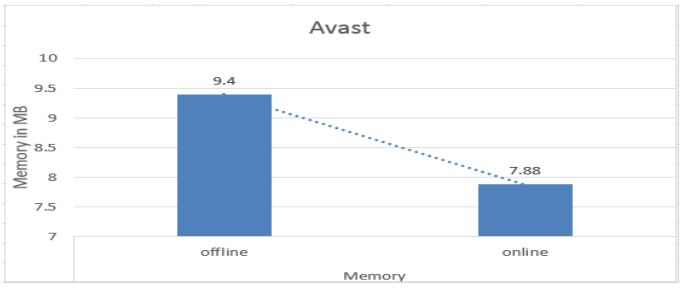

Figure 4.8:Memory consumption of Avast

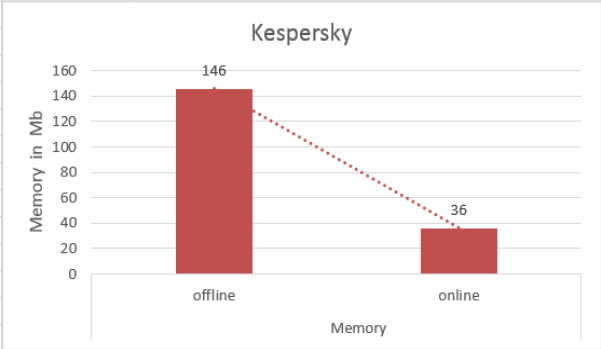

Figure 4.8: Memory consumption of Kaspersky

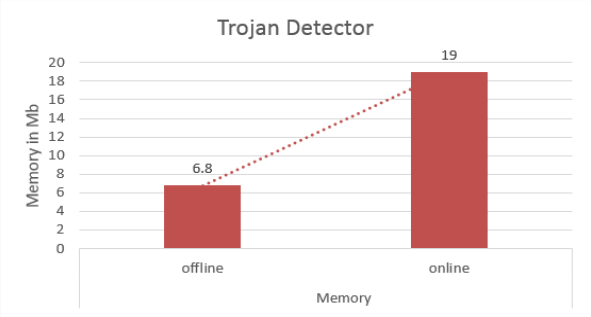

Figure 4.9: Memory consumption of Trojan detector

5. CONCLUSION

It has been determined in this research that the result shows a comparative study among the Avast, Kaspersky, and Trojan Detector. This protection system will be established by utilizing signatures to erudition prototype & this is an accomplishment in action at its uppermost level based on visual studio frame. This is a fulfillment that this protection system will be based on strengthen signature-based protection system that functions at the application layer. It is also executed that this protection evaluation system exhibits essential high level identifying proficiency and looks after research space regression, along with-it assistances in clearing a collection of issues linked with available approach. The focus of this study is to create a prototype and implement one through the intrusion detection system. It has been described that Trojan detection system as an intrusion detection system by comparing `the detection of Trojans attacks online and offline with Avast detection system for detection of Trojan attack and Kaspersky antivirus. Intrusion detection system supports the detection process. first comparing with Avast, second comparing with Kaspersky and third one implemented here as antivirus named Trojan Detector. Here the comparison is made among these three detection systems in terms of Time, Memory consumed and accuracy. As a result, it is found that the Avast took 120 seconds offline and 78 seconds online likewise the Kaspersky took 300 seconds offline and 25 seconds online and Trojan detector took 304 seconds offline and 7.88 seconds online. From these results it is clear that Trojan detector takes highest time in offline mode than others and Avast take highest time in online mode. In Memory Consumption, Avast took 9.4 MB in offline mode, and 7.88 MB in online mode and 304 MB in run time mode, in the same way the Kaspersky took 146 MB in offline mode, 36 MB in online mode and 262 MB in run time mode. Finally, the Trojan detector took 6.8 MB in offline mode, 19 MB in online mode and 78 MB in run time mode.

From the above results it is found that the Avast and Trojan detector take average memory consumption in offline mode while Kaspersky consumes 20 times more memory than Avast and Trojan detector.

In online mode the Avast consumed 7.8MB that is less memory consumption as compared to Kaspersky and Trojan detector and Trojan detector consumes 19MB that is average memory consumption as compared to Avast and Trojan detector and finally the Kaspersky consumes 36 MB that is the highest level of memory consumption as compared to Avast and Trojan detector. It means Kaspersky takes the highest amount of memory in online mode.

ACKNOWLEDGEMENT

Authors would like to thank reviewers for valuable suggestions which improve the quality of paper.

REFERENCES

1. Anitha, A. and Vaidehi, V., 2006, July. **Context based application level intrusion detection system**. In International conference on Networking and Services (ICNS'06) (pp. 16-16). IEEE.
2. Mohd Saudi, M. and Abuzaid, A.M., 2015. **A New Model for Trojan Detection using Machine Learning Inspired by Al-Furqan Verse**.
3. Chakraborty, R.S., Narasimhan, S. and Bhunia, S., 2009, November. **Hardware Trojan: Threats and emerging solutions**. In *2009 IEEE International high level design validation and test workshop* (pp. 166-171). IEEE.
4. Chen, Q.Z., Cheng, R. and Gu, Y.J., 2009, November. **Classification algorithms of Trojan horse detection based on behavior**. In *2009 International Conference on Multimedia Information Networking and Security* (Vol. 2, pp. 510-513). IEEE.
5. Mircovic, J., Dietrich, S., Dietrich, D. and Reiher, P., 2005. **Internet Denial of Service: Attack and Defense**. *Mechanisms. Prentice Hall, Engle Wood Cliffs, NJ*.
6. Denker, G., Kagal, L., Finin, T., Paolucci, M. and Sycara, K., 2003, October. **Security for daml web services: Annotation and matchmaking**.

In *International Semantic Web Conference* (pp. 335-350). Springer, Berlin, Heidelberg.

7. He, Y., Chen, W., Yang, M. and Peng, W., 2004, October. **Ontology based cooperative intrusion detection system**. In *IFIP International Conference on Network and Parallel Computing* (pp. 419-426). Springer, Berlin, Heidelberg.
8. Hung, S.S. and Liu, D.S.M., 2006, October. **A user-centric intrusion detection system by using ontology approach**. In *9th Joint International Conference on Information Sciences (JCIS-06)*. Atlantis Press.
9. Bidgoli, H., 2006. **Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management** (Vol. 3). John Wiley & Sons.
10. Karri, R., Rajendran, J., Rosenfeld, K. and Tehranipoor, M., 2010. **Trustworthy hardware: Identifying and classifying hardware trojans**. *Computer*, *43*(10), pp.39-46.
11. Krügel, C., Toth, T. and Kirda, E., 2002, March. **Service specific anomaly detection for network intrusion detection**. In *Proceedings of the 2002 ACM symposium on Applied computing* (pp. 201-208).
12. Abuzaid, A.M.K., 2014. **Designing a new model to detect Trojan Horse based on knowledge discovery and data mining** (Doctoral dissertation, Universiti Sains Islam Malaysia).
13. Liu, Y.F., Zhang, L.W., Liang, J., Qu, S. and Ni, Z.Q., 2010, July. **Detecting Trojan horses based on system behavior using machine learning method**. In *2010 International Conference on Machine Learning and Cybernetics* (Vol. 2, pp. 855-860). IEEE.
14. Lin, J.C. and Chen, J.M., 2007, October. **The automatic defense mechanism for malicious injection attack**. In *7th IEEE International Conference on Computer and Information Technology (CIT 2007)* (pp. 709-714). IEEE.
15. Tang, S., 2009, August. **The detection of trojan horse based on the data mining**. In *2009 Sixth International Conference on Fuzzy Systems and Knowledge Discovery* (Vol. 1, pp. 311-314). IEEE.
16. Shamsoshoara, A., Korenda, A., Afghah, F. and Zeadally, S., 2020. **A survey on physical unclonable function (PUF)-based security solutions for Internet of Things**. *Computer Networks*, *183*, p.107593.
17. Gupta, M.K. and Chandra, P., 2020. **A comprehensive survey of data mining**. *International Journal of Information Technology*, pp.1-15.
18. Husák, M., Bajtoš, T., Kašpar, J., Bou-Harb, E. and Čeleda, P., 2020. **Predictive cyber situational awareness and personalized blacklisting**: A sequential rule mining approach. *ACM Transactions on Management Information Systems (TMIS)*, *11*(4), pp.1-16.
19. Abuzaid, A.M., Saudi, M.M., Taib, B.M. and Abdullah, Z.H., 2013. **An efficient trojan horse classification (ETC)**. *International Journal of Computer Science Issues (IJCSI)*, *10*(2), p.96.
20. Zhao, S. and Jia, Y., 2010, October. **The Model of Trojan Horse Detection System Based on Behavior Analysis**. In *2010 International Conference on Multimedia Technology* (pp. 1-4). IEEE.