Security Measurements of Internet Website Zone for IE ٩ Based on Fuzzy Logic

Lecturer Dr. Mohammed Ali Tawfiq
Computer and Software Engineering Department, College of Engineering, Al-Mustansiriya University, Baghdad, Iraq (e-mail: drmatawfiq@yahoo.com).

Abstract

Internet security zones are an Internet Explorer (IE) features that allow users to access websites based on their level of trust. Internet explorer assigns all websites to one of four security zones, in which, each zone has some settings that specifies its standard security level. IE categorizes the security to five levels represented by linguistic variables (Low/ Medium-Low/ Medium/ Medium-High/ High). Combination between different standard individual setting, or changing the standard setting will produce a custom level of security with undefined value. Indicating a scaled numeric value to the security level of Internet website zones gives a valuable sense to the users even when these levels are customized. The main contribution of this paper is to put forward a method to measure the security of IE ٩'s Internet website zone for standard and customized security levels. This method is based on fuzzy logic system. The designed system considers two boundary limits to the security level. These two limits are considered to be within the interval [٢٠-٩٠] of a total scale of ١٠٠ units. It is found that the evaluated output of the fuzzy inference system (FIS) for different individual settings is proportional to the degree of the required security level.

Index Terms— **Fuzzy logic, IE٩ security levels, Website zone**.

قياس امنية مواقع الانترنت لمستعرض الانترنت IE ٩ اعتمادا على المنظم الضبابي

م .د محمد علي توفيق
قسم هندسة الحاسبات والبرامجيات
كلية الهندسة /الجامعة المستنصرية
العراق /بغداد

الخلاصة:

ان أمنية انطقة الانترنيت هي عبارة عن ميزات لمستعرض الانترنيت (IE) التي تسمح للمستخدمين بالوصول الى مواقع الانترنيت اعتماداً على مستوى موثوقية الموقع. يصنف مستعرض الانترنيت كافة الانطقة الى أربعة أصناف اعتماداً على مستوى امنيتها التي يتم تحديدها اعتماداً على بعض الاعدادات القياسية وان أي موقع من مواقع الانترنيت يقع ضمن أحد هذه

الانطقة. كما ان هنالك خمسة مستويات امان قياسية معتمدة في مستعرض الانترنيت جرى تقسيمها باستخدام متغيرات لفظية هي (منخفض/ متوسط - منخفض/ متوسط/ متوسط - عالي/ عالي). ان الجمع ما بين اعدادات مستويات الامان أو تغيير بعض من هذه الاعدادات سينتج عنه مستوى امني مخصص غير قياسي وغير معروف القيمة. ان استحداث مقياس رقمي الى مستوى أمنية مواقع الانترنيت يعطي انطباع قيم ومطمئن للمستخدمين سواء كان مستوى الامنية قياسي او مخصص. ان الهدف الرئيسي من هذا البحث هو تقديمه لطريقة مستحدثة لقياس مستوى امنية انطقة مستعرض الانترنيت النسخة التاسعة (IE ٩) للمستويات القياسية والمخصصة وتعتمد هذه الطريقة على نظام المنطق الضبابي. تم اعتماد قيمتين تمثل الحدود النهائية لمستوى الامنية في النظام المصمم تنحصر في الفترة [٢٠ – ٩٠] ضمن قياس كلي يبلغ ١٠٠ وحدة. وقد وجد ان مخرجات منظومة الاستدلال الضبابي التي تم تقييمها لأعدادات مختلفة تتناسب مع مستوى الامنية المطلوبة.

١. INTRODUCTION

Different standard security levels are available in Internet Explorer (IE). These levels can determine the security of Internet website zones. IE categorizes the security to five standard levels using the following linguistic variables, “High”, “Medium-high”, “Medium”, Medium-low”, and “Low”. Each security level has its individual settings. These settings can be changed, either by using the IE slider controls, or by changing the status of the individuals. In some cases, when visiting a new or an unfamiliar websites, it is recommended that the security setting should be in High level, which means preventing some features. But when working on trusted websites, and there is a need to access the features that the High setting doesn’t permit, then the security level should be reduced. In some cases it is required to change the states of some individuals which bring up a customized security level. The customized settings have undefined security value and there were no any indication on which level the setting is now. With no any adopts, this will make the user confused about the new security level. To handle this problem we found that it is better to describe the security level with numeric values rather than linguistic variable, for both standard and customize settings.

Fuzzy logic (FL) is a convenient way to map an input space to an output space. The distinctive feature of FL is that in FL everything is, or is allowed to be, a matter of degree **[١]**. FL is almost synonymous with the theory of fuzzy sets, a theory which relates to classes of objects with unsharp boundaries in which membership is a matter of degree. Another basic concept in FL, which plays a central role in most of its applications, is that of a fuzzy if-then rule or, simply, fuzzy rule **[٢].**

The configuration of website zones' security can be found in several literatures. Authors literatures try to manage, evaluate, and analyze website zone security. A full description to IE security zones, architecture, configuration, and standard settings can be found in **[٣].** Ref. **[٤]** analyzed the network system faced by common threats and attack methods and introduced a solution to the existing security problem in current website system.

Schechter, et, al,**[٥]** evaluate some website authentication measures and investigate how a study's design affects participant behavior. Ref. **[٦]** introduces an approach for service governance framework that deals with the security. The derived approach was implemented in a healthcare website application for demonstrating how security issues are tacked.

Adding or removing a website to a specific zone to control the level of security in Windows IE٧ and IE٨ is illustrated in **[٧]**. Boem-Hwan, et al. **[٨]** proposed a security management framework based on secure zone. Khandewa **[٩]** proposed an approach in website security mechanism with respect to E-Commerce trust management. Schechter, et al. **[١٠]** evaluated website authentication that are designed to protect users from man-in-the-middle, phishing, and other site forgery attacks. Wei Wang and Xito Lin **[١١]** established a website performance analysis model, then find out the factors that influence the level of website performance. The management of URL security zones with full description about how administrators can customize the default URL security zones can be found in Ref**. [١٢].**

This paper is organized as follows; the next section describes security zones in Internet explorer. Section ٣ introduces the standard security settings. In section ٤ the security measurements based on fuzzy logic are described. The evaluated and calculated results are contained in section ٥, while, section ٦ presents the conclusion of this work.

٢. SECURITY ZONES IN INTERNET EXPLORER

Security zones can be defined as Internet Explorer features that allow sorting websites depending on their level of trust in them. Internet Explorer assigns all websites to one of four security zones: "Internet", "local intranet", "trusted sites", or "restricted sites". Each of these zones has a different default security level; however these levels can be modified and controlled.

٢,١ Local Intranet Zone

By default the Local Intranet Zone contains all networks connections that were established using a Universal Naming Convention path or has names that do not contain periods **[١٣]**. In general, the Local Intranet zones are used for content located on an organization's intranet. This is because the servers and information are within an organization's firewall. The default security level for the Local Intranet zone is set Medium-Low in Internet Explorer ٩.

٢,٢ Trusted Sites Zone

The Trusted Sites zones are used for content located on Web sites that are considered more reputable or trustworthy than other sites on the Internet.

The Trusted Sites zone has a Medium level of security in IE٩, which is higher than the local Intranet zone but low enough to allow various types of enhanced content to run or be displayed.

٢,٣ Restricted Sites Zone

The Restricted Sites zones are used for Web sites that can cause problems or contains malicious files that can damage computer's system when downloaded. Using this zone causes the Internet Explorer to alert if there were potentially-unsafe content about to download, or to prevent that content from downloading. The Restricted Sites zone has a High level of security.

٢,٤ Internet Zone

The Internet zone can be used for the Internet websites that do not belong to another zone. This default setting causes Internet Explorer to prompt the user whenever potentially unsafe content is about to download. Note: Web sites that are not mapped into other zones automatically fall into this zone. By default, in IE٩ the Internet zone uses the Medium-High setting.

٣. Standard security Settings

The zone to which a website is assigned specifies the security settings of that site. These settings can be controlled and/or modified either by using the IE's slider controls, or by changing the security setting options to a customize one. A numerous custom options for setting individual security features are available.

The following articles and tables show how IE٩ sets every option of features to each of the standard security levels for different IE's classes. The nomenclature used in these tables is as follows:

D: Disable, **E:** Enable, **P:** Prompt, **L:** Low, **ML:** Medium-Low, **M**: Medium**, MH:** Medium-High, **H**: High.

٣,١ .NET Framework

The .NET Framework is an integral Windows component that supports building and running the next generation of applications and XML Web services. The .NET Framework has two main components: the common language runtime and the .NET Framework class library. The common language runtime manages memory, thread execution, code execution, code safety verification, compilation, and other system services. The .NET Framework class library is a collection of reusable types that tightly integrate with the common language runtime **[١٤].** The standard individual setting for this class is shown in table ١.

Table ١ .NET Framework standard setting

Class: .NET Framework	Individual settings for the standard IE٩ security levels				
	L	ML	M	MH	H
Loose XAML	E	E	E	E	D
XAML browser applications	E	E	E	E	D
XPS documents	E	E	E	E	D

٣,٢ .NET framework-Reliant Components

The settings in this class, which is shown in table ٢, specifically apply to manage controls in the browser (referenced by an object tag) and HREF-exes (managed applications referenced by a link) [١٥].

Table ٢ .NET Framework-Reliant standard setting

Class: .NET Framework-Reliant Components	Individual settings for the standard IE٩ security levels				
	L	ML	M	MH	H
Permissions for components with manifests	H	H	H	H	D
Run components not signed with Authenticode	E	E	E	E	D
Run components signed with Authenticode	E	E	E	E	D

٣.٣ ActiveX and Plug-Ins

ActiveX and Plug-Ins are two technologies directed at the Internet Explorer and Netscape browser platforms respectively. A Microsoft ActiveX control is essentially a simple OLE object that supports the "IUnknown". This section offers solutions for making a control work well in the Internet environment, with the ultimate goal of delivering optimal quality of service to users. Plug-ins are native to Netscape. In many respects they are similar to ActiveX. Table ٣ shows how IE٩ sets every option for each of the security levels for this class.

Table ٣ ActiveX and Plug-Ins standard setting

Class: ActiveX Controls and Plug-Ins	Individual settings for the standard IE٩ security levels				
	L	ML	M	MH	H
Allow ActiveX Filtering	D	D	D	E	E
Allow previously unused ActiveX controls to run without prompt	E	E	E	D	D
Allow Scriptlets	E	E	D	D	D
Automatic prompting for ActiveX controls	E	E	D	D	D
Binary and script behaviors	E	E	E	E	D
Display video and animation on a webpage that does not use external media player	D	D	D	D	D
Download signed ActiveX controls	E	P	P	P	D
Download unsigned ActiveX controls	P	D	D	D	D
Initialize and script ActiveX controls not marked as safe for scripting	P	D	D	D	D
Only allow approved domains to use ActiveX without prompt	D	D	D	E	E
Run ActiveX controls and plug-Ins	E	E	E	E	D
Script ActiveX controls marked safe for scripting	E	E	E	E	D

٣.٤ Downloads

Some files contain objects that have the potential to harm the computer system under some circumstances when downloaded. When the individuals of this class are set to disable, then downloads are prohibited. The standard setting of this class is shown in table ٤.

Table ٤ Downloads standard setting

Class: Downloads	Individual settings for the standard IE٩ security levels				
	L	ML	M	MH	H
File download	E	E	E	E	D
Font download	E	E	E	E	D

٣.٥ Enable .NET Framework setup

Enabling the option of this class will prevent .NET Framework from being installed. It is enabled in all zones except Restricted sites, as shown in table ٥.

Table ٥ Enable .NET Framework setup standard setting

Class: Enable .NET Framework setup	Individual settings for the standard IE٩ security levels				
	L	ML	M	MH	H
Enable .NET Framework setup	E	E	E	E	D

٣.٦ Miscellaneous

This class controls whether users can access data sources across domains, submit nonencrypted form data, launch applications and files from IFRAME elements, install desktop items, drag and drop or copy and paste files, and access software channel features from this zone [٣]. The setting of this class is illustrated in table ٦.

Table ٦ Miscellaneous standard setting

Class: Miscellaneous	Individual settings for the standard IE٩ security levels				
	L	ML	M	MH	H
Access data sources across domains	E	P	D	D	D
Allow META REFRESH	E	E	E	E	D
Allow scripting of Internet Explorer web browser control	E	E	D	D	D
Allow script-initiated windows without size or position constraints	E	E	D	D	D
Allow Web pages to use restricted protocols for active content	P	P	P	P	D
Allow websites to open windows without address or status bars	E	E	E	D	D
Display mixed content	P	P	P	P	P
Don't prompt for client certificate selection when no certificates or only one certificate exists	E	E	D	D	D
Drag and drop or copy and paste files	E	E	E	E	P
Enable MIME Sniffing	E	E	E	E	D
Include local directory path when uploading files to a server	E	E	E	E	D
Launching applications and unsafe files	E	E	P	P	D
Launching programs and files in an IFRAME	E	P	P	P	D
Navigate sub-frames across different domains	E	E	D	D	D
Submit nonencrypted form data	E	E	E	E	P
Use Pop-up Blocker	D	D	E	E	E
Use SmartScreen Filter	D	D	D	E	E
Userdata persistence	E	E	E	E	D
Web sites in less privileged web content zone can navigate into this zone	P	E	E	E	D

٣.٧ Scripting

Scripting options specify how Internet Explorer handles scripts. The setting of this class is shown in table ٧.

Table ٧ Scripting standard setting

Class: Scripting	Individual settings for the standard IE٩ security levels				
	L	ML	M	MH	H
Active scripting	E	E	E	E	D
Allow Programmatic clipboard access	E	E	P	P	D
Allow status bar updates via script	E	E	E	D	D
Allow websites to prompt for information using scripted windows	E	E	E	D	D
Enable XSS filter	D	D	D	E	E
Scripting of Java applets	E	E	E	E	D

٣.٨ User Authentication – Logon

The User Authentication option controls how HTTP user authentication is handled. This is shown in table ٨.

Table ٨ User Authentication standard setting

Class: User Authentication	Individual settings for the standard IE٩ security levels				
	L	ML	M	MH	H
Logon	Automatic logon with current user name and password	Automatic logon only in Intranet Zone	Automatic logon only in Intranet Zone	Automatic logon only in Intranet Zone	Prompt for user name and password

These security options are for ٦٤-bit and ٣٢-bit versions of the Microsoft® Windows® operating system MSDN library,.

٤. Security measurements based on Fuzzy logic

One of the most important steps in fuzzy logic is the definition of the fuzzy rules and the decision on which membership function (MF) to be used on each fuzzy set. The other step is the range of values of each quantitative attribute. These values must be designed to be consistent with the degree of security level in which it represented.

The security settings of IE٩ contain a large number of individuals. It seems to be a difficult problem to represent all of these individuals as inputs to a single fuzzy logic system.

In order to handle this problem, the alternative technique used here is to categorize the security individuals according to their classes. Then a fuzzy inference system (FIS) is used to measure the security level of each class.

According to number of individuals illustrated in the tables ١ through ٨, a weight value w_i (i=١, ٢, …, N) is assigned to each class.

The final degree of measured security level S is determined by:

$$S = \frac{1}{M}\sum_{1}^{N} w_i F_i \qquad \ldots \quad (١)$$

Where, M is the total number of individuals, N is the number of classes, and F_i is the output of fuzzy logic systems for each class. Table ٩ illustrates the weight of each class.

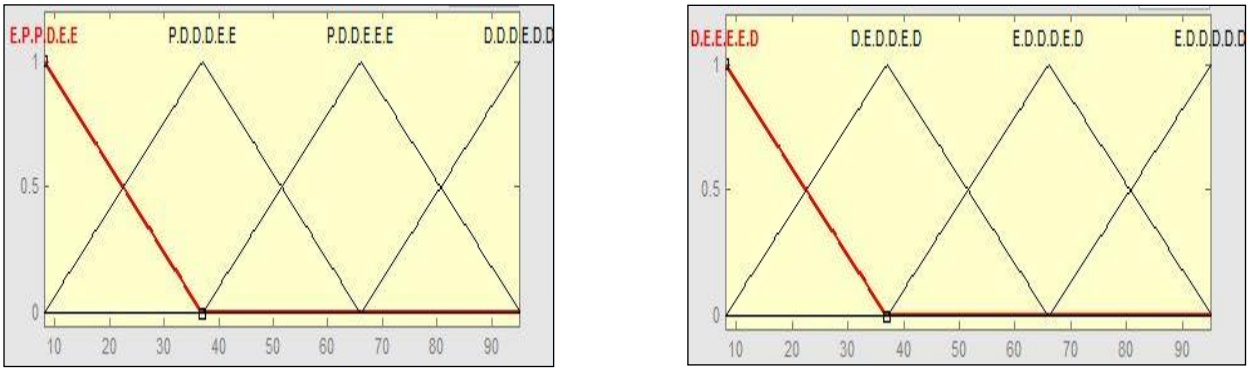
Table ٩ Weights of the classes

Class No.	Class name	Weight
١	.NET Framework	٣
٢	.NET Framework-Reliant Components	٣
٣	ActiveX Controls and Plug-Ins	١٢
٤	Downloads and Enable .NET Framework setup	٣
٥	Miscellaneous	١٩
٦	Scripting	٦
٧	User Authentication	١

In this work the fuzzy rules are based mainly on the standard level setting of the classes and its individuals. Any variation to these settings leads to a new degree of security level.

Two types of MF are used to represent the fuzzy terms depending on the features extracting from the standard setting of the individuals in each class. These functions are the trigonometric and the trapezoidal ones. The inputs' fuzzy set terms used here are (E, D, and P, stand for enable, disable, and prompt, respectively). The combinations of the standard setting between these terms are also used to represent a new fuzzy term that occupies several individuals combined together, such as E.E.E.D.D, which means that this term represents five individuals, in which the first three individuals are in Enable mode, and the last two individual are set to be in Disable mode.

The output set terms are L for Low, ML for Medium-Low, M for Medium, MH for Medium-High and H for High. In more details, consider the case with the class of "ActiveX Control and Plug-Ins". This class consists of ١٢ individuals. The combination standard setting of the first six individuals are assumed to be the first input to the FIS, while the combination of the standard setting of the second six individuals represent the second input to the system. These inputs are as shown in Fig١.



(a) Combination of the first six individual

(b) Combination of the second six individual

Fig. ١ ActiveX Control and Plug_Ins inputs

The output of the FIS is represented by five trigonometric MFs as shown in Fig. (٢).

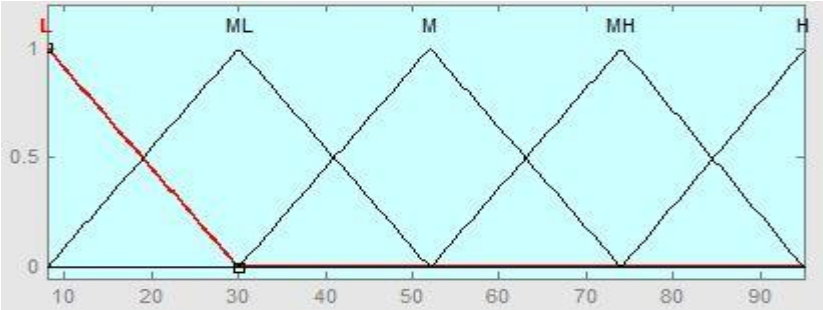


Fig. ٢ ActiveX Control and Plug_Ins outputs

A roadmap of the whole fuzzy inference process for the class of "ActiveX Control and Plug-Ins" is shown in Fig. ٣. In this figure the two plots across the top of the figure represent the first base rule [*If (x١-->x٦ is D.E.E.E.E.D) and (x١٧-->x١٢ is E.P.P.D.E.E) then (ActiveXcontrol is L)*]. Each rule is a row of plots, and each column is a variable (the first variable x١→x٦ is represented by the first column and the second variable x٦→x١٢ is represented by the second column). So the first two columns of the plots show the membership functions referenced by the antecedent of the base rule, or "if-part", of each rule. The third column of plots shows the membership functions referenced by the consequent, or "then-part" of each rule. The aggregation occurs down the rightmost column, and the resultant aggregate plot is shown in the single plot to be found in the lower right corner of the plot field.

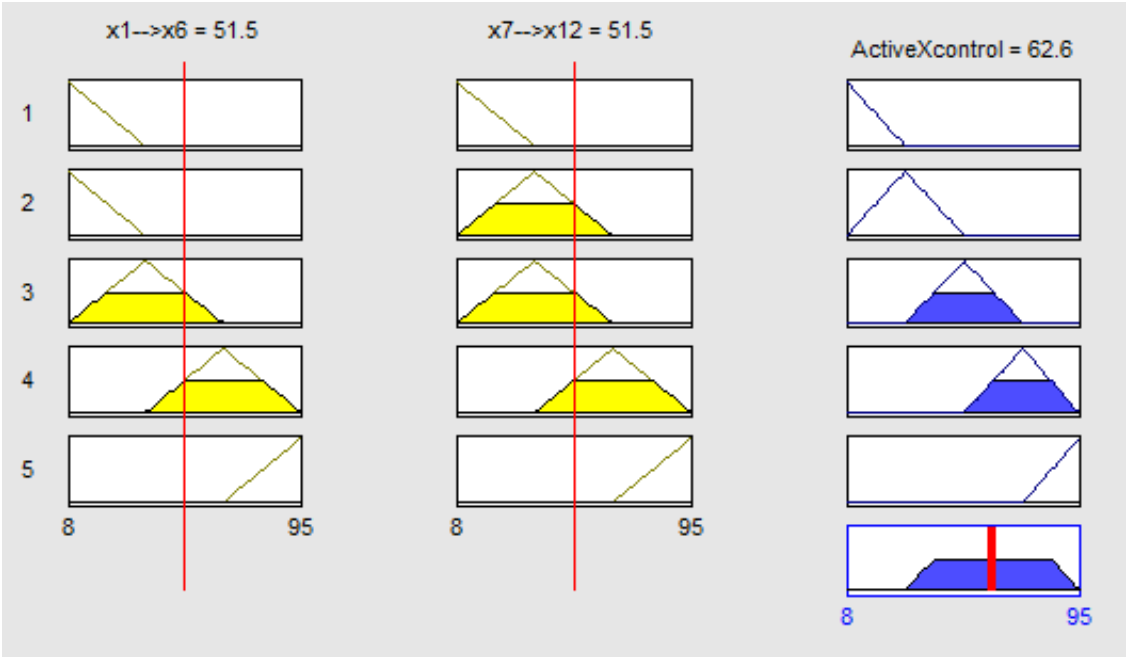


Fig. ٣ Fuzzy inference processes

The center of gravity (CoG) defuzzification method has been used in this work, in which;

$$u = \frac{\sum_{n=1}^{N} I_n \mu_n}{\sum_{n=1}^{N} \mu_n} \quad \ldots (٢)$$

Where, u is crisp output of the fuzzy system, I_n is the interval value, μ_n is the membership value at the interval n , n= ١, ٢, …, N, and N is the total no. of intervals**.**

٥. Results

In determining the range of security level for all the individuals, it is needed to specify the minimum and the maximum security value's level (i.e. the degrees of low and high security levels). The standard High setting is not the highest level. To achieve a higher than high security, or the absolutely maximum high security, then every thing possible should be disabled on a general principles. This will leads to probably never retrieving the desired websites. In the spot of this point we can say the same thing about the standard Low security setting, (i.e., the standard Low doesn't mean it has zero value). Thus, to make the range of values consistent with the degree of security level in which it represented, we have considered the final measurement range of security level to be greater than ٢٠ units (for the standard Low) and less than ٩٠ units (for the standard High) in a total scale of ١٠٠ units.

Because of the large number of individuals, the correlation between each evaluated scaled point and other points are not practical. Thus, the work is designed in a way that the individuals in each class are subgrouped in two main variables. These two variables are the inputs to the FIS system.

The evaluated outputs from each FIS system are subdivided to six equal input periods of equal lengths. These periods are selected in a way that can give a good impression to the behavior of the FIS system for the full range of its output.

The correlations between the values of these periods which represent the measurement of the security level for each class are illustrated in table ١٠ through table ١٦. In these tables the crisp output for the aggregate values calculated according to the CoG method of equation (٢). The final measurements of the overall security levels for all the classes are calculated according to equation (١) and tabulated as shown in table ١٧.

Tables ١٠, ١١, and ١٣ contain the measurements of the security level for class ١, class ٢, and class ٤ respectively. In these tables, it is clear that varying the value of one of the input variables to not more than ٦١ units does not affect the security level. On the other hand when the values of both inputs exceed the ٦١ units, the level of the security is increased to be approximately in the high level. This is because the number of individuals in these classes is very limited. The security level measurements of these classes are shown in Fig. ٤, Fig. ٥ and Fig. ٧ respectively.

Table ١٠ Security level measurements for .NET Framework

Period	١٠	٢٧	٤٤	٦١	٧٨	٩٥
١٠	٤٧,٦	٤٧,٦	٤٧,٨	٥٠,٣	٥١,٥	٥١,٥
٢٧	٤٧,٦	٤٧,٦	٤٧,٨	٥٠,٣	٥١,٥	٥١,٥
٤٤	٤٧,٦	٤٧,٦	٤٧,٨	٥٠,٣	٥١,٥	٥١,٥
٦١	٤٧,٦	٤٧,٦	٤٧,٨	٥٠,٣	٥١,٥	٥١,٥
٧٨	٥١,٥	٥١,٥	٨٥,٦	٨٧,٨	٨٨,٠	٨٨,٠
٩٥	٥١,٥	٥١,٥	٨٥,٦	٨٧,٨	٨٨,٠	٨٨,٠

Table ١١ Security level measurements for .NET Framework-Reliant Components

Period	١٠	٢٧	٤٤	٦١	٧٨	٩٥
١٠	٤٧,٦	٤٧,٦	٤٧,٦	٤٧,٦	٥١,٥	٥١,٥
٢٧	٤٧,٦	٤٧,٦	٤٧,٦	٤٧,٦	٥١,٥	٥١,٥
٤٤	٤٧,٦	٤٧,٦	٤٧,٦	٤٧,٦	٥١,٥	٥١,٥
٦١	٤٧,٦	٤٧,٦	٤٧,٦	٤٧,٦	٥١,٥	٥١,٥
٧٨	٥١,٥	٥١,٥	٥١,٥	٥١,٥	٨٨,٠	٨٨,٠
٩٥	٥١,٥	٥١,٥	٥١,٥	٥١,٥	٨٨,٠	٨٨,٠

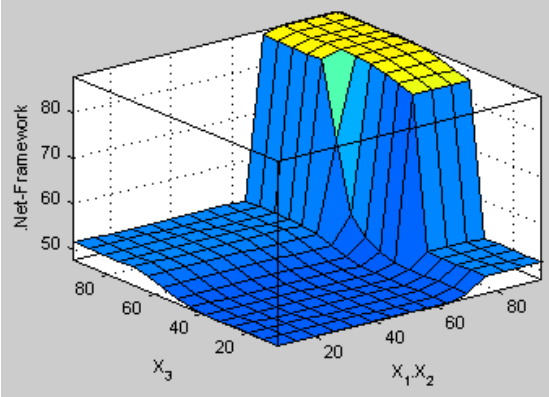


Fig. ٤ .NET Framework sec. level

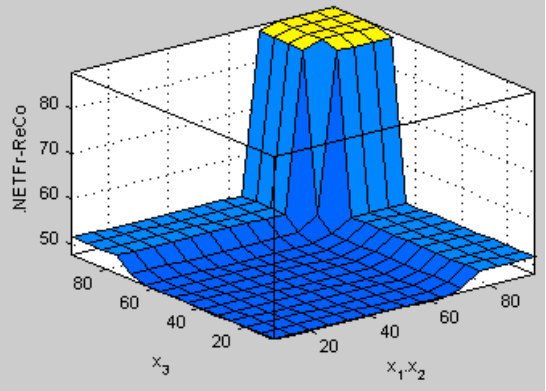


Fig. ٥ .NET Framework-Reliant Components sec. level

The measured security values of class ٣, class٥, and class ٦ are contained in tables ١٢, ١٤, and ١٥. These classes have a large number of individuals; this will leads to construct a wide range of security settings. Thus, the security in these classes has obviously nonlinear levels as it is shown in figures ٦, ٨, and ٩.

Table ١٢ Security level measurements for ActiveX Controls and Plug-Ins

Period	١٠	٢٧	٤٤	٦١	٧٨	٩٥
١٠	٢٢,٧	٣٠,٩	٣٢,٢	٣٥,٨	٥١,٥	٥١,٥
٢٧	٢٨,	٤٢,١	٤٣,٨	٤٣,٨	٥١,٥	٥١,٥

Table ١٣ Security level measurements for Downloads

Period	١٠	٢٧	٤٤	٦١	٧٨	٩٥
١٠	٤٧,٦	٤٧,٦	٤٧,٦	٤٧,٧	٥١,٥	٥١,٥
٢٧	٤٧,٦	٤٧,٦	٤٧,٦	٤٧,٧	٥١,٥	٥١,٥

	٠					
٤٤	٥٢,٠	٥٢,٠	٥٧,٩	٦٤,٦	٧٣,٦	٧٣,٣
٦١	٥٢,٠	٥٢,٠	٦٤,٦	٦٨,٩	٧٣,٦	٧٣,٣
٧٨	٥٢,٠	٥٢,٠	٧٣,٦	٧٣,٦	٧٥,٥	٨٥,٧
٩٥	٥٢,٠	٥٢,٠	٧٣,٣	٧٣,٣	٨٥,٧	٨٧,٦

٤٤	٤٧,٦	٤٧,٦	٤٧,٦	٤٧,٧	٥١,٥	٥١,٥
٦١	٤٧,٧	٤٧,٧	٤٧,٧	٤٨,١	٨٥,٣	٨٥,٣
٧٨	٥١,٥	٥١,٥	٥١,٥	٨٥,٣	٨٨,٠	٨٨,٠
٩٥	٥١,٥	٥١,٥	٥١,٥	٨٥,٣	٨٨,٠	٨٨,٠

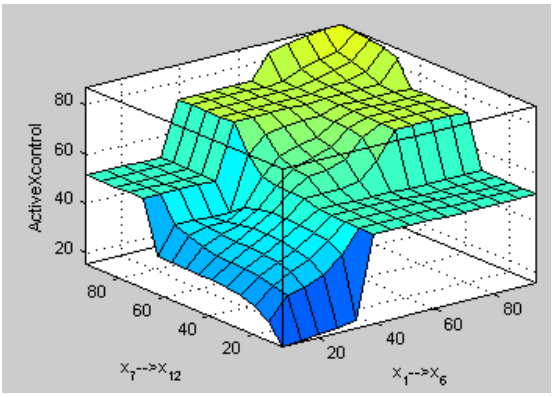


Fig. ٦ ActiveX Controls and Plug-Ins sec. level

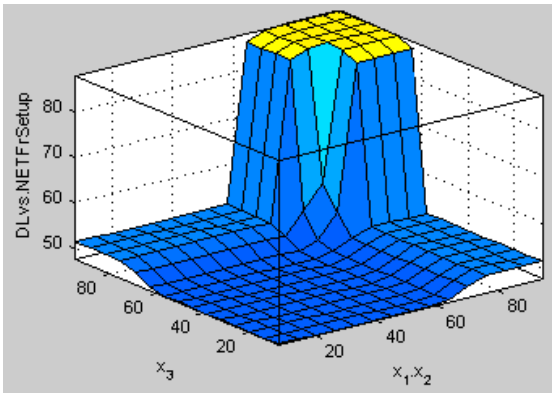


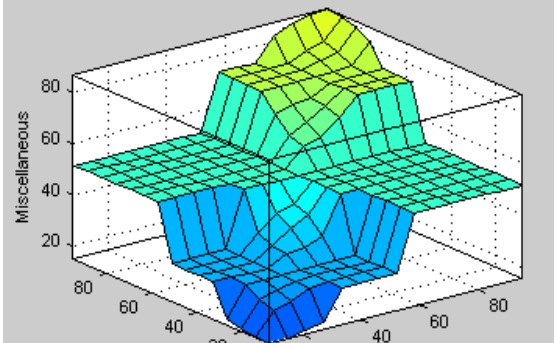
Fig. ٧ Downloads sec. level

Table ١٤ Security level measurements for Miscellaneous

Period	١٠	٢٧	٤٤	٦١	٧٨	٩٥
١٠	١٨,٨	٢٧,٣	٢٩,٨	٥١,٥	٥١,٥	٥١,٥
٢٧	٢٧,٣	٢٩,٥	٢٩,٨	٥١,٥	٥١,٥	٥١,٥
٤٤	٢٩,٨	٢٩,٨	٤٣,٤	٥١,٥	٥١,٥	٥١,٥
٦١	٥١,٥	٥١,٥	٥١,٥	٦١,٣	٧٣,٣	٧٣,٣
٧٨	٥١,٥	٥١,٥	٥١,٥	٧٣,٣	٧٣,٨	٨٣,١
٩٥	٥١,٥	٥١,٥	٥١,٥	٧٣,٣	٨٣,١	٨٧,٠

Table ١٥ Security level measurements for Scripting

Period	١٠	٢٧	٤٤	٦١	٧٨	٩٥
١٠	١٨,٨	٢٩,٥	٣٣,٢	٥١,٥	٥١,٥	٥١,٥
٢٧	٢٢,٣	٢٩,٤	٤٣,٤	٥١,٥	٥١,٥	٥١,٥
٤٤	٥١,٥	٥١,٥	٥١,٥	٥٨,٦	٧٣,٦	٧٣,٧
٦١	٥١,٥	٥١,٥	٥١,٥	٦٧,٤	٧٣,٥	٧٣,٧
٧٨	٥١,٥	٥١,٥	٥١,٥	٧٣,٦	٧٤,٠	٨٤,٢
٩٥	٥١,٥	٥١,٥	٥١,٥	٧٣,٦	٧٤,٠	٨٦,٤



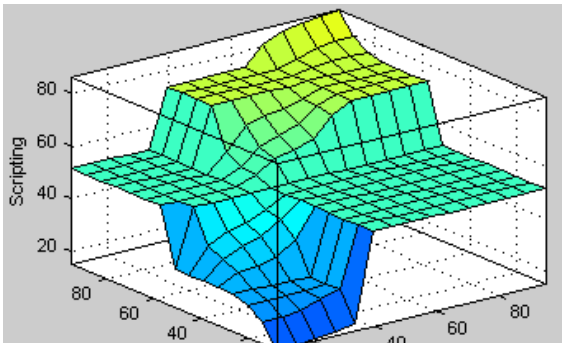


Fig. ٨ Miscellaneous sec. level **Fig. ٩ Scripting sec. level**

Class ٧ (Authentication – Logon) contains only one individual, i.e. there is only one input to the FIS system of this class, thus the output of the fuzzy system here can be easily described as shown in Fig. ١٠. The measured security level of this class is show in table ١٦.

The overall security measurements for all the outputs of the fuzzy systems calculated according to eq.(١) and tabulated as shown in table ١٧, and illustrated in Fig. ١١. It is found that the minimum calculated security level is about ٢٤,٧ units, while the maximum calculated value is about ٨٧,٥ units. These two values represent the standard Low level and the standard High level. The obtained minima and maxima values are met the consideration of the security range for the designed system (i.e., the standard Low is greater than ٢٠ units and the standard High is less than ٩٠ units).

Table ١٦ Security level measurements for User Authentication - Logon

Period	١٠	٢٧	٤٤	٦١	٧٨	٩٥
١٠	١٥,٠	١٥,٠	١٥,٠	١٥.٠	١٥,٠	١٥,٠
٢٧	٤٨,٣	٤٨,٣	٤٨,٣	٤٨,٣	٤٨,٣	٤٨,٣
٤٤	٥١,٥	٥١,٥	٥١,٥	٥١,٥	٥١,٥	٥١,٥
٦١	٥١,٥	٥١,٥	٥١,٥	٥١,٥	٥١,٥	٥١,٥
٧٨	٦٦.١	٦٦,١	٦٦,١	٦٦,١	٦٦,١	٦٦,١
٩٥	٨٨,٠	٨٨,٠	٨٨,٠	٨٨,٠	٨٨,٠	٨٨,٠

Table ١٧ The final measurements of IE٩'s security levels

Period	١٠	٢٧	٤٤	٦١	٧٨	٩٥
١٠	٢٤,٧	٣٢,٢	٣٤,٠	٤٦,٢	٥٠,٧	٥٠,٧
٢٧	٣٠,٥	٣٦,٦	٣٩,٠	٤٨,٢	٥١,٤	٥١,٤
٤٤	٤٢,١	٤٢,١	٤٩,١	٥٥,١	٥٩,٩	٥٧,١
٦١	٥٠,٩	٥٠,٩	٥٤,١	٦١,٣	٧٠,٩	٦٨,٠
٧٨	٥١,٨	٥١,٨	٥٩,٦	٧٣,٥	٧٦,٨	٨٤,٨
٩٥	٥٢,٣	٥٢,٣	٦٠,٠	٧٣,٩	٨٣,٦	٨٧,٥

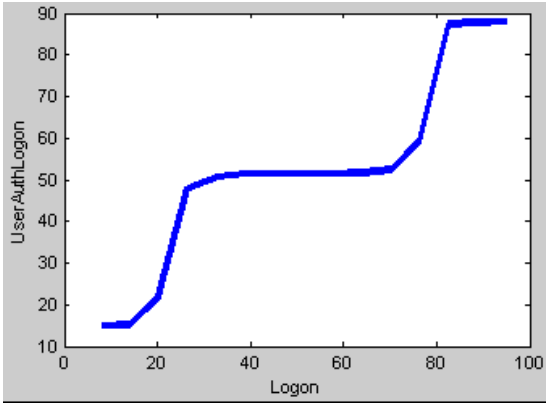


Fig. ١٠ Authentication - Logon sec. level

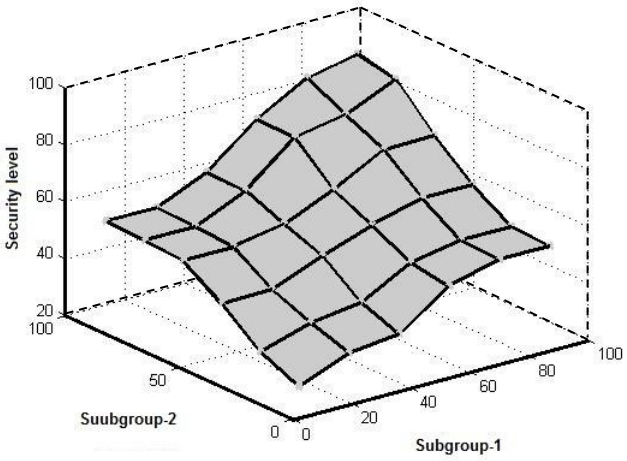


Fig. ١١. Final security level measurements of IE٩

٦. Conclusion

Changing the current security level to the next level using IE slider controls meaning either preventing or permitting the access to many classes or subclasses of features. In general, the movement of IE slider controls is used to pickup one of the standard security levels, in which they are categorized in five main levels (Low, Medium-Low, Medium, Medium-High, and High). But changing the setting of any security individual to be out of the standard one will leads to a customize setting with undefined security level. Thus, giving graduate security level permits the user to prevent or allow the access to a single or a group of features, with a measurement that gives an indication to a meaningful scalable security level. This work introduces a method to measure the security level for IE٩ based on fuzzy logic system.

After evaluating and calculating the security of different individual settings, it is found that the designed method work properly and the measured values are consistent with the degree of required security level.

REFERENCES

[١]. S. Sumathi, Surekha p., "**Computational Intelligence Paradigms**", ٢٠١٠, Taylor and Francis Group, LLC

[٢]. J.-S. Roger Jang, Ned Gulley, "**MATLAB Fuzzy Logic Toolbox User's Guide**", ١٩٩٧, The MathWorks, Inc.

[٣]. Microsoft |TechNet, , "**TechNet Library- Chapter ٤: Security Zones**", Internet Explorer TechCenter, ٢٠١١H .

[٤]. Gaoqi Wei and Xiaoyao Xie, "Research **and solution of existing security problems in current internet_website system** ", ٢nd International Conference on Anti-counterfeiting, Security and Identification, Year ٢٠٠٨, Pages: ١٣٢-١٣٥, IEEE Publisher: IEEE DOI: ١٠,١١٠٩/ IWASID. ٢٠٠٨,٤٦٨٨٣٧٨.

[٥]. Schechter, S.E., Dhamija, R. Ozment, A. and Fischer, I. "**The Emperor's New Security Indicators**", Journal IEEE Symposium on Security and Privacy, ٢٠٠٧.

[٦] Yu, W.D, Srinivasan, K, Pericherla, S. "**An Approach in Security and Privacy for Service Governance Framework"**, IEEE ٧th International Conference on E-Business Engineering Year ٢٠١٠, Pages: ٣١٣-٣١٨.

[٧]. MSDN library, "**adding sites to the enhanced security configuration zones**".

[٨]. Beom-hwan Chang A, Dong-soo Kim B, Hyun-ku Kim B, Jung-chan Na A, et al., " **Active security management based on Secure Zone**", ٢٠٠٨ **,**Citeseer**.**

[٩]. Dr. A.S. Khandelwal, "**Enhancing trust beliefs in e-commerce through whitelist website security paradigm**" , Indian Journal of Computer Science and Engineering ISSN: ٠٩٧٦٥١٦٦, ٢٠١١ Volume: ٢ Issue: ٢ Pages: ٢٤٨-٢٥٤ , DOAJ, Eng Journals Publications

[١٠]. Schechter, S.E., Dhamija, R., Ozment, A., Fischer, I., "**The Emperor's New Security Indicators"**, IEEE Symposium on Security and Privacy (SP '٠٧) ISSN: ١٠٨١٦٠١١ ISBN: ٠٧٦٩٥٢٨٤٨, ٢٠٠٧, pp. ٥١-٦٥, IEEE DOI: ١٠,١١٠٩/SP.٢٠٠٧,٣٥

[١١]. Wei Wang, Xitao Liu, "**Research on Government Website Performance Based on Grey Correlation Analysis to Thirteen Cities in Heilongjiang Province**", ٢٠٠٩ International Conference on E-Business and Information System Security ٢٠٠٩ Pages: ١-٣ Provider: IEEE Publisher: IEEE DOI: ١٠,١١٠٩/EBISS.٢٠٠٩,٥١٣٨٠٤٩

[١٢]. MSDN library, **"About URL Security Zones"**, Available: http://msdn. microsoft.com/en-us/library/ms٥٣٧١٨٣(VS.٨٥).aspx

[١٣]. Winfero Software, "**Internet Explorer Security Zones**", windows-security/internet-explorer-security-zones, ٢٠٠٧.

[١٤]. MSDN library, ".**NET Framework ١,١,٤٣٢٢ .NET Framework ٢,٠,٥٠٧٢٧ .NET Framework ٤".**

[١٥]. Microsoft Support, **"Internet Explorer security zones registry entries for advanced users**", Article ID: ١٨٢٥٦٩, Sep. ٢٠١١.