

Sudan University of Science and Technology
College of Graduate Studies



Internal Cloud Data Firewall
(ICD-Firewall)
الجدار الناري الداخلي لبيانات الحوسبة السحابية

Thesis
Submitted in Partial fulfillment for the Requirements of the
Degree of M.Sc in Computer and Network Engineering

By:
Razan Abdelrahim Mohamed Elnour

Supervisor:
Dr.Rania Abdelhamid Mukhtar

January 2015

ACKNOWLEDGEMENT

In preparing this thesis, I was in contact with many people, researchers, academicians, and practitioners. They have contributed towards my understanding and thoughts. In particular, I wish to express my sincere appreciation to my main thesis supervisor, Dr. Rania Abdelhameed, for encouragement, guidance, critics and friendship. I am also very thankful to Dr. Rashid A. Saeed and Associate Eng. Mohammed Elamian for their guidance, advices and motivation. Without their continued support and interest, this thesis would not have been the same as presented here.

ABSTRACT

Cloud computing has become increasingly popular as the next infrastructure for deploying software and services. Despite the benefits at hand, Cloud data is an important form of cloud computing, Cloud has composed types of cloud attacks many existing and new, so network security of data center is also very important. To protect cloud data centers from these attacks, establishing a cloud firewall is an effective and necessary choice. Traditional firewalls are the first line when defending against malicious traffic. However, the diversity of cloud services and complex attacks make traditional packet level firewalls unsuitable for cloud platform, as typically they are deployed for a local area network which hosts relatively simple and limited services. Addition to the cloud as any web application, the available method doesn't concentrate on this type of attack especially when be internally. This thesis presents implementation of internal cloud data firewall to protect specific script in the web server at the datacenter, through hidden algorithms for sensitive data on (config.file), which is the most significant goal for all type of attacks. ICD-Firewall system is designed to be compatible, simple and more secure. Some useful implications obtained from this system include data integrity, data intrusion from external and internal attack. The security level can be increased with huge number of firewall tables count and size, and insert lines of code to the algorithm to be more complicated, the generation value will be more intruded ,beside of misunderstanding by hackers, so more efficient .Also can increase security level with prevent from script code injection threat.

المستخلص

تقنية الحوسبة السحابية أصبحت متزايدة والعالم متجه نحوها تدريجياً التي تعتمد على مبدأ مشاركة الموارد ومن أهمها وحدات التخزين، الحوسبة السحابية لديها مميزات متنوعة، ناجمة عن موقع الحوسبة أو ناتجة عن المميزات التقليدية للشبكة؛ لذلك حماية البيانات من أهم المشاكل التي تواجه كل مزودي خدمات الحوسبة السحابية.

بيانات المستخدمين المختلفه تحفظ في مراكز بيانات ضخمة، ويكون هنالك جدار ناري للحماية من قبل الأشخاص الغير مخول لهم، لكن تكمن المشكلة هنا في أنه يوجد اختراق داخلي ممن لديهم صلاحيات الوصول لبياناتهم ، وهذا هو أكبر خطر يهدد عالم الحوسبة السحابية.

خدمات الحوسبة يتم الوصول إليها وكأنها تطبيق ويب عبر المتصفح الذي يربطنا بالخادم ومنه لقواعد البيانات لجلب البيانات، وللأسف كل ما يهدد هذا النوع من التطبيقات تعتبر مشكله أساسيه للحوسبة السحابية. التي دائماً يتم اختراقها عبر الهدف وهو ملف التهيئة الذي يحوي بيانات الاتصال لقواعد البيانات (اسم المستخدم \ كلمة المرور)، لذلك عن طرق هذا الملف يتم الدخول لقاعده البيانات التي تحوي بيانات لكل من يقوم بالتخزين عبر الحوسبة السحابية.

لذا في هذا المشروع الهدف تصميم جدار ناري يقوم بحماية الهدف للمخترقين الذي يعتبر الوسيلة التي من خلالها يتم اختراق البيانات، وذلك من خلال اخفاء بيانات الاتصال داخل جداول وهميه تابعة للجدار الناري ، و استبدالها في ملف التهيئة بمتغيرات ; لتضليل المخترق.

الغرض من هذا النظام التوافقيه والسريه للبيانات من حيث سلامة البيانات ، وخداع المخترقين وذلك بالقيم الوهميه التي توجد في قاعده بيانات الجدار الناري، التي كلما زدنا عدد جداولها كلما زدنا مستوى السريه للبيانات، ايضاً كذلك من خلال زياده تعقيد الخوارزمية التي يتم من خلالها توليد قيم جداول الجدار الناري، بمافيهم بيانات الاتصال المخفيه داخله ; وبذلك يصبح النظام أكثر كفاءة.

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	ACKNOWLEDGEMENTS.....	II
	ABSTRACT.....	III
	ABSTRACT IN ARABIC.....	IV
	TABLE OF CONTENTS.....	VII
	LIST OF FIGURES.....	X
1	INTRODUCTION.....	2
	1.1 Preface	2
	1.2 Problem Statement.....	4
	1.3 Proposed Solution.....	5
	1.4 Aim and Objectives.....	5
	1.5 Significance of Study.....	6
	1.6 Thesis Outlines	6
2	BACKGROUND AND LITERATURE REVIEW.....	8
	2.1 Background.....	8
	2.1.1 Cloud Service Provider.....	9
	2.1.2 Cloud Computing Components and Layers.....	11
	2.1.3 Features and obstacle.....	14
	2.1.4 Cloud computing challenges	17
	2.1.5 Security Aspects Focus on in Cloud Computing.....	20
	2.1.6 Threats of Cloud Computing.....	23

2.2	Literature Review.....	28
2.2.1	Security Problems history.....	28
2.2.2	Current solution.....	29
2.2.3	Current problems.....	32
2	METHODOLOGY	35
3.1	ICD-Firewall Technique.....	35
3.2	System Implementation.....	37
3.2.1	ICD Firewall Scenario.....	38
3.2.2	Hiding Algorithm.....	39
3.2.3	System Constructing.....	44
3.2.4	System Interfaces.....	45
4	RESULT AND ANALYSIS.....	48
4.1	Result.....	48
4.2	Analysis.....	53
5	CONCLUSION AND RECOMMENDATION.....	57
5.1	Conclusion.....	57
5.2	Future work.....	57
	REFERENCES.....	59
	APPENDICES	

LIST OF FIGURES

FIGURE NO	TITLE	PAGE
1.1	Demonstrate the IDC rating.....	2
1.2	Typical Topology Diagram for Data Center.....	3
2.1	Main Cloud service providers.....	9
2.2	Cloud Environment Architecture-adopted from NIST.....	11
1.3	The Proposed ICD-Firewall model.....	35
3.2	Process flow inside Web Server.....	36
3.3	The proposed ICD-Firewall Block diagram	37
3.4	ICD firewall scenario.....	38
3.5	Firewall Config file (Wdll.php).....	39
3.6	Phase 1 of Hiding Algorithm.....	40
3.7	Phase 2 of Hiding Algorithm.....	41
3.8	Phase 3 of Hiding Algorithm.....	42
3.9	Phase 4 of Hiding Algorithm.....	43
3.10	System constructing I.....	44
3.11	System constructing II.....	45
3.12	Login Screen.....	45
3.13	DB Info Screen.....	46
3.14	Installation Done Screen.....	46
4.1	Testing Firewall Script.....	48
4.2	Traditional Config file.....	49
4.3	Config file with firewall.....	49
4.4	Login Script Admin Account	50
4.5	Script Admin Account Login successfully	50
4.6	Login Could Data with Real Value.....	51
4.7	Cloud Database Login Successfully.....	51

4.8	Login Cloud Data with Replaced Variables.....	52
4.9	Cloud Data Login Warning.....	52
4.10	Sample of Firewall Tables.....	54