Malware Analysis in Web Application Security: An Investigation and Suggestion

Abhishek Kumar Pandey[1]
Department of Information Technology
BBA University
Lucknow UP, India

Fawaz Alsolami[2]*
Computer Science Department
King Abdulaziz University
Jeddah, Saudi Arabia

***Abstract*—Malware analysis is essentially used for the identification of malware and its objectives. However, the present era has seen the process of malware analysis being used for enhancing security methods for different domains of technology. This study has attempted to analyze the current situation and status of malware analysis in web application security through some objectives. These objectives helps the authors to analyze the purpose, used methodology of malware analysis in web application security previously as well as authors select and find a prioritized technique of malware analysis through a hybrid multi criteria decision making procedure called fuzzy-Analytical Hierarchy Process. This fuzzy-AHP methodology helps the authors to find and recommend a most prioritized malware analysis techniques and type as well as suggest a ranking of various malware analysis techniques that used in web application security frequently for experts and developers use. Furthermore, second section of paper forecast the attack statistics and publication statistics of malwares and malware analysis in web application security respectively for understanding the sensitivity of topic and need of investigation. The proposed tactic intends to be an effective reckoner for web developers and facilitate in malware analysis for securing web applications. Additionally, the study also forecast the publication and attack scenario of malware and malware analysis for web application security that gives a complimentary overview of domain.**

Keywords—Malware analysis; web application; application security; fuzzy-AHP; forecasting

I. Introduction

Ever since the internet came into existence, its use has become expansive and ubiquitous. According to a report of the Internet World State in March 2019, “50.1% of the population in Asia uses the internet, 16.4% of the population uses the internet in Europe, 11.2% in Africa and 7.5% in North America [1]”. These statistics show a marked involvement and effect of internet on the life of people. Nevertheless, internet services also have their defined set of threats and risks. Unfortunately, there has been a massive increase in these threats in the recent years. Data statistics from anti-virus companies and security experts also show the rise of malware and cyber-attacks. Malware is one of the biggest threats for current web applications [2]. Easy accessibility of web is the biggest reason behind the rise of malware attacks against the web. Though the research domain in malware is increasing day by day, the number of attacks and attack-technologies are also increasing simultaneously.

Moreover, contending with these emerging attack-technologies has become a formidable challenge for the researchers and investigators in the field of malware analysis. Malware analysis is the process of determining the functionality, origin and potential impact of a given malware sample such as a virus, worm, Trojan horse, root kit, or backdoor. Defense against malware attacks is malware analysis. Malware analysis is the process of identifying, investigating and measuring the objective, functionality, and the harmful effects of any malware. Malware analysis is a combination of static and dynamic analysis methods. According to a testing lab survey, the success ratio of malware analysis is 96.67% [3]. There are many methods like API chaser, Sandboxing, Call graph method and others for providing accurate malware analysis result.

The focus of this Investigation is to summarize and review the previous research work that has been done on malware analysis and find a link for securing web applications through the malware analysis process. It is very important to analyze and classify the previous work done on securing web application through malware analysis properly for helping the future researchers. To the best of our knowledge, very limited work has been done on collating systematic literature reviews in the context of securing web application through malware analysis and other malware analysis related fields. This paper gives an overview of the previous research work done in the cited area and, further, it intends to help the researchers in identifying the areas where investigations need to be done more effectively for containing the harm done through malware attacks.

For facilitating an exhaustive investigation, the authors of this study have also classified malware attacks based on different categories, which have been further segregated into sub categories to explain the malware threats. Additionally, the study also categorize and prioritize various malware analysis methodologies through a scientific multi criteria decision making approach (MCDM) called fuzzy-Analytical Hierarchy Process (AHP). Fuzzy-AHP is a verified and effective approach for ranking and prioritizing. The use of fuzzy-AHP for ranking malware analysis methodologies can provide a view and idea to experts and researchers. The results of ranking experiment in proposed study will definitely beneficial for future research endeavors and authors believes that results can also be adopted by malware analysts in order to enhance the malware analysis techniques.

*Corresponding Author

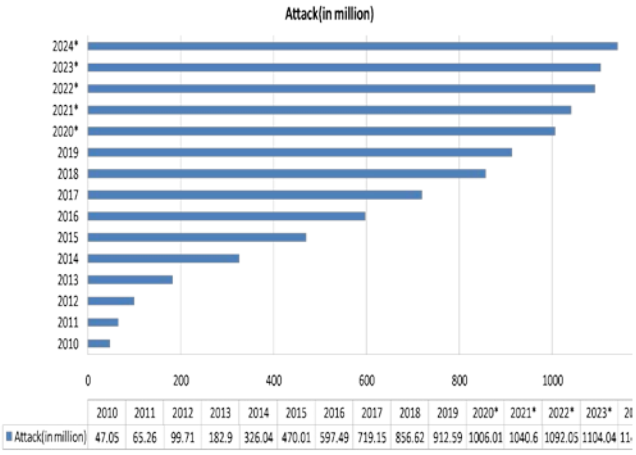
Furthermore, The proposed study is constructed as the second section of study tells about the need of investigation through previous and future forecasted statistics of attacks and publications, then third section tells about the objective of study and fourth and fifth sections defines various experiments conducted by authors in order to achieve objectives. After that in next sixth and seventh section of study authors discuss and conclude the results and study, respectively.

II. Need of Investigation

Web applications and their security is the foremost concern in current digitalized world. Malwares are the most harmful threat actors for web application and most used vector for exploiting web applications. Authors of proposed study finds that malwares are the most used and effective threat vector against web application. Similarly, malware analysis is the only path for identifying and mitigating malwares in early stage according to various research and authors opinion. In order to understand the scenario of malwares against web application security authors find the previous cyber-attack tends against we applications and then forecast the possible growth for future years in malware attacks through a forecasting tool called GMDH Shell DS [4].

Fig 1 discusses the previous and future statistics of malware attack based on an online study [5-7]. The attack ratio shown by the authors in Fig. 1 tells that the condition of malware attacks is highly critical and the future statistics of attacks (based on previous datasets) show that the situation is going to be worst in the next 5 years.

After identifying the scenario of attacks and forecast it authors try to understand the research scenario also for analyzing the research ratio against the attack because the attack situation clearly represent that there is need for a solid and unified solution against malwares in web application security. Due to this need it is important for authors to understand the research condition of malware analysis in web application security. For achieving this goal authors select only quality databases and research articles that pose a contribution in web application security as a malware analysis technique. In order to analyze previous researches authors find following counts and forecast these previous statistics for next five years to understand the future scenario also.



	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020*	2021*	2022*	2023*	20
■ Attack(in million)	47.05	65.26	99.71	182.9	326.04	470.01	597.49	719.15	856.62	912.59	1006.01	1040.6	1092.05	1104.04	11

Fig. 1. Previous and Future Attack Ratio.

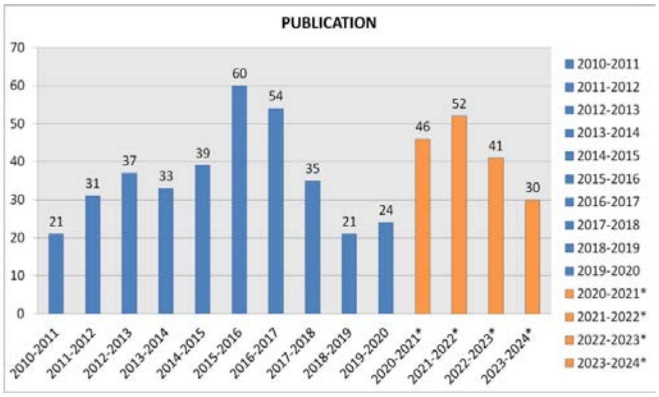


Fig. 2. Previous and Future Forecasted Statistics of Research Publications.

The ratio of previous and future forecasted data is not very different and clearly represent that it is not sufficient for web application security against malwares in the comparison of attack trends that is discussed in Fig. 1. Authors strongly believe that there is need for more research publications and research endeavors. These statistics and forecasted ratio of attacks and publications motivate authors to investigate the malware analysis in web application security with some universally adopted and effective objectives. In order to understand the objectives authors discuss about them in next section.

III. Investigation Objective

Every investigation has their objective. These objectives are the goals that are achieved by investigator or a researcher during the whole analysis process. In the context of this study, authors have two main and significant objectives. These objectives are described below:

Objective 1: Why and which malware analysis process is used in previous research in order to secure web applications?

Motivation: Malware analysis is a process that is normally used for identifying malwares or malicious activities after the harm is done in system. But in current situation from some previous year’s malware analysis techniques are used for variety of works and security mechanism from different types and attributes. Authors choose this objective just because there is need to associate and summarize the whole previous scenario of malware analysis as a security approach for web application in one place.

Objective 2: Which approach plays a key role as an effective technique of malware analysis that helps the future researchers as a research topic or development idea?

Motivation: Authors aim is to provide a systematic prioritization wise list of various malware analysis techniques to effectively help the experts and researchers. A prioritization method effectively contributes in malware analysis research. Selection and prioritization of techniques can provide step wise path to developers and experts in order to secure web application.

Further, for achieving these two objectives authors performed condition examination and ranking examinations that are described and discussed in next sections.

IV. Condition Examination

This type of examination is introduced by authors to analyze and review the current situation of malware analysis in web application security perspective. During this type of examination authors identify the various aspects of malware analysis in previous web application security research with malware analysis. Various sub-assessments that are performed by authors are written below:

A. Purpose Analysis

The main goal of this analysis is to identify the purpose of use of malware analysis in web application security. This type of analysis can provide some effective and crisp analyzed information regarding malware analysis as well as its use. These objectives or purposes will help the prospective researchers and practitioners to find the purpose of malware analysis and the need for malware analysis for web application security. Malware analysis targets objectives like Cyber-attacks, privacy harm and several others in previous research initiatives. Additionally, in this type of analysis authors find following objectives or purpose of malware analysis for web application security.

Cyber Attacks: Recent experiences of web applications services show that cyber-attacks are the foremost focus of many research publications. Malwares are the primary and mostly used source of any cyber-attacks. Malware analysis approaches provide a path for experts and researchers to provide a prevention mechanism for them. The model given by GuozhuMeng [8], in May 2018, is probably the most accurate approach for addressing this issue. In this model, the combination of security analyst approach and web security works properly for securing Android app market from harmful malicious apps. There are other papers [9, 10] which also discuss the challenges and threats of malware as cyber-attack. These papers [9, 10] provide a deep need of malware analysis by raising the malware issue as the biggest threat for web applications.

Harm on Privacy: Privacy on the web applications is the most pertinent issue for any user and is rated as the top priority by all service users. Harm on privacy objective shows that malwares are rapidly targeting web applications and the biggest challenge for experts now is in privacy issues [11].

Network Security: Malware has emerged as a potent weapon for the attackers and in today’s scenario, the attackers use malware in almost every place for exploit. Aziz Mohaisen has proposed a method of malware detection in a network by using artifact behavior analysis [12]. This approach includes static analysis automated tool technique for better results and less consumption of time.

Enhancing Malware Analysis: Many researchers use different types of methodologies and hybrid methods for enhancing malware analysis procedures. Igocio Martin has proposed a machine level approach for android signature-based malware detection [13].

B. Technique Analysis

This section is an important part of investigation. In order to analyze the used various techniques of malware analysis in web application security authors conducted an in-depth analysis of previous researches to gauge the analyzed solution. The findings related to malware analysis methods have been categorized into different parts by the authors. In the process of assimilating the findings from the publications, authors found two classic malware analysis methods; i.e. Behavior-based Analysis and Signature-based Analysis. These methods are used by the experts and researchers for facilitating malware analysis methodology in their paper. Table II shows the approaches that have been discussed as follows:

Behavior-based Identification: Behavior-based malware analysis is the most used methodology by previous researchers. In the process of behavior-based analysis of malware the tool or technique analyze and examine the behavior of commands, code work-flow and network traffic, etc. [14-18]. This type of methodology is effectively used in current era of malware analysis. Behavior-based analysis techniques that are used in web application security through previous researchers are described following:

Machine Level Approaches: In this part, the authors found papers discussing the same approaches with different methods for their different objectives. A Mohaisen talks about antivirus malware identification methods with the help of machine level method for better results [19]. There are many other papers [20, 21, 22] related to machine level approaches for identification, classification, and analysis of malware. Table II combines the approaches with the application of research papers.

Sandboxing (API Chaser): In this part, the authors have included the papers that discuss the dynamic methodology of analysis. Sandboxing is a tool-based identification methodology that analyzes the API calls of a particular program. Yuhi Kawakoya proposed a method of sandboxing technique to analyze malicious application [23]. The taint coding methods have also been used for identifying malicious code sliding in API calls. The method is an effective approach for identification of malware. There are many other papers, at present, that discuss the sandboxing approach in different ways for performing malware analysis [24, 25].

Network Traffic Analysis: In this sub-section, the authors have discussed about several research papers based on network traffic analysis method for identifying malware artifacts. Network traffic is a collection of incoming and outgoing connections which help an examiner to collect footprints and essence of malware. XiaolinGuiet et al. has proposed a model XcodeGhost [26]. According to Gui, the model can find the ratio of infection devices and categorize the characteristics of malicious application traffic for analysis purpose.

Signature-based Identification: Authors of this study found that less number of studies and researchers are using or adopting signature-based malware analysis into the comparison of behavior-based analysis or identification. Signature-based analysis of malwares is the process of identifying malicious attributes from comparing previously identified and stored attribute or file [14]. But on the other hand, as per the Table II, it is also evident that signature-based analysis of malwares are adopted as well as used for achieving every objective in previous research initiatives. This study has analyzed the previously used main techniques for signature-based identification under the following headings.

Artifact Ordering: In this part, the authors included those papers which discussed the static analysis approaches based on artifact analysis. Aziz Mohaisen proposed a paper discussing network traffic analysis based on artifact ordering [12]. An author of one research study has also proposed a model for analysis with the help of autosomal and n-gram feature extractor. There are many other papers that have discussed the static analysis approaches and artifact analysis features [27].

Virus scan/Comparing previously identified malicious signatures: In this sub-section, the authors have discussed about different signature-based approach papers that have been used by previous researchers for better malware analysis process [28]. The signature-based method is a static analysis approach for analyzing malware. Cristian Adrián Martínez et al. have discussed the signature based mechanism of malware detection in cloud environment [29]. Cristian proposed a model uCLAVS that has some predefined set of protocols based on previous malware signatures and actions. The model efficiently collects the malicious activity information and with the help of IDS (Intrusion Detection System) notifies about the harmful activity.

Portable Executable file analysis: PE file analysis is a process of analyzing executable files for the possibility of malicious attribute in it. It is a signature-based identification process that compares the PE header with previous malware signatures for identifying the malicious attributes of file.

Reverse Engineering: Reverse engineering is a type of method that is use as a last option by many malware examiners. It is a process where examiner chose the software engineering approach called reverse engineering for disassemble the code and analyze the whole code I reverse order node by node for deep and exact identification of malicious activity. Reverse engineering is a lengthy but effective process for malware identification with static analysis attributes. Extracting malicious activity of code or application from low level of language analysis and examination is most effective quality of reverse engineering that makes it an effective approach. Further, authors also find that reverse engineering is not a part of classical malware analysis methodology it is added after the hybrid malware analysis approach came into existence in modern malware analysis methodology.

V. Ranking Examination

Ranking examination is a process that is adopted by authors to select and find an effective and prioritized malware analysis technique list with a most prioritized malware analysis approach for developers and experts. Previously, authors discuss about various malware analysis techniques that are effective and useful additionally, in order to construct a hierarchy of malware analysis techniques authors examine the malware analysis process and find that before discussing the techniques of malware analysis there is a classification of malware analysis types that is one of the most significant and effective part of malware analysis process [30]. Further, it is important to discuss about these types before constructing a tree like structure of malware analysis techniques. Descriptive descriptions of various types of malware analysis are:

The authors have categorized and calculated the overall percentage of three basic types of malware analysis for better and easy understanding. This type of categorization will help the readers to easily comprehend the trend and functionality of the malware analysis research related to web applications. This categorization also provides an overall percentage classification of basic malware analysis types. Fig. 3 describes the percent ratio of a malware analysis types through the previous research initiatives.

Static Analysis: Static analysis is the most useful identification mechanism for malware and manual static analysis of a malicious code (If possible) is the first approach that a researcher takes in any kind of malware identification. In the process of classification, the authors found that 30% of the papers are based on static analysis approaches. For example, a method of Application Security Triage (MAST) helps in malware selection by statistical analysis approach [31-35]. The authors of this SLR also found similar static analysis studies that proposed a better research environment.

Dynamic Analysis: In this sub-section, the authors have included research publications that have discussed the dynamic malware identification approach and detection methodology for web applications or can be useful for web applications. Dynamic approach of analysis is automated computerized technique for analyzing malware. At the categorizing period, the authors found that 34% of the papers talked about dynamic analysis approach [36-40]. Moreover, many dynamic analysis papers that are available discuss about the vulnerabilities of dynamic mechanism. For example, Katsunari Yoshioka et al. have discussed the vulnerability of public sandboxing analysis system in [41-45]. Katsunari has discussed that public sandboxing system enables remote host service for updating and alteration in analysis during the examination from the company's end but this service can cause high risk. K.Y. provides a solution for this kind of vulnerability by dynamic IP addressing.

Hybrid Analysis: During the classification of basic malware analysis approaches, the authors found quite a few papers that discussed about the combination of static and dynamic analysis. In fact after gauging several publications, it was obvious that Hybrid analysis was the most accepted analysis technique for several researchers [42-45]. The share ratio of publication is 36 % for hybrid analysis in types of malware analysis approaches. The hybrid analysis includes hardware and software combination also, like Das S et al. delivers hardware for malware detection online [46]. Das proposed an embedded system by combining the processor and FPGA. The aim of hardware is to capture the behavior of malware and detect it online.

Furthermore, now after discussing the types of malware analysis approaches authors construct the hierarchy of various types and techniques of malware analysis by summarizing and associating all the techniques under one roof. Authors develop a hierarchical figure of malware analysis techniques and types that is described in Fig. 4.

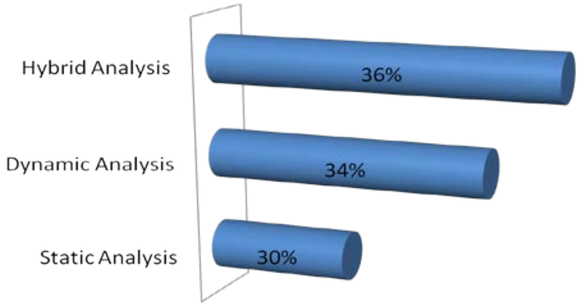


Fig. 3. Percentage Contribution of Various Types of Malware Analysis Types According to Current Trend.

Fig. 4 represents the whole malware analysis types and techniques that are used for securing web applications. Authors apply a multi criteria decision making (MCDM) approach called fuzzy- Analytical Hierarchy Process (AHP) for evaluating the priority and finding the most prioritized approach and type of malware analysis [46-52]. Fuzzy-AHP is methodology that is pre-verified and authors has expertise in fuzzy-based various MCDM approaches through their previous experience [53-56]. Fuzzy-AHP methodology works on triangular fuzzy numbers and provides some crisp and effective outcomes [57-61]. Authors strongly believe that fuzzy-AHP is the most promising and effective technique for assessing the priority of malware analysis techniques and types.

A. *Numerical Assessment*

Numerical assessment of malware analysis types and techniques from fuzzy-AHP methodology is associated with the inputs of 70 experts from industry and academic that is taken by authors for evaluation process. Further, after collection of suggestions authors apply the fuzzy-AHP technique on layered Fig. 2 and find the following pair wise comparison matrix that is defined in Tables I to IV [62-66]. Now after, successful construction of pair wise comparison matrix of every layer and malware type and technique authors apply defuzzification of calculated weights in pair wise comparison matrix through adopted fuzzy-AHP methodology [67-71]. Table V to Table IX shows the defuzzification of local weights and their associated dependent weight. Final ranking of sub-factors are displayed in Table X.

Above Table X represents the calculated weights and their associated ranking of various malware analysis techniques and types that are described in Fig. 2. The result discussed in Table X clearly describes that hybrid analysis and its second layered attribute dynamic + static analysis (combined) has most priority and rank in all the malware analysis techniques. Similarly, the Table X represents the various ranking list of malware analysis techniques that can be utilized and adopted by developers and researchers for producing effective and useful malware analysis techniques and approaches that enhance the web application security more frequently.

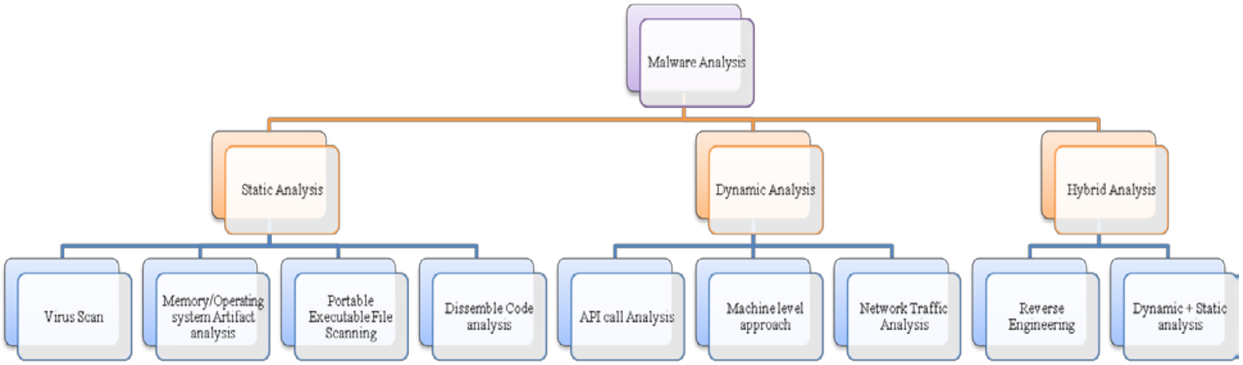


Fig. 4. Hierarchy of Malware Analysis.

TABLE I. COMPARISON MATRIX FOR LEVEL 1 OF FIGURE 4

	Static Analysis (R1)	**Dynamic Analysis (R2)**	**Hybrid Analysis (R3)**
Static Analysis (R1)	1.00000, 1.00000, 1.00000	0.40670, 0.54970, 0.78760	0.49560, 0.70290, 0.93300
Dynamic Analysis (R2)	-	1.00000, 1.00000, 1.00000	0.79120, 0.88310, 1.02040
Hybrid Analysis (R3)	-	-	1.00000, 1.00000, 1.00000

TABLE II. COMPARISON MATRIX FOR LEVEL 2 FOR R1 OF FIGURE 4

	Virus Scan (R11)	**Memory/OS artifact analysis (R12)**	**PE file analysis (R13)**	**Dissemble code analysis (R14)**
Virus Scan (R11)	1.00000, 1.00000, 1.00000	0.55980, 0.89940, 1.37050	0.48760, 0.67100, 0.89000	0.38360, 0.54830, 0.83440
Memory/OS artifact analysis (R12)	-	1.00000, 1.00000, 1.00000	0.80010, 1.23760, 1.78120	0.27700, 0.38540, 0.63400
PE file analysis (R13)	-	-	1.00000, 1.00000, 1.00000	0.59660, 0.70930, 0.90950
Dissemble code analysis (R14)	-	-	-	1.00000, 1.00000, 1.00000

TABLE III. Comparison Matrix for Level 2 for R2 of Figure 4

	API call Analysis (R21)	**Machine level Analysis (R22)**	**Network Traffic Analysis (R23)**
API call Analysis (R21)	1.00000, 1.00000, 1.00000	0.55060, 0.58810, 0.66470	0.22550, 0.27620, 0.35740
Machine level Analysis (R22)	-	1.00000, 1.00000, 1.00000	0.68980, 0.88600, 1.10020
Network Traffic Analysis (R23)	-	-	1.00000, 1.00000, 1.00000

TABLE IV. Comparison Matrix for Level 2 for R3 of Figure 4

	Reverse Engineering (R31)	**Dynamic + Static Analysis (R32)**
Reverse Engineering (R31)	1.00000, 1.00000, 1.00000	0.30510, 0.38920, 0.56090
Dynamic + Static Analysis (R32)	-	1.00000, 1.00000, 1.00000

TABLE V. Combined Matrix for Level 1 of Figure 4

	Static Analysis (R1)	**Dynamic Analysis (R2)**	**Hybrid Analysis (R3)**	**Weights**
Static Analysis (R1)	1.00000	0.57340	0.70860	0.241684
Dynamic Analysis (R2)	1.74400	1.00000	0.89450	0.378445
Hybrid Analysis (R3)	1.41120	1.11790	1.00000	0.379871
C.R.= 0.00580878				

TABLE VI. Combined Matrix for Level 2 for R1 of Figure 4

	Virus Scan (R11)	**Memory/OS artifact analysis (R12)**	**PE file analysis (R13)**	**Dissemble code analysis (R14)**	**Weights**
Virus Scan (R11)	1.00000	0.93230	0.66470	0.57870	0.184502
Memory/OS artifact analysis (R12)	1.07260	1.00000	1.26420	0.42050	0.211198
PE file analysis (R13)	1.50440	0.79100	1.00000	0.73040	0.233061
Dissemble code analysis (R14)	1.72800	2.37810	1.36910	1.00000	0.371239
CR= 0.0237475					

TABLE VII. Combined Matrix for Level 2 for R2 of Figure 4

	API call Analysis (R21)	**Machine level Analysis (R22)**	**Network Traffic Analysis (R23)**	**Weights**
API call Analysis (R21)	1.00000	0.59790	0.28390	0.168952
Machine level Analysis (R22)	1.67250	1.00000	0.89050	0.348472
Network Traffic Analysis (R23)	3.52240	1.12300	1.00000	0.482576
C.R.= 0.0220487				

TABLE VIII. Combined Matrix for Level 2 for R3 of Figure 4

	Reverse Engineering (R31)	**Dynamic + Static Analysis (R32)**	**Weights**
Reverse Engineering (R31)	1.00000	0.41110	0.291333
Dynamic + Static Analysis (R32)	2.43250	1.00000	0.708667
C.R.=0.000000			

TABLE IX. Calculated Final Weights

Main	**Local Weights**	**Sub**	**Local Weights**	**Dependent Weights**
R1	0.241684	R11	0.184502	0.044591
		R12	0.211198	0.051043
		R13	0.233061	0.056327
		R14	0.371239	0.089723
R2	0.378445	R21	0.168952	0.063939
		R22	0.348472	0.131877
		R23	0.482576	0.182629
R3	0.379871	R31	0.291333	0.110669
		R32	0.708667	0.269202

TABLE X. OVERALL WEIGHTS AND PRIORITIES

Sub- Regions	Weightages	Percentages	Overall Ranks
R11	0.04459	4.45%	9
R12	0.05104	5.10%	8
R13	0.05633	5.63%	7
R14	0.08972	8.97%	5
R21	0.06394	6.37%	6
R22	0.13188	13.18%	3
R23	0.18263	18.26%	2
R31	0.11067	11.06%	4
R32	0.26920	26.92%	1

VI. DISCUSSION AND LIMITATION

This section is totally dedicated for assessing the objectives of the investigation that leads the authors to conduct the examination of previous research from various point of views.

A. Assessment of Objective 1

Objective 1 of authors is totally dedicated to find and summarize the current status of malware analysis techniques in web application security based on why and how they are. In order to find and achieve the objective 1 author conduct the purpose analysis and technique analysis to find why and how the malware analysis approaches are applied in web application security previously. These analysis sections clearly represent the status and used techniques associated with their objectives or purpose in web application security. Following Table XI represents the techniques and the associated purpose of malware analysis use in web application security for presenting a systematic view on the situation of malware analysis techniques and its purpose of use in web application security.

After evaluating the situation of malware analysis as a security approach for web applications authors find some following attributes and challenges of malware analysis types and techniques.

Security will remain a strong focus for malware analysis: Malware analysis for web security is the main topic of this SLR. As per the findings of the authors, statistics and data show that research trends are focusing on the security aspect of the web, Android and other relevant areas of computer. For example, Brandon Amos et al. has proposed a technique by combining machine learning and dynamic analysis approach for better detection of malware online[47, 72-74].

Minimum number of related articles and research endeavors: The authors found that there is no SLR on malware analysis for securing the web application, though there were many other surveys that discussed other related domains like-the static analysis, dynamic analysis of malware and malware detection survey and others. One of the examples in this context is that of Rami Sihwail et al. The study provides a brief discussion on current malware analysis techniques [48], classification of malware in the current situation and also provides literature about different kinds of malware detection methods. There are some other related papers present in the study [49, 50, 75].

The need for Controlling Malware attacks: After studying all the relevant publications and articles, it is evident that the malware attacks are the biggest threat to web security and there is an imminent need of a good malware analysis procedure that can reduce the threat of malware attacks in web applications.

B. Assessment of Objective 2

Second objective of authors is to select and suggest a prioritized malware analysis technique for future use and development in web application security. Additionally, for achieving this goal authors adopt the methodology fuzzy-AHP for evaluating the priority of various malware analysis techniques and types that are identified by authors through their first objective. A prioritization approach is performed by ranking examination section in the paper. Further, after a successful implementation of ranking examination authors find the following result:

Hybrid Approach produce better result: After an intensive analysis of the papers, the authors found that a hybrid approach of malware analysis mechanism is a key for better results in web application security. Many researchers are focusing on the hybrid malware analysis technique in their research endeavors. The hybrid approach opens the door for researchers to use static and dynamic methods at the same time as a combination. This combination increases the possibility of malware detection as well as decreases the threat ratio for web applications. One of the relevant examples in this context is that of Shahid Alam et al.'s study that proposed a framework for metamorphic analysis mechanism for real-time detection of malware [52]. Metamorphic malware analysis is based on binary code analysis, a part of dynamic analysis that uses a static approach in the identification of old malware.

In simple words the framework uses a combination of dynamic and static malware analysis in a unique way for producing effective malware detection. The authors of this study have also extracted some other papers [76, 77, 51, 53, 27, 8, 15] that have delivered hybrid approaches for better results. Moreover for providing more convincing discussion on this topic, the authors of this study have comparatively analyzed all three malware analysis approaches. Table III illustrates the comparative study. The results of comparative study clearly portray that dynamic and static malware detection have shortcomings in their own environment. However, a hybrid approach overcomes those lacunae by providing extremely effective detection ratios.

For example, sometimes it is crucial to run the malicious file without understanding the malware class and its behavior during the run stage [30]. During this period of analysis, the hybrid approach provides a static detection of malware class from its static analysis and at the same time malware analyst prepares the analysis environment according to the result of static analysis for further dynamic analysis. Such an approach facilitates a secure and accurate success ratio in malware analysis process.

Further to help and motivate the analyzed outcome of investigation authors performed and present a comparative study of static, dynamic and hybrid malware analysis techniques based on some standards that are defined by [30] in Table XII.

TABLE XI. APPROACHES THAT HELP THE OBJECTIVE

	Approach	Attack	Harm of Privacy	Network based Security	Enhancing Malware Analysis
Behavior-based Analysis	***Machine level***	✓	✓		✓
	Sandboxing (API Chaser)		✓	✓	✓
	Network Traffic Analysis	✓	✓	✓	✓
Signature-based Analysis	***Artifact Ordering***			✓	
	Virus Scan	✓	✓	✓	✓
	Portable Executable file analysis	✓	✓	✓	
Reverse Engineering		✓	✓	✓	✓

TABLE XII. COMPARATIVE STUDY OF MALWARE ANALYSIS TECHNIQUES

Analysis Techniques/Parameters	Condition (Mode) of malware at the time of analysis	Consumed time in analysis process	Effect of anti-malware analysis tools & techniques	Extracted information from analysis process
Static Analysis	At Rest Mode	Usually less through static analysis tools.	Normally anti-detection techniques can easily bypass or hide their malicious attribute from static analysis.	Very less and low in impact.
Dynamic Analysis	At Running mode	Usually more time consumed due to activated or running motion of malware.	Normally need more advance anti-detection tool or technique to bypass the dynamic analysis because of its running motion nature.	Highly informative and extract useful information.
Hybrid Analysis	Both (At rest and run mode)	More time taking into the comparison of static analysis and dynamic analysis.	It is most challenging and critical task for anti-detection tools and techniques to bypass or tackle the hybrid analysis due to its hybrid (Static detection + Dynamic detection) nature.	Provide a perfect blend of useful information associated with risk factors and its approximate impact.

VII. CONCLUSION AND FUTURE WORK

Research on malware analysis for web security is rapidly maturing. This research endeavor specifically focuses on the current status or situation of malware analysis in web application security and tries to suggest a malware analysis technique and priority ranking of various malware analysis techniques that helps in web application security through fuzzy-AHP method. The investigation itself has several defined and categorized procedures for tabulating the situation of malware analysis based on previous research endeavors. As per the results discussed in the above sections, the following possible directions for future work can be envisioned:-

First: A good and effective malware analysis procedure has to be employed for controlling malware attacks and losses of enterprises. Malware analysis is the only way for understanding malware and their respective objectives. However, there is a gap between malware and malware analysis procedures. There is no systematic framework available for malware analysis and for securing web applications specifically.

Second: The outcome of the research work done on malware, as of now, is not effective and practical. Practically possible implementations are needed for malware analysis field in securing web application. There is a huge gap between malware analysis approaches and web application security that needs to be filled.

Third: The authors also found that the old web application security mechanisms are not totally updated in regular mode in many organizations. A validated process for securing web application through malware analysis is strictly required from the perspective of security. A deep analysis between different malware analyses approaches are recommended for producing an effective work flow for web application security by the authors.

Fourth: The proposed research review only provides a critical view on current malware analysis mechanisms that are used and adopted by web application security practitioners. Finding various defense mechanisms and integrating defense scenario with current mechanism trends is the research possibility for future initiatives. Our SLR has cited several studies on defense strategies like access control mechanisms, encryption and cryptography, etc. which could be a premise for further research investigations.

This study conclusively asserts the situation and suggestion for malware analysis to ensure optimum web application security. The research Endeavour tries to fill the gap between malware analysis approach and web applications by providing a snap of its status and suggest a path through a scientific verified methodology. The authors reiterate that a systematic malware analysis framework in web application security perspective can enhance the security mechanism of web applications and reduce the attack rates of the malwares.

References

[1] (2019), Internet Uses in the World by Region, Accessed on 20 April 2020, [online]. Available at: https://www.internetworldstats.com /stats.htm.

[2] (2019), The Biggest Cyber Threats to Watch Out for in 2019, Accessed on 20 April 2020, [online]. Available at: https://www. Securitymagazine.com/articles/89581-the-biggest-cyber-threats-to-watch-out-for-in-2019.

[3] (2019), Malware Detection Rates Revealed for 28 AV Programs, Accessed on 20 April 2020, [online]. Available at: https://techtalk. pcpitstop.com/2017/04/10/detection-rates-revealed/ .

[4] Rajeev Kumar, Suhel Ahmad Khan, Raees Ahmad Khan (2017), Fuzzy Analytic Hierarchy Process for Software Durability: Security Risks Perspective, Advances in Intelligent Systems and Computing, Volume 508, pp. 469-478, Springer. DOI: https://doi.org/10.1007/978-981-10-2750-5_49.

[5] Rajeev Kumar, Suhel Ahmad Khan, Raees Ahmad Khan (2016), Secure Serviceability of Software: Durability Perspective, Communications in Computer and Information Science, Volume 628, pp. 104-110, Springer. DOI: https://doi.org/10.1007/978-981-10-3433-6_13.

[6] Gayatri Kapil, Zaiba Ishrat, Rajeev Kumar, Alka Agrawal, Raees Ahmad Khan (2020), Managing Multimedia Big Data: Security and Privacy Perspective, Advances in Intelligent Systems and Computing (Originally Published with the Title: Advances in Intelligent and Soft Computing), Volume 1077, pp. 1-12, Springer. DOI: https://doi.org/ 10.1007/978-981-15-0936-0_1.

[7] Rajeev Kumar, Abdullah Baz, Hosam Alhakami, Wajdi Alhakami, Mohammed Baz, Alka Agrawal, Raees Ahmad Khan (2020), A Hybrid Model of Hesitant Fuzzy Decision-Making Analysis for Estimating Usable-Security of Software, IEEE Access, Volume 8, Issue 4, pp. 72694-72712. IEEE. DOI: 10.1109/ACCESS.2020.2987941.

[8] GMDH Shell DS, Accessed on 25 April 2020, [online]. Available at: https://gmdhsoftware.com/.

[9] (2019), Malware, Accessed on 21 April 2020, [online]. Available at: https://www.av-test.org/en/statistics/malware/.

[10] Rajeev Kumar, Alka Agrawal, Raees Ahmad Khan (2020), A wakeup Call to Data Integrity Invulnerability, Computer Fraud & Security, Volume 2020, Issue 4, pp. 14-19. Elsevier. Available at Thomson Reuters. DOI: https://doi.org/10.1016/S1361-3723(20)30042-7.

[11] Alka Agrawal, Mohammad Zarour, Mamdouh Alenezi, Rajeev Kumar, Raees Ahmad Khan (2019), Security durability assessment through Fuzzy Analytic Hierarchy process, PeerJ Computer Science, PeerJ Inc., pp. 1-43. DOI: https://doi.org/10.7717/peerj-cs.215.

[12] Bethencourt, John; Song, Dawn; Waters, Brent: Analysis-Resistant Malware. figshare. Journal contribution, 2018.

[13] Saxe Joshua, Turner Rafael, Blokhin Kristina. CrowdSource: Automated Inference of High level Mlawrae Functionality from Low-Level Symbols Using a Crowd Trained Machine Learning Model. 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE), 2014.

[14] Akour M, IzzatAlsmadi, MamounAlazab, The Malware Detection Challenge of Accuracy. 2nd International Conference on Open Source Software Computing (OSSCOM), 2016.

[15] (2019), Your Web Applications Are More Vulnerable Than You Think, Accessed on 25 April 2020, [online]. Available at: https://security intelligence.com/your-web-applications-are-more-vulnerable-than-you-think/.

[16] Aziz Mohaisen, Omar Alrawi, Jeman Park, Joongheon Kim, DaehunNyangManarMohisen. Network-based Analysis and Classification of Malware using Behavioral Artifact Ordering. EAI Endorsed Transaction on security and safety, 5(16), 2018.

[17] Chang, J., Venkatasubramanian, K. K., West, A. G., & Lee, I. Analyzing and defending against web-based malware. ACM Computing Surveys, 45(4), 1–35, 2013.

[18] Damodaran, A., Troia, F. D., Visaggio, C. A., Austin, T. H., & Stamp, M. A comparison of static, dynamic, and hybrid analysis for malware detection. Journal of Computer Virology and Hacking Techniques, 13(1), 1–12, 2015.

[19] Bermejo, J., Abad, C., Bermejo, J.R., Sicilia, M.A., Sicilia, J.A. (2020). A Systematic Approach to Malware Analysis (SAMA). Applied Sciences, 10(4), 1360. https://www.mdpi.com/2076-3417/10/4/1360.

[20] De Vicente Mohino, J., Bermejo, J., Bermejo, J.R. & Sicilia, J.A. (2019). The Application of a New Secure Software Development Life Cycle (S-SDLC) with Agile Methodologies. Electronics, 8 (11), 1218. https://doi.org/10.3390/electronics8111218.

[21] Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (n.d.). Role-based access control: a multi-dimensional view. Tenth Annual Computer Security Applications Conference.doi:10.1109/csac.1994. 367293.

[22] Islam, MD. S., Islam, MD. R., Kayes, A. S. M., Liu, C., & Altas, I. A Survey on Mining Program-Graph Features for Malware Analysis. In ATCS 2014 (Vol. 153, pp. 220-236). Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2014. https://doi.org/10.1007/978-3-319-23802-9_18.

[23] Mohaisen, O. Alrawi, Av-meter: An evaluation of antivirus scans and labels, in S. Dietrich (Ed.), Detection of Intrusions and Malware, and Vulnerability Assessment. Springer International Publishing, Cham, pp. 112–131, 2014.

[24] SibiChakkaravarthy, S., Sangeetha, D., &Vaidehi, V. A Survey on malware analysis and mitigation techniques. Computer Science Review, 32, 1–23, 2019.

[25] Sethi, K., Chaudhary, S. K., Tripathy, B. K., &Bera, P. A Novel Malware Analysis Framework for Malware Detection and Classification using Machine Learning Approach. Proceedings of the 19th International Conference on Distributed Computing and Networking - ICDCN ’18, 2018.

[26] Jan Stiborek, TomášPevný, Martin Rehák. Probabilistic analysis of dynamic malware traces. Computer & Security Elsevier, Volume 74, pp 221-239, 2018.

[27] YuheiKawakoya, EitaroShioji, Makoto Iwamura, Jun Miyoshi. Taint-Assisted Sandboxing for Evasive Malware Analysis. Journal of Information Processing; Vol.27 297-314, 2019.

[28] M. Alaeiyan, S. Parsa and M. Conti, Analysis and classification of context-based malware behavior, Computer Communications (2019), https://doi.org/10.1016/j.comcom.2019.01.003.

[29] M. Alaeiyan, S. Parsa and M. Conti, Analysis and classification of context-based malware behavior, Computer Communications (2019),https://doi.org/10.1016/j.comcom.2019.01.003.

[30] XiaolinGui, Jun Liu, Mucong Chi, Chenyu Li, Zhenming Lei. Analysis of Malware Application Based on Massive Network Traffic. Services and Applications China Communications. August 2016.

[31] Weijie Han, JingfengXue, Yong Wang, Lu Huang a ,Zixiao Kong, Limin Mao. MalDAE: Detecting and explaining malware based on correlation and fusion of static and dynamic characteristics. Computer & Security Elsevier, Volume 83, pp 208-233, 2019.

[32] Gregory Blanc, RuoAno, YoukiKadobayashi. Term-Rewriting Deobfuscation for Static Client-Side Scripting Malware Detection. 4th IFIP International Conference on New Technologies, Mobility and Security, 2011.

[33] Altay, B., Dokeroglu, T., &Cosar, A. Context-sensitive and keyword density-based supervised machine learning techniques for malicious webpage detection. Soft Computing, 2019.

[34] Christopher C. Elisan, Advance Malware Analysis, McGraw-Hill Education, ISBN: 978-0-07-181975-6, 2015.

[35] Alexander Moshchuk, Helen J. Wang, and Yunxin Liu. 2013. Content-based isolation: rethinking isolation policy design on client systems. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (CCS '13). Association for Computing Machinery, New York, NY, USA, 1167–1180. DOI:https:// doi.org/10.1145/2508859.2516722.

[36] Onarlioglu, Kaan, William Robertson and Engin Kirda. "Overhaul: Input-Driven Access Control for Better Privacy on Traditional Operating Systems." 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (2016): 443-454.

[37] Rajeev Kumar, Abhishek Kumar Pandey, Abdullah Baz, Hosam Alhakami, Wajdi Alhakami, Mohammed Baz, Alka Agrawal, Raees Ahmad Khan (2020), Fuzzy-Based Symmetrical Multi-Criteria Decision- Making Procedure for Evaluating the Impact of Harmful Factors of Healthcare Information Security, Symmetry, 12 (664), pp. 1-23. Multidisciplinary Digital Publishing Institute (MDPI). DOI: 10.3390/sym12040664.

[38] Suhel Ahmad Khan, Mamdouh Alenezi, Alka Agrawal, Rajeev Kumar, Raees Ahmad Khan (2020), Evaluating Performance of Software Durability through an Integrated Fuzzy-Based Symmetrical Method of ANP and TOPSIS, Symmetry, 12 (4), pp. 1-15. Multidisciplinary Digital Publishing Institute (MDPI). DOI: 10.3390/sym12040493.

[39] Sanjeev Das, Yang Liu, Wei Zhang, MahinthamChandramohan. Semantics-based Online Malware Detection: Towards Efficient Real-time Protection against Malware. IEEE Transactions on Information Forensics and Security(2019), DOI 10.1109/TIFS.2015.2491300.

[40] Alka Agrawal, Mamdouh Alenezi, Rajeev Kumar, Raees Ahmad Khan (2020), A Unified Fuzzy-Based Symmetrical Multi-Criteria Decision-Making Method for Evaluating Sustainable-Security of Web Applications, Symmetry, 12 (3), pp. 1-23. Multidisciplinary Digital Publishing Institute (MDPI). DOI: 10.3390/sym12030448.

[41] Rajeev Kumar, Asif Irshad Khan, Yoosef B. Abushark, Md Mottahir Alam, Alka Agrawal, Raees Ahmad Khan (2020), An Integrated Approach of Fuzzy Logic, AHP and TOPSIS for Estimating Usable-Security of Web Applications, IEEE Access, Volume 8, Issue 3, pp. 50944-50957. IEEE. DOI: 10.1109/ACCESS.2020.2970245.

[42] Adil Hussain Seh, Mohammad Zarour, Mamdouh Alenezi, Amal Krishna Sarkar, Alka Agrawal, Rajeev Kumar, Raees Ahmad Khan (2020), Healthcare Data Breaches: Insights and Implications, Healthcare, 8 (133), pp. 1-18. Multidisciplinary Digital Publishing Institute (MDPI). DOI: 10.3390/healthcare8020133.

[43] Rajeev Kumar, Asif Irshad Khan, Yoosef B. Abushark, Md Mottahir Alam, Alka Agrawal, Raees Ahmad Khan (2020), A Knowledge Based Integrated System of Hesitant Fuzzy Set, AHP and TOPSIS for Evaluating Security-Durability of Web Applications, IEEE Access, Volume 8, Issue 2, pp. 48870-48885. IEEE. DOI: 10.1109/ACCESS. 2020.2978038.

[44] Gamal Abdel Nassir Mohamed and NorafidaBteIthnin. Survey on Representation Techniques for Malware Detection System. American Journal of Applied Sciences. 2017.

[45] ShahidAlam a, R.NigelHorspool a, IssaTraore b, Ibrahim Sogukpinar. A framework for metamorphic malware analysis and real-time detection. Computer & Science Elsevier, Volume 48, 212-233, 2015.

[46] Alka Agrawal, Adil Hussain Seh, Abdullah Baz, Hosam Alhakami, Wajdi Alhakami, Mohammed Baz, Rajeev Kumar, Raees Ahmad Khan (2020), Software Security Estimation Using the Hybrid Fuzzy ANP-TOPSIS Approach: Design Tactics Perspective, Symmetry, Volume 12 (4), pp. 1-21. Multidisciplinary Digital Publishing Institute (MDPI). DOI: 10.3390/sym12040598.

[47] Abhishek Kumar Pandey, Asif Irshad Khan, Yoosef B. Abushark, Md Mottahir Alam, Alka Agrawal, Rajeev Kumar, Raees Ahmad Khan (2020), Key Issues in Healthcare Data Integrity: Analysis and Recommendations, IEEE Access, Volume 8, Issue 1, pp. 40612-40628. IEEE. DOI: 10.1109/ACCESS.2020.2976687.

[48] Yasuyuki Tanaka, Mitsuaki Akiyama, AtsuhiroGoto. Analysis of Malware Download Sites by Focusing on Time Series Variation of Malware. Journal of Computational Science Elsevier. Volume 22, pp 301-313, 2017.

[49] Rajeev Kumar, Mohammad Zarour, Mamdouh Alenezi, Alka Agrawal, Raees Ahmad Khan (2019), Measuring Security-Durability through Fuzzy Based Decision-Making Process, International Journal of Computational Intelligence Systems, Volume 12, Issue 2, pp. 627 – 642, Atlantis Press. (Previous Publisher: Taylor and Francis). DOI: 10.2991/ijcis.d.190513.001.

[50] Gayatri Kapil, Alka Agrawal, Abdulaziz Attaallah, Abdullah Algarni, Rajeev Kumar, Raees Ahmad Khan (2020), Attribute Based Honey Encryption Algorithm for Securing Big Data: Hadoop Distributed File System Perspective, PeerJ Computer Science, Feb 2020. PeerJ Inc., pp. 1-32. DOI: 10.7717/peerj-cs.259.

[51] K. Sahu and Rajshree, Software Security: A Risk Taxonomy, International Journal of Computer Science & Engineering Technology. pp. 36-41, 2015.

[52] Rajeev Kumar, Suhel Ahmad Khan, Alka Agrawal, Raees Ahmad Khan (2018), Measuring the Security Attributes through Fuzzy Analytic Hierarchy Process: Durability Perspective, ICIC Express Letters-An International Journal of Research and Surveys, Volume 12, Number 6, pp. 615-620. DOI: 10.24507/icicel.12.06.615.

[53] Mamdouh Alenezi, Alka Agrawal, Rajeev Kumar, Raees Ahmad Khan (2020), Evaluating Performance of Web Application Security through a Fuzzy based Hybrid Multi-Criteria Decision-Making Approach: Design Tactics Perspective, IEEE Access, Volume 8, Issue 1, pp. 25543-25556. IEEE. DOI: 10.1109/ACCESS.2020.2970784.

[54] Rajeev Kumar, Suhel Ahmad Khan, Raees Ahmad Khan (2016), Durability Challenges in Software Engineering, CrossTalk-The Journal of Defense Software Engineering, July/August, pp. 29-31, Software Technology Support Center (STSC). (Available at: http://static1.1. sqspcdn.com/static/f/702523/27213496/1472233523657/201609-Kumar.pdf?token=OW3YGQ6YHTeC66R3FYAtESkLyNg%3D).

[55] RabiaTahir. A Study on Malware and Malware Detection Techniques. I.J. Education and Management Engineering. 2, 20-30, 2018.

[56] Zahra Bazrafshan, HashemHashemi, Seyed Mehdi HazratiFard, Ali Hamzeh. A Survey on Heuristic Malware Detection Techniques. 5th Conference on Information and Knowledge Technology (IKT), 2013.

[57] Alka Agrawal, Mamdouh Alenezi, Rajeev Kumar, Raees Ahmad Khan (2019), Measuring the Sustainable-Security of Web Applications through a Fuzzy-Based Integrated Approach of AHP and TOPSIS, IEEE Access, Volume 7, Issue 11, pp. 153936-153951. IEEE. DOI: 10.1109/ACCESS.2019.2946776 .

[58] Abhishek Kumar Pandey, Ashutosh Kumar Tripathi, Mamdouh Alenezi, Alka Agrawal, Rajeev Kumar, Raees Ahmad Khan (2020), A Framework for Producing Effective and Efficient Secure Code through Malware Analysis, International Journal of Advanced Computer Science and Applications, Vol. 11, Issue 2, pp. 497-503, The Science and Information (SAI) Organization Limited. DOI: 10.14569/ IJACSA.2020.0110263.

[59] Abdullah Algarni, Masood Ahmad, Abdulaziz Attaallah, Alka Agrawal, Rajeev Kumar, Raees Ahmad Khan. (2020), A Fuzzy Multi-Objective Covering-based Security Quantification Model for Mitigating Risk of Web based Medical Image Processing System, International Journal of Advanced Computer Science and Applications, Vol. 11, Issue 1, pp. 481-489, The Science and Information (SAI) Organization Limited. DOI: 10.14569/IJACSA.2020.0110159.

[60] Alka Agrawal, Mamdouh Alenezi, Suhel Ahmad Khan, Rajeev Kumar, Raees Ahmad Khan (2019), Multi-level Fuzzy System for Usable-Security Assessment, Journal of King Saud University-Computer and Information Sciences, pp. 1-9, (Article in Press) April 2019, Elsevier. DOI: https://doi.org/10.1016/j.jksuci.2019.04.007.

[61] K. Sahu, and R. K. Srivastava, " Needs and Importance of Reliability Prediction: An Industrial Perspective", Information Sciences Letters. Information Sciences Letters, Vol.9, issue 1, pp. 33-37, 2020.

[62] Alka Agrawal, Mamdouh Alenezi, Rajeev Kumar, Raees Ahmad Khan (2019), A Source Code Perspective Framework to Produce Secure Web Application, Computer Fraud & Security, Volume 2019, Issue 10, pp. 11-18, Elsevier. Available at Thomson Reuters. DOI: https:// doi.org/10.1016/S1361-3723(19)30107-1.

[63] Rajeev Kumar, Suhel Ahmad Khan, Alka Agrawal, Raees Ahmad Khan (2018), Security Assessment through Fuzzy Delphi Analytic Hierarchy Process, ICIC Express Letters-An International Journal of Research and Surveys, Volume 12, Number 10, pp. 1053-1060. DOI: 10.24507/icicel.12.10.1053.

[64] K. Sahu and Rajshree, “Stability: abstract roadmap of security”, American International Journal of Research in Science, Engineering & Mathematics, pp. 183-186, 2015.

[65] Alka Agrawal, Mamdouh Alenezi, Rajeev Kumar, Raees Ahmad Khan. (2019), Securing Web Applications through a Framework of Source Code Analysis, Journal of Computer Science, Volume 15, Issue 12, pp. 1780-1794, Science Publications. DOI : 10.3844/jcssp.2019.1780.1794.

[66] Mamdouh Alenezi, Rajeev Kumar, Alka Agrawal, Raees Ahmad Khan (2019), Usable-Security Attribute Evaluation using Fuzzy Analytic Hierarchy Process, ICIC Express Letters-An International Journal of Research and Surveys, Volume 13, Number 6, pp. 453-460. DOI: 10.24507/icicel.13.06.453.

[67] Rajeev Kumar, Suhel Ahmad Khan, Raees Ahmad Khan (2015), Revisiting Software Security Risks, British Journal of Mathematics & Computer Science, Volume 11, Issue 6, pp. 1-10, SCIENCEDOMAIN International. DOI: 10.9734/BJMCS/2015/19872.

[68] K. Sahu and Rajshree, Helpful and Defending Actions in Software Risk Management: A Security Viewpoint, Integrated Journal of British, pp. 1-7, 2015.

[69] Rajeev Kumar, Suhel Ahmad Khan, Raees Ahmad Khan (2014), Software Security Durability, International Journal of Computer Science and Technology, Vol. 5, Issue 2, pp. 23-26, Unit of Cosmic Journals Group. (Available at: http://ijcst.com/vol52/1/rajeev_kumar.pdf).

[70] Alka Agrawal, Mamdouh Alenezi, Dhirendra Pandey, Rajeev Kumar, Raees Ahmad Khan (2019), Usable-Security Assessment through a Decision Making Procedure, ICIC Express Letters-Part B, Applications, Volume 10, Number 8, pp. 665-672, IEEE. DOI: 10.24507/icicelb.10.08.665.

[71] Kavita Sahu, Raj Shree, Rajeev Kumar (2014), Risk Management Perspective in SDLC, International Journal of Advanced Research in Computer Science and Software Engineering, pp. 1247-1251. (Available at: http://ijarcsse.com/Before_August_2017/3_March2014.php).

[72] K. Sahu, and R. K. Srivastava. "Revisiting software reliability." Data Management, Analytics and Innovation. Springer, Singapore, 2019. 221-235.

[73] Katsunari Yoshioka, Yoshihiko Hosobuchi, TatsunoriOrii, Tsutomu Matsumoto. Vulnerability in Public Malware Sandbox Analysis Systems. 10th Annual International Symposium on Applications and the Internet, 978-0-7695-4107-5/10, 2010.

[74] K. Sahu, and R. K. Srivastava, “Soft Computing Approach for Prediction of Software Reliability”, ICIC Express Letters, Vol.12, No.12, pp. 1213–1222, 2018.

[75] Wagner, M., Fischer, F., Luh, R., Haberson, A., Rind, A., Keim, D., Aigner, W., Borgo, R., Ganovelli, F., Viola, I.: A Survey of Visualization Systems for Malware Analysis. In: EG Conference on Visualization (EuroVis)-STARs, pp. 105–125. EuroGraphics (2015).

[76] Rami Sihwail, Khairuddin Omar, K. A. Z. Ariffin. A Survey on Malware Analysis Techniques: Static, Dynamic, Hybrid and Memory Analysis. International Journal Advance Science Engineering Information Technology. Vol.8 (2018) No. 4-2 ISSN: 2088-5334, 2018.

[77] Malware Analysis Market (2020 to 2026) - Global Industry Analysis, Trends, Market Size, and Forecasts, Avaliable at: https://www.businesswire.com/news/home/20200626005281/en/Malware-Analysis-Market-2020-2026---Global.