Final Report

For Research Projects Funded through the
National Science, Technology and Innovation Plan (NSTIP)

1. Project Information:

Project ID	**11-INF1609-04**
Project Title	**Modeling and Mitigation of Economic Denial of Sustainability (EDoS) Attacks in Cloud Computing**
Principal Investigator	**Dr. Mohammed H. Sqalli (COE)**
Institution	**King Fahd University of Petroleum & Minerals**
Strategic Technology Area	**Information Technology**
Project Period (Starting Month/Year – Ending Month/Year)	**March 2012 – February 2014**
Reporting Period (Start Month/Year – End Month/Year)	**March 2012 – February 2014**
Report Type: Final (FR), Revised Final (RFR)	**FR**

Project Summary

Through this project we have addressed a novel attack that targets the cloud computing economic resources. The attack, referred to as the Economic Denial of Sustainability (EDoS) attack, occurs when zombie machines (part of a botnet) send a large amount of undesired traffic towards the cloud. The purpose of EDoS attacks is to exploit the cloud's elasticity so as to chalk up an exorbitant amount of cost on a cloud adopter's bill, leading to a large-scale service withdrawal or bankruptcy. We have proposed, implemented, and evaluated a number of techniques for mitigating EDoS attacks, namely, EDoS-Shield, Enhanced EDoS-Shield, and EDoS Defender. We have then used simulation, analytical modeling, and experimentation to evaluate the proposed techniques. And, we have shown that the proposed techniques can improve considerably the behavior of a Cloud under EDoS attacks. The project directly contributed to the strategic goals of NSTIP as the project falls well within the strategic technology area of "Information Technology." Moreover, through the project we have provided numerous approaches for protecting computer networks that are foreseen to provide cloud computing services in the near future in the Kingdom of Saudi Arabia (KSA). The outcomes of the project will help in mitigating the effects of EDoS attacks and make the KSA cloud computing infrastructure more secure.
One of the schemes proposed as part of the project limits the rate of arrival of requests from malicious users who are involved in an EDoS attack. The rate-limiting scheme prevents suspect requests from being granted service before passing further investigative tests. This is accomplished by involving several components, including a firewall, an investigator, a load balancer, and a database, operating hand in hand, to control access to cloud services. Subsequently, the scheme limits access permission for cloud services for each end user based

on the level of trust associated with the end user. This particular value varies based on the rate of arrival of requests from a given source, and other system-level parameters, that are time-dependent and not count-dependent. The proposed mitigation technique is able to detect and mitigate the EDoS attack effectively. Moreover, the cost and user-perceived delays imposed through the scheme in the underlying cloud communications infrastructure were found to be minimal. As part of our future work, we intend to further analyze our proposed rate-limiting scheme and its performance when service provider and network-level parameters are varied, to accurately reflect the behavior of an EDoS attacker against cloud-based services. Moreover, we plan to deploy diverse application scenarios, wherein a variable number of cloud resources will be scaled up and down according to pre-defined criteria, and its impact on the performance of the rate-limiting scheme will be studied. The frequency of update of a maintained black list within the firewall of the proposed scheme will be further studied as it may have an impact on the performance of the attack mitigation scheme. As part of our future work, network-level dynamics will be incorporated so as to help emulate a real computer network within the cloud providers' end, and study the resulting effects on the performance of the proposed scheme.

2. Project Accomplishments

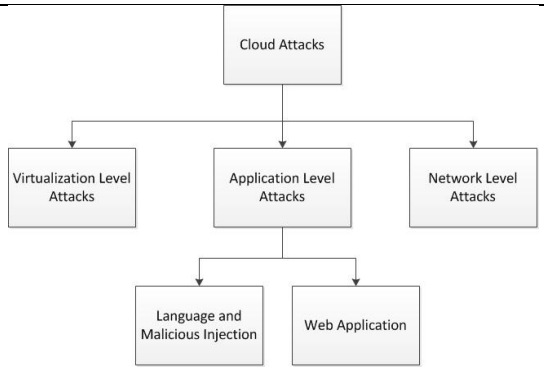
Objectives	Phases	Tasks	**Status** (Completed, Modified*, Discontinued*)	**Percentage of achievement**
1	1	1.a, 1.b	Completed	100
2	1, 2	1.c, 2.a, 2.b, 2.c	Completed	100
3	3	3.a, 3.b, 3.c, 3.d	Completed	100
4	1, 2, 3	1.c, 2.c, 3.d	Completed	100
5	4	4.a, 4.b	Completed	100
6	5, 6, 7	5.a, 5.b, 6.a, 6.b, 7.a, 7.b, 7.c	Completed	100
7	8, 9	8.a, 8.b, 9.a, 9.b, 9.c, 9.d, 9.e	Completed	100

(*) Give details below if Modified or Discontinued.

- **Progress made toward achieving the above objectives, including a description of results;**

  In order to devise techniques for detecting and mitigating EDoS attacks, the team commenced the project by surveying the literature with the objective of identifying the possible causes for EDoS attacks. To achieve this objective, the team reviewed various existing malicious attacks in legacy computer networks that can be used to cause an EDoS attack. Moreover, the team examined several deliberate attacks against the cloud infrastructure with an emphasis on EDoS attacks, and explored existing vulnerabilities in the cloud infrastructure that can be exploited to cause an EDoS attack.

  Subsequently, the team classified the attacks on the cloud infrastructure according to two criteria; the three service delivery models, and the cloud hierarchy level targeted by the attack. The three service delivery models include Software as a Service (SaaS), Platform as a Service (Paas), and Infrastructure as a Service (IaaS). On the other hand, the team classified the attacks that target the cloud security into three categories: virtualization level attacks, application level attacks, and network level attacks. The three categories are shown in the following figure.



The virtualization level attacks target the cloud infrastructure hypervisor, which is also called the virtual machine monitor (VMM). As a result of such an attack, a hacker compromises the hypervisor and gains privileges that would enable him to control all the virtual machines that reside on this hypervisor. In addition to compromising the hypervisor, an attacker can also use a malicious virtual machine to attack and compromise virtual machines from this layer, i.e., hypervisor.

On the other hand, the application level attacks target the applications used in cloud computing. Since the cloud services are accessed through the web, almost all the attacks that are used in regular web applications are applicable to cloud computing. Application level attacks can be further classified to language and malicious injection attacks, and web application attacks. Language and malicious injection attacks target the weaknesses in the programming languages and protocols. Whereas, the web application attacks target the weaknesses of the web services. Application level attacks may either target the end user of the cloud services, or target the cloud solution adopter itself.

In contrast, the network level attacks target the network that is used for accessing the cloud services. Networks are vulnerable to many different types of attacks that may result in disastrous problems to the cloud adopter and/or the end user of the cloud.

Subsequently, and as shown in the following table, the team summarized many of the attacks on the legacy computer networks as well as the attacks on the cloud infrastructure according to the three service delivery models and the cloud hierarchy level targeted by the attack criteria.

	Virtualization Level Attacks	Application Level Attacks		Network Level Attacks
		Language and Malicious Injection	Web Application Attacks	
IaaS	Side channel attack. Timing channel attack. Cross-VMs attack. Indirect Denial of Service attack. Covert Channel Attacks.	-	-	Eavesdropping MITM Attack. Replay Attack. Impersonation Attack. DNS Cache Poisoning Attack. Sniffer Attacks. Byzantine Failure. BGP Prefix hijacking. IP Address Reuse Attack.
PaaS	Cross-VMs attack. Blue Pill attack.	Buffer Overflow Attack. Backdoor and Debug Options.	-	DDoS Sybil Attack. Impersonation Attack. Byzantine Failure.
SaaS	-	Buffer Overflow Attack. XML Signature Wrapping Attack. Trojan horse / Malware. Backdoor and Debug Options. Hidden Field Manipulation Attack. Metadata Spoofing Attacks.	SQL injection Attack. Cross-Site-Scripting (XSS): Stored or Reflected. Cookie Poisoning. CAPTCHA Breaking. DDoS URL Guessing Attack. Phishing Attack.	-

Moreover, the team examined which of the attacks presented in the table above can cause an EDoS attack. Accordingly, the following three tables show the virtualization infrastructure level attacks, the application level attacks, and the network level attacks that may result in EDoS attacks, respectively.

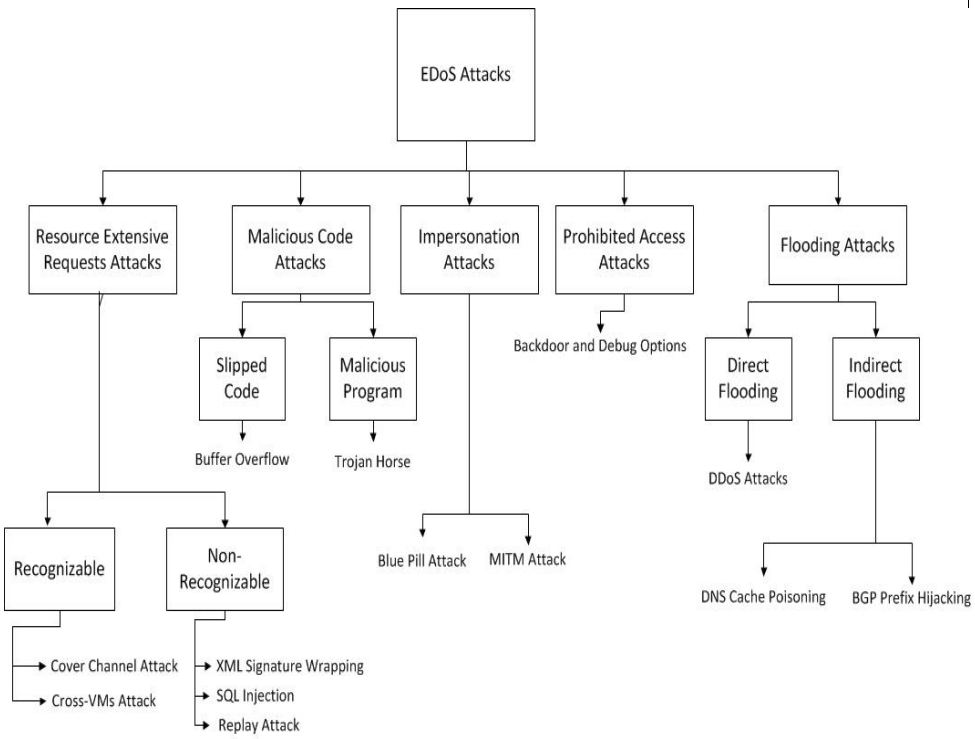
Attack	EDoS?
Covert channel attack	**Yes**
Side channel and Timing channel attacks	No
Cross-VMs attack	**Yes**
Blue Pill attack	**Yes**
Indirect DoS	No

Attack	EDoS?
Buffer overflow attack	**Yes**
XML signature wrapping	**Yes**
Trojan horse	**Yes**
Backdoor and debug options	**Yes**
Hidden field manipulation attack	No

Meta data spoofing	Indirect

Attack	EDoS?
SQL injection attack	**Yes**
Cross-Site-Scripting (XSS) attack	No
Cookie poisoning	Indirect
CAPTCHA breaking	Indirect
URL guessing	No
Phishing	No

Based on the previous analysis, the team developed the following taxonomy of the EDoS attacks. By categorizing the EDoS attacks into a limited number of categories, a single mitigation technique for an attack category can possibly be used to countermeasure other EDoS attacks that fall under the same category.



Finally, the team explored existing vulnerabilities in the cloud infrastructure that can be exploited to cause an EDoS attack. In addition, the team considered the possible countermeasures for such vulnerabilities. The following table summarizes the findings of the team.

Vulnerability	Classification	Countermeasures

Weak Authentication Schemes	general security issue	▪ Multi-factor authentication technique ▪ Strong password policy ▪ Encrypted transmission for authentication tokens
Pooling and Elasticity Characteristic	cloud feature	▪ Distributed Cloud Intrusion Detection ▪ Confidence-Based Filtering (CBF) ▪ EDoS-Shield
Virtualization	cloud feature	Lack of Resource Isolation: ▪ Protecting the VMs against their VMM ▪ Protecting the VMM ▪ Applying a strong compartmentalization ▪ SilverLine Inter-VM traffic within a host: ▪ Enforce a security policy on each host at VM level ▪ Protecting the VMM
Remote Access to Management Interface	general security issue	▪ Providing a secure protocol for remote access ▪ Fixing the web browser vulnerabilities
Poor Key-Management Procedures	general security issue	▪ Separating the key management from cloud provider ▪ Storing the keys in a restricted location ▪ Use strong key generation functions ▪ Set an expiry date for the key ▪ Trusted Third Party (TTP) ▪ Governmental use of scalable key management and exchange strategies

Several techniques for detecting and mitigating EDoS attacks against cloud infrastructures were proposed, implemented, and tested during the course of the project. Following is a summary of the main techniques:

1. EDoS-Shield: The main idea of the EDoS-Shield is to verify whether the requests coming from users are from a legitimate person or generated by bots. This is achieved by forwarding the first request to a verifier node in the proposed architecture. This verifier node is responsible for the verification process and for updating the white and black lists based on the results of this verification process. The subsequent requests coming from the bots will be blocked by a virtual firewall since their IP addresses will be found in the black list. On the other hand, the subsequent requests coming from legitimate clients will be forwarded directly to the target cloud service since their IP addresses will be found in the white list. As a result, only the requests from legitimate clients will reach the target cloud service and thus mitigating the EDoS attack. The proposed approach reduces the overhead due to indirect routing since subsequent packets after the first successful request would be forwarded directly to the protected cloud service. Moreover, the technique does not require that the IP addresses of the verifier nodes be clear to the public; hence reducing the probability of exploiting these nodes. The proposed approach does not suffer from the problem of location-hiding as it is not required in the approach to hide the location of the protected cloud service. Through simulation, the scheme was tested. It was observed that the EDoS-Shield yields a constant response time regardless of the intensity of EDoS attack traffic. The computational power associated with the scheme was also found to be lower than the case where the scheme is not operational. Therefore, the proposed scheme proved to be very effective in mitigating the EDoS

attack.

2. Enhanced EDoS-Shield: The Enhanced EDoS-Shield is an improved version of the EDoS-Shield mitigation technique. The issue of IP spoofing found in the previous technique was addressed. The TTL values found in the IP header were exploited for the purpose of detecting spoofed IP packets. Any requests to the cloud service originating from these spoofed packets are dropped and therefore the attack mitigation technique proves to be more effective than EDoS-Shield. The response time of the proposed scheme yielded one order improvement in performance when compared to the previous technique. In addition, the overall cost appertaining to computation time and resource utilization was also found to have improved through this enhanced technique.

3. EDoS Defender: As part of the EDoS Defender scheme, user requests are verified for legitimacy. Most existing mitigating techniques use traffic filtering mechanisms, generally, with high overhead. The EDoS Defender does not operate continually, rather it is triggered based on suspicious user activity. Investigation performed by the EDoS Defender leads to dropping of attack traffic subsequent to three phases of operation; Firstly, the auto-scaling threshold of the cloud service is monitored. Requests in excess of a pre-defined threshold are analyzed further. During phase 2, monitoring is done based on the auto-scaling parameters of the cloud service. In this phase, the average CPU utilization is observed based on an upper and a lower level threshold, and therefore automatic scaling of resources is prevented. Once an attack is detected, all new requests are forwarded to the EDoS Defender component. Graphical Turing tests are sent to all users, and only those users correctly responding to these requests are granted access to the cloud service. During phase 3, all requests originating from users failing the Turing test are dropped. The proposed scheme performs well in terms of reducing the cost incurred through processing of illegitimate request, and was found to be a good solution to the EDoS mitigation problem. The performance measures show the effectiveness of the EDoS Defender mitigation technique. This mitigation technique was compared with the EDoS-Shield. The comparison shows that EDoS Defender has an improved performance in terms of mitigating the effect of the EDoS attack in comparison with the EDoS Shield. However, there is a small increase in the response time because of the delay of sending CAPTCHA during the attack, to all suspicious users. Overall, the EDoS Defender mitigation technique showed promising results.

Simulation, analytical modeling, and experimentation all have been carried out to evaluate the performance of the proposed mitigation techniques. And, results have been reported in the form of several conference and journal papers. A diverse set of cloud infrastructures have also been thoroughly investigated in terms of vulnerabilities. Deployments such as VMWare-based, Cloud Stack, and OpenStack, have been investigated, and a feasibility of deployment of these vendor-specific cloud technologies on hardware, for subsequent testing, has been carried out for experimentation purposes. The test-bed used for experimentation ensures Autoscaling and network monitoring, in the presence of attack traffic.

- **Challenges encountered while trying to accomplish the tasks (for example, delays in obtaining equipment, turnover in personnel, or recent scientific discoveries that affected your research program) and how you overcame them;**

  A prime challenge was on clearly defining the EDoS attack, and how existing malicious attacks can lead to such novel attacks. Several brainstorming sessions were conducted and the exercise was fruitful, as the entire team came to an agreement as far as the definition and causes of EDoS attacks are concerned. An important component required for the project was auto-scaling; which was initially thought to be a straight-forward component, required much research and proof-of-concepts from various vendors. Few graduate students who had initially shown interest in the project eventually backed out during the course of the project. Having said that, a total of 7 M.S. students and 2 PhD students were engaged in the project, out of whom 1 PhD student and 3 M.S. students have already completed their theses.

- **Implemented changes to the original objectives, tasks, materials, resources or timeline;**

  A SAR 250,000 VBlock Infrastructure package was originally approved as part of our proposal. However, evolving cloud technology and the interests of the project led us to replace this particular hardware item with several software/hardware resources. All equipment has been utilized efficiently for preparing several test-beds.

  Co-Investigator 3 was unable to continue for the second year due to his other commitments. Tasks assigned to him were distributed among the remaining investigators. As a result the project timeline remained unchanged. We were also successfully able to meet the 24 month deadline to provide the approved deliverables.

3. Personnel Involvement

Provide details addressing the contributions of each person in accomplishing the project tasks/objectives during the reporting period. Include personnel involved that are not supported by NISTP award.

Team Members	Name	Contribution to the Project
Investigator	Dr. Mohammed H. Sqalli (PI)	a. Attended the project meetings and participated in the project related discussions. b. Supervised the team including students. c. Held a weekly meeting to review work accomplishments and distribution of work, and to assess progress and direction. d. Coordinated the preparation and the submission of the first interim report. e. Lead tasks 3.b, 4.a, and 6.b. f. Assisted others on tasks 1.a, 1.c, 2.b, 2.c, 4.b, 5.a, 5.b, 7.a, 7.b, 8.a, 8.b, and 9.a. g. Supervised Fahd Al-Haidari, a PhD student, on his dissertation work titled: "Modeling and Mitigation of Economic Denial of Sustainability (EDoS) Attacks in Cloud Computing" leading to successful defense. h. Supervised Mohammed Al-Kaff, an MS student, in his independent research work titled: "Design and Deployment of a Cloud Computing Platform for Testing Attacks" i. Supervised Saeed Al-Sowail, an MS student, in his independent research work titled: "Impact of Known Attacks on the Cloud" j. Working on several journal papers and conference papers with the above students. k. Presented a seminar entitled "Securing the Cloud from DDoS and EDoS Attacks" at the PMU Cloud 2012 workshop, at PMU, Al-Khobar on April 30th, 2012. l. Presented a COE seminar entitled "Is the Cloud Protected from DDoS Attacks?" at KFUPM on May 8th, 2012. m. Attended CloudCom 2013 conference

		in UK during 1-12-2013 – 7-12-2013. n. Coordinated the preparation of the quotations and the purchase order for the project equipment.
Co-investigators	2. Dr. Zubair Baig, CI-1	a. Attended the project meetings and participated in the project related discussions. b. Presented a seminar entitled 'Cloud Security: Do Legacy Solutions Hold?' at the PMU Cloud 2012 workshop, at PMU, Al-Khobar on April 30th, 2012. c. Presented a seminar titled "Network Intrusion Detection using Intelligent Computing," delivered at Prince Mohammad bin Fahd University, October, 2012. d. Was present during first month of summer for the second year of the project. e. Took care of task 1.b and 6.a completely, with consultancy. f. Lead tasks 2.b, 3.c, 4.b, 5.b, and 7.a. g. Assisted others on tasks 3.b, 6.a, 7.c, 8.a, 8.b, 9.b, 9.c, 9.d, and 9.e.
	3. Dr. Marwan Abu-Amara, CI-2	a. Attended the project meetings and participated in the project related discussions. b. Lead tasks 1.a, 2.a, 3.a, 3.d, 5.a, 7.b, 7.c, 8.a, 8.b, and 9.a. c. Assisted others on tasks 3.c, 4.a, and 6.b, 9.b, 9.c, 9.d, and 9.e. d. Performed duties of Principal Investigator for the last two months of the project. e. Supervised M.S. thesis of one student.
	4. Dr. Adel A. Ahmed, CI-3	a. Attended the project meetings and participated in the project related discussions. b. Lead tasks 1.c and 2.c. c. Assisted others on tasks 2.a and 3.d.
Consultant	Dr. Khaled Salah	a. Collaborated through email providing important insights to project discussions and minutes. b. Had meetings with project investigators to discuss project progress and gave feedback. c. Assisted other investigators in tasks 1.b, 2.a, 3.a, 4.b, 6.a, 7.c, and 9.a. d. Consultation and feedback in editing and reviewing two journal papers and one conference paper on cloud EDoS

		attacks, particularly on the realistic assumptions for the simulation and mathematical modeling to capture the behavior of the EDoS attacks and the effectiveness of the proposed countermeasures. e. Online and Skype consultation on the PhD thesis work of Mr. Fahd Haidari on the subject of EDoS attacks on the cloud. f. Attended PhD defense of Fahd Al-Haidari. g. Attended MS defense of Mohammed Yahya Alkaff and Saeed Omar Alsowail throughskype.
Students	Fahd Al-Haidari, (PhD student)	a. Reviewing the attack model. b. Investigating attack parameters. c. Investigating cloud service parameters like provisioning. d. Proposed new technique to mitigate EDoS attacks and do required simulations. e. Writing a paper about the impact of the attack.
	DhiaaAbdulrab Ali Musleh (PhD student)	a. Investigated several external attacks on cloud computing. b. Investigated how attacks are targeting cloud elasticity. c. Investigated metrics and performance measurements needed to measure and/or identify the attacks. d. Proposed an initial attacks' detection scheme that will enhance the cloud service provider defending against EDoS attacks and maintain the advantage of cloud elasticity.
	Farid Salem Saeed Binbeshr (M.S student)	a. A literature review in the vulnerabilities (weaknesses) of the cloud infrastructures with respect to security. b. Classifying the vulnerabilities that may cause EDoS attack into vulnerabilities inherited from cloud features and vulnerabilities inherited from general security issues. c. Working on scenarios and solutions for the vulnerabilities that can cause EDoS. d. Installed and deployed several cloud infrastructure including CloudStack 3.0.2 with citrix XenServer 6.0.2,

		Citrix CloudPlatform 3.0.5 with citrix XenServer 5.6 SP. e. Investigating the auto-scaling feature of several solutions including NetScaler, RightScale and Scalr. f. Arranging demos for managing CloudStack resources, including autoscaling, with RightScale. g. Installing and configuring citrix Netscaler vpx 10.e. h. Investigating how Windows Server 2012 supports auto-scaling. i. Running DoS attack using Jmeter studying the behavior of that attack using Wireshark. j. Trying multiple load generator tools such as Tsung and LOIC for attack. k. Configuring Lab network. l. Install, configure and finalize design of testbed. m. Get components like auto-scaling and costing to work properly. n. Design experiments. o. Carry out experiments for validation. p. Test and compile results.
	Mohammed Yahya Alkaff (M.S student)	a. Design and Deployment of a private Cloud Computing Platform using VMware vCloud, with components including VMware vCloud Director, VMware vCenter Server, VMware vSphere, VMware vShield Manager. b. Design and Deployment of a private Cloud Computing Platform using open source Eucalyptus. c. Implemented a web server on the public cloud AWS Amazon using EC2 instances (virtual servers on the cloud). d. Investigated the hybrid cloud for the VMware platform using VMware Connector. e. Launch a Denial of service attack on VM configured as a web server on VMware private cloud. f. Using BackTrack and scripts to launch the DoS attack. g. Investigate the Ixia to launch attack on web server. h. Install the latest Eucalyptus open source platform using FastStart, integrate Eucalyptus with Nagios tool.

		i. Connect Eucalyptus with RightScale, Kaavo and Scalr (web based tool) trial version. j. Communicate with GroundWork and enStratus for the features of their tool. k. Investigate the best platform to get Auto-Scaling and Monitoring features. l. Investigated the EDoS existing mitigation techniques. m. Came up with a new mitigation technique namely "EDoS Defender" based on rate control and take some advantages of the EDoS existing mitigation techniques. n. Worked on simulation and cloud-sim simulation to understand how to simulate "EDoS Defender". o. Developed a simulation using C# to study attacks. p. Finalize new mitigation technique namely "EDoS Defender" based on rate control and take some advantages of the EDoS existing mitigation techniques.Do theoretical design of new technique. q. Validate theoretical model with simulations. r. Compile results, prepare, and defend MS thesis.
	Saeed Omar Alsowail (M.S student)	a. DDoS attacks on existing networks have been studied and investigated to find out if they can be transformed to EDoS attacks in the cloud. b. A survey on the vulnerabilities and attacks on the cloud infrastructure has been conducted with an emphasis on EDoS attacks. c. The vulnerabilities in the existing networks that EDoS attackers may exploit have been explored. d. Malicious attacks in computer networks that are applicable to the cloud infrastructure in general have also been explored. e. Configured the lab network to use NAT. This gave us tens of thousands of private IP addresses and simplified remote access. In addition, the network of the lab is now more flexible. f. Prepared a number of documents that

		describes and explains our cloud requirements. g. Prepared a comprehensive taxonomy of cloud attacks that may result in EDoS attack. h. Prepared a journal paper. i. Deployed several cloud platforms including OpenStack (quick start), Rackspace private cloud software (all-in-one-node), Openstack's management node (Folsom Open Source Release), several CloudStack cloud platforms to be used to test autoscaling successfully in the lab. j. Studied autoscaling solutions including RightScale and Scalr. k. Participating in deploying the EDoS-Shield mitigation technique. l. Studying the effect of EDoS attack in a cloud environment where the spot pricing model is used. m. Studying the cloud pricing models in general. n. Built the complete and final testbed that is ready for the experiments. o. Started studying the traffic generation tools. One of these tools will be used for the attack. p. Prepared a paper that have been submitted to a conference, but rejected unfortunately. q. Started preparing a whitepaper that documents how to create a cloud that supports AutoScaling from scratch.
	Rashad Lutfi Salem Balfaqih (M.S student)	a. Studied virtual machines co-residency checking approaches. Also, studied cloud cartography (i.e. mapping instances' locations). b. Studied potential internal attacks among VMs on the same physical machine. c. Investigated the contention over certain shared resources (CPU, memory, hard drive) among VMs within the same physical machine. d. Performed experiments on VMware workstation which examined the shared resource environment using benchmarks, namely: PerformanceTest and BurnIn Test Pro.

		e. Collaborating in deploying an open-source cloud platform, CloudStack. f. Taking part in implementing experimental aspect of proposed EDoS-Shield mitigation technique. Investigated several external attacks on cloud computing systems of different classifications and approaches. g. Investigated how attacks are targeting the feature of cloud elasticity that may affect a cloud service provider economically. h. Participated in configuring the cloud lab network's topology. i. Investigated metrics and performance measurements needed to measure and/or identify the attacks. j. Proposed an initial attacks' detection scheme that will enhance the cloud service provider defending against EDoS attacks and maintain the advantage of cloud elasticity.
	Farooq Riaz Siddiqui (M.S student)	a. Contributed in tasks 8.b through design and deployment of a website.
	Qazi M. Umer (M.S student)	a. Deployment of Private Cloud based on VMware Technology. b. Deployment of Cloud Stack. c. Testing of Eucalyptus (on Virtual Machine). d. Deployment of Private Cloud based on VMware Technology.
	Muhammad Shoeib Arshad, (M.S student)	a. Inventory and assets management. b. Worked on Hyper-V Installation and Configuration in Windows 2008R2.
Research Staff	Yusuf Sharif Hassan (Project Manager)	a. Attended the project meetings and participated in the project related discussions. b. Arranged and coordinated weekly meetings. c. Managed efficient communication between project members and other stakeholders. d. Prepared progress report. e. Procured hardware and software resources. f. Closed procurements. g. Closed project.

	Muneeb Iqbal (Technician)	a. Periodic visits for network and hardware support. b. Technical inspection of the new hardware received. c. Follow up with supplier frequently to deliver the quoted item. d. Connection setup for Mobily internet. e. Movement of Server Racks from remote locations to cloud computing lab. f. Movement of Unused/Obsolete items from 23-083 to 23-017. g. Working on new lab design for 23-083. h. Installation of new server rack in the Lab 22-083 along with the 9 servers, KVM Switch & Network Switch. i. Dismantling and movement of server rack from 22-129 to Lab 22-083. j. Movement and installation of Dell Servers in Lab 22-129 for students. k. Movement of Unused/Obsolete items from 23-083 to 23-017. l. Reroute the networks cables of old server racks.
	Ferdinand Viray (Technician)	a. Periodic visits for network and hardware support. b. Movement of Server Racks from remote locations to cloud computing lab. c. Movement of Unused/Obsolete items from 23-083 to 23-017.
Administrative Staff	M. Hafeez Mughal (Secretary)	a. Arranging and coordinating visit of Dr. Khaled Salah as consultant for the project with relevant university internal departments and with external government departments. b. Performed administrative assistance to communicate with relevant departments for arrangement of resources for project.
	Khurshid Akhter (Secretary)	a. Coordinated with food services department for Dr. Khaled Salah's visit.
Others	Karim Asif Sattar (Engineer)	a. Study the VMware vCloud model and its billing mechanism, b. Study the licensing requirements for Cloud c. Minimum requirements (hardware) for setup of Cloud for the Lab. d. Review of Cloud solutions of

		different vendors (vCloud, Microsoft, vBlock, HP, Fujustu , Ericson, Eucalyptus, XCP). e. Provided hand-on training for IXIA traffic generator. f. Provided suggestions on how to design and implement experimental design of proposed mitigation technique.) g. Expert advice on setting up different modules required for testing and simulation of proposed solutions. h. Minimum requirements (hardware) for setup of Cloud for the Lab.
	Khalid J. Mallick (Engineer)	a. Network Hardware Support. b. Installation of new server rack in the Lab 22-083 along with the 9 servers, KVM Switch & Network Switch. c. Relocation of hardware components as per need. d. Reroute the networks cables of old server racks. e. Installation of new server rack in the Lab 22-083 along with the 9 servers, KVM Switch & Network Switch. f. Relocation of hardware components as per need. g. Reroute the networks cables of old server racks.

Describe any significant changes in personnel and/or their roles over the course of the project. Please include individuals not included in your original proposal that provided significant contribution to the project. Also, report on any change in the status of the participants (e.g., promotion, graduation, etc.) during the award period.

Co-Investigator-3 could not continue in the second year of the project. This was due to the fact that he had numerous other commitments and was unable to spare time for the project. This change was mitigated by assigning his responsibilities to the remaining investigators; Principal Investigator and Co-investigators 1 and 2. Hence, no other investigator had to be included in the project personnel list.

The initial estimation for the project mandated inclusion of several BS students. However, as work initiated and progressed forward, it appeared that more MS students will be needed and the contribution of BS students was not required.

4. Project Outputs

Include information in the following categories that **directly relates** to your NSTIP-funded project. Include details, status, and dates (e.g., accepted, published, submitted, under preparation) for each category that applies to your project.

OUTPUTS:

Patents: *(List details on a separate sheet)*	**Quantity**	**Status**	**Date**
Patent applications			
Patent registrations			
Licenses			
Other research commercialization activities			
Publications: (*List on a separate sheet, the details of the publication, e.g., title, journal, impact factor with source such as Thomson Reuters ISI)*	**Quantity**	**Status**	**Date**
Refereed publications	7	**See details below** ***(One paper has been cited 22 times as of May 31, 2014)***	
Non-refereed publications such as journal articles, reviews, conference papers, books and book chapters			
Presentations	**Quantity**	**Status**	**Date**
State the quantity and list & specify on a separate sheet whether they were conference talks, seminars, lectures, invited talks, etc., and whether they were institutional, regional, national or international.	**4**	**See details below**	
Technical Outputs	**Quantity**	**Status**	**Date**
List below any technical outputs such as CDs, software programs, databases, algorithms, and measurement instruments.			

Service to the Research Community	Quantity	Status	Date
List any membership on national and international science committees, advisory boards, journal editorial boards, conference organizing committees, etc.			
Impact on Policy	**Quantity**	**Status**	**Date**
List any contributions to development of research or clinical guidelines, review protocols, indicators, membership on government advisory committees, commissioned governmental agencies, meetings with policy makers, etc.			
Awards and Honors	**Quantity**	**Status**	**Date**
List any major awards, indicating their scale—regional, national, international—and honors such as academic chairs and endowed positions.			
Other	**Quantity**	**Status**	**Date**
List any other forms of research dissemination that is intended for non-scientific audiences (such as radio talks, newspaper articles, television appearances).			

5. Broader Impacts of the Project

Include information in the following categories that **directly relates** to your NSTIP-funded project. Include details and dates for each category that applies to your project.

Teaching and Training

Describe courses, classes, and workshops that were developed, and your role in the activity (for example, teacher, organizer, developer).

1) **Dr. Mohammed H. Sqalli (PI) in his role as course instructor assigned the following graduate course projects that are related to this NSTIP-funded project:**
   a. **The projects assigned as part of the graduate course on "Computer Network Design (CSE 550)" in the spring of 2012. The projects were on designing a cloud for a university environment. 15 students worked on these projects.**
   b. **The projects assigned as part of the graduate course on "Network Management (CSE 552)" in the fall of 2012. The projects were on developing Cloud Monitoring Tools (CloudMon). The tools were designed to monitor the Cloud, including collecting statistics about the use of cloud resources such as number and size of instances, duration of use, bandwidth utilization, etc. 6 students worked on these projects.**
   c. **The projects assigned as part of the graduate course on "Computer Network Design (CSE 550)" in the spring of 2013. The projects were on designing and implementing a secure and scalable private cloud. 9 students worked on these projects.**

2) **As part of this project,**
   a. **Fahd Abdulsalam Mohammad Al-Haidari defended his PhD in ComputerScience & Engineering at KFUPM in November 2012 entitled: "Modeling and Mitigation of EconomicDenial of Sustainability (EDoS) Attacks in Cloud Computing".**
   b. **Mohammed Yahya Alkaff defended his MSc in Computer Networks at KFUPM in December 2013 entitled: "An Enhanced Mitigation Technique for Economic Denial of Sustainability (EDoS) Attack".**
   c. **Saeed Omar Alsowail defended his MSc in Computer Networks at KFUPM in December 2013 entitled: "Evaluating the EDoS-Shield Mitigation TechniqueUsing an Experimental Testbed".**
   d. **Two other Masters students are completing their MS Thesis as part of this project.**

Infrastructure

If you purchased equipment, describe how it adds to the capability of the institution and training of researchers outside the project. Indicate whether this equipment is available elsewhere in the institution and, if so, why its purchase was necessary for this project.

Equipment purchased has been used to establish at least two Cloud Computing test-beds that are currently being used by students completing their MS Thesis.

The test-beds can be used later by other researchers who are not necessarily working on this project.

It was necessary to purchase this equipment in order to establish a test-beds that can be used for the purpose of this project, i.e., evaluating the impact of EDoS attacks and implementing techniques for mitigating such attacks. No other lab on campus provides a similar test-beds.

Collaborations

Describe the institution, disciplinary focus, research expertise, and nature of any new or unforeseen partnerships that were developed during the project.

1) **The following activities were in collaboration with PMU, Al-Khobar:**
   a. **A seminar entitled "Securing the Cloud from DDoS and EDoS Attacks" presented by Dr. Mohammed H. Sqalli at the PMU Cloud 2012 workshop, at PMU, Al-Khobar on April 30th, 2012.**
   b. **A seminar entitled "Cloud Security: Do Legacy Solutions Hold?" presented By Dr. Zubair Baig at the PMU Cloud 2012 workshop, at PMU, Al-Khobar on April 30th, 2012.**
   c. **A seminar entitled "Network Intrusion Detection using Intelligent Computing," presented By Dr. Zubair Baig at Prince Mohammad bin Fahd University in October, 2012.**

2) **Dr. Mohammed H Sqalli participated in the 3rd Annual Cloud World Forum that was held on19th- 20thMarch at the JW Marriott Marquis, Dubai, UAE. It was an occasion to meet many experts and delegates and discuss the possibilities of collaborations. Some of the solutions discussed include ASG CloudFactory provided by ASG Software Solutions.**

3) **Collaborated with Dr. Khaled Salah at Khalifa University, Sharjah, UAE who provided important insights to the project and participated in co-authoring papers related to the project.**

4) **Collaborated with many vendors including NetScaler for the purpose of finding a suitable solution for our test-bed.**

Funding

Describe how this research has led to additional funding or prospects for future funding awards and contracts for project investigators, students and staff. Please list the applications, dates, reference numbers, and amount awarded, if applicable.

No additional funding related to this research was sought or awarded.

However, based on the initial results obtained, there is a great prospect for future funding.

Contributions to the Strategic Technologies Goals of NSTIP

The following are the Strategic Goals for the Information Technology Area:

- Support an expanding and innovative KSA IT industry.
- Advance IT capabilities to meet critical needs in the Kingdom in areas, such as computer networking and security.
- Develop innovative high quality IT applications to meet specialized needs in the
- Kingdom, such as for the oil and gas industry, and Islamic applications.
- Develop world class capabilities in language technologies, especially applied to serve the Arabic Language.
- Improve scientific and supercomputing facilities to expand the Kingdom's capabilities in science and engineering through modeling, simulation, and visualization.

Others

Describe the benefits of your research to society that are not covered by the categories above.

There is a large proliferation of Cloud Computing in the society and therefore the benefits of such project will be of great use to adopters of the Cloud in the local market.

6. Budget

Category	First year		Second year	
	Amount Awarded	Amount Expended	Amount Awarded	Amount Expended
Principal Investigator	**60,000**	**60,000**	**48,000**	**0**
Co-Investigator	**150,000**	**150,000**	**150,000**	**0**
Consultant	**40,000**	**40,000**	**52,000**	**52,000**
Students (Ph.D)	**30,000**	**30,000**	**22,500**	**22,500**
Students (M.S)	**76,000**	**76,000**	**66,000**	**62,000**
Research Staff (Project Manager)	**25,000**	**25,000**	**25,000**	**0**
Research Staff (Engineer)	**20,000**	**20,000**	**7,500**	**7,500**
Research Staff (Technician)	**11,200**	**11,200**	**11,200**	**11,200**
Administrative Staff	**9,600**	**9,600**	**9,600**	**9,600**
Major equipment (list items >100,000 SR below)	**250,000**	**215,940**	**0**	**0**
Other Equipment (list items >10,000 SR below)	**88,000**	**66,650**	**0**	**0**
Materials & Supplies	**20,000**	**6,548**	**10,000**	**169**
Travel (e.g., training, conference, field trips)	**48,000**	**1,302**	**48,000**	**8,538.88**
Dissemination (e.g., publications, patents, workshops, public outreach)	**0**	**0**	**10,000**	**4888.38**
Other (specify any >1,000 SR)	**0**	**0**	**0**	**0**
Total				

Please list equipment (>10,000 SR) purchased. In addition, provide brief descriptions of travel, dissemination, and other expenditures during the reporting period. If funding sources other than NISTP supported any aspect of the research program, please describe the funding amount and nature of support (financial, in-kind, facilities, etc.) Also, comment on any existing core or shared research facilities that you have used during the course of the project. If the expenditures exceeded or fell short by more than 5 % of the original award in any of the categories above, please comment. (max. 150 words).

Equipment over 10,000:

We had three orders that were over 10,000 SAR. The items procured through these orders are listed below.

1. Servers
2. Network Attached Storage
3. KVM
4. NetScaler

Travel:

1. Dr. Khaled Salah's (Consultant) visit to attend the defense of PhD student Dr. Fahd Al-Haydari.
2. Dr. Sqalli's attended CloudCom conference in UK from 1-12-2013 till 7-12-2013.

Expenditures below 5% than awarded:

1. The category for Co-Investigator will be utilized much less than 95% since one of the co-investigators could not continue for the second year due to his other commitments. Only 66% of the allocation for the second year will be utilized.
2. Major equipment and other equipment heads will also not be utilized 95% or more as it was realized after initial investigation that the initially requested vBlock will not be as useful and buying individual components will be more useful. Also, there was already some equipment at our disposal from previous projects.
3. Materials and suppliers, travel and dissemination expenses cost also much less than the amount awarded. This was due to the fact that not as much supplies were required and the number of trips done were quite less than initially anticipated.

7. Describe any other concerns and comments related to the final reporting of the research project that were not covered in the sections above. (max. 250 words)

Thanks

List of Publications (Published):

1. **Zubair A. Baig and Farid Binbeshr, "Controlled Virtual Resource Access to Mitigate Economic Denial of Sustainability (EDoS) Attacks against Cloud Infrastructures", The IEEE International Conference on Cloud Computing and Big Data (CloudCom-Asia)**, Fuzhou, China, December 16-19, 2013.

2. **Fahd Al-Haidari, Mohammed H. Sqalli, and Khaled Salah, "Impact of CPU Utilization Thresholds and Scaling Size on Autoscaling Cloud Resources",** The 5th IEEE International Conference on Cloud Computing Technology and Science (IEEE CloudCom 2013), Bristol, United Kingdom, December 2-5, 2013.

3. **Mohammed Yahya Alkaff** and **Mohammed H. Sqalli, "Design and Deployment of a Cloud Computing Platform for Testing Attacks,"** The Fourth Scientific Conference for Students of Higher Education in the K.S.A. (SSC4), Makkah, Saudi Arabia, April 29- May 2, 2013.

4. **Mohammed H. Sqalli, Mohammed Al-Saeedi, Farid Binbeshr, and Mohammed Siddiqui, "UCloud: A Simulated Hybrid Cloud for A University Environment",** The 1st IEEE International Conference on Cloud Networking (IEEE CLOUDNET 2012), Paris, France, November 28-30, 2012.

5. **Fahd Al-Haidari, Mohammed H Sqalli, and Khaled Salah, "Enhanced EDoS-Shield for Mitigating EDoS Attacks Originating from Spoofed IP Addresses",** The 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp.1167-1174, Liverpool, United Kingdom, June 25-27, 2012.

6. **Mohammed H. Sqalli, Fahd Al-Haidari,** and **Khaled Salah, "EDoS-Shield - A Two-Steps Mitigation Technique against EDoS Attacks in Cloud Computing,"** The 4th IEEE/ACM International Conference on Utility and Cloud Computing (UCC 2011), Melbourne, Australia, December 5-7, 2011. ***(Cited 22 times as of May 31, 2014)***

7. **Fahd Al-Haidari, Mohammed H. Sqalli, and Khaled Salah, "Evaluation of the Impact of EDoS Attacks against Cloud Computing Services",** Arabian Journal for Science and Engineering (AJSE), Volume 40, Issue 3, pp. 773-785, March 2015.

List of Publications (Submitted or Under Preparation):

8. **Zubair A Baig, Sadiq M. Sait, and Farid Binbeshr, "Controlled Access to Cloud Resources for Mitigating Economic Denial of Sustainability (EDoS) Attacks,"**

Submitted to the Journal of Network and Computer Applications, November 2014.

9. **Mohammed H. Sqalli, Saeed Alsowail, Marwan Abu-Amara, Khaled Salah, and Zubair Baig, "Experimental Evaluation of the Effectiveness of EDoS-Shield Mitigation Technique",** *Submitted to the Journal of Security and Communication Networks (SCN), May 2015.*

10. **Fahd Al-Haidari, Mohammed H. Sqalli, and Khaled Salah, "An Analytical Evaluation of the Effectiveness of the EDoS-Shield Mitigation Technique",** *Under Preparation for a journal submission*.

11. **Mohammed H. Sqalli, Mohammed Yahya Alkaff, Zubair Baig, Khaled Salah, and Marwan Abu-Amara, "EDoS-Defender - A Mitigation Technique against EDoS Attacks in Cloud Computing",** *Under Preparation for a journal submission*.

Presentations:

1. **A seminar entitled "Securing the Cloud from DDoS and EDoS Attacks" presented by Dr. Mohammed H. Sqalli at the PMU Cloud 2012 workshop, at PMU, Al-Khobar on April 30th, 2012.**

2. **A seminar entitled "Cloud Security: Do Legacy Solutions Hold?" presented By Dr. Zubair Baig at the PMU Cloud 2012 workshop, at PMU, Al-Khobar on April 30th, 2012.**

3. **A COE seminar entitled "Is the Cloud Protected from DDoS Attacks?"presented by Dr. Mohammed H. Sqalli at KFUPM on May 8th, 2012.**

4. **A seminar entitled "Network Intrusion Detection using Intelligent Computing," presented By Dr. Zubair Baig at Prince Mohammad bin Fahd University in October, 2012.**

General Secretariat of National Science, Technology and Innovation Plan
King Abdulaziz City for Science and Technology
P. O. BOX 6086 Riyadh 11442
Tel: 014813390 Fax: 014814693
Email : secretariatNSTIP@kacst.edu.sa