The workflow as follow:

1- Registration for Data owner and Data Consumer

   a. Data owner, Data Consumer register to SCaaS

   b. SCaaS generate Key Pair

2- Data owner, Data Consumer, receive Key Pair Public key and Certificate sign request CRS

3- Web server forward CRS to trusted authority local CA

4- CA validate CRS

5- CA transfer certificate to the web server

6- Web server transfer certificate to Do, Data Consumer

7- Data owner, Data Consumer, have now client certificate

Two work case scenarios:

- First, uploading the data second downloading the data.

1- Web server enforces two-factor auth. Firstly by utilizing client certificate secondly by utilizing username and password

2- After user auth. Data owner fill the form and write keywords which describe the components and then upload the file through TLS tunnel

3- Traffic will pass to IPS to check the behaviors.

4- File will pass to Malware detection:

   a. If the file is marked as unknown then it will be forwarded to the sandbox., Sandbox will check for privilege need to run this file and will check for virus, if the file is clean it will be forwarded to proxy

   b. If file is clean it be forward to proxy

   c. If file is infected, it will be dropped. and Sandbox will update the malware protection signature database with the signature of the infected file.

5- The proxy will encrypt the file utilizing PBRE (proxy broadcast re-encryption) technique and save it to the storage.

6- Keywords will be saved in a database for further searching with an agent.

Second Data Consumer wants to download the file from SCaaS:

1- After the registration process

2- Web server will transmit a request to TA to check for authentication

3- Web server will inform Data owner that Data Consumer want to download his file and send the Public key to the Data Consumer

4- Data owner will generate Re-encryption key utilizing his private key and public key for the Data Consumer

5- Data owner will send it to the web server through TLS tunnel

6- Web server will forward Re-encryption key to the proxy

7- Proxy will decrypt the file utilizing PBRE (proxy broadcast re-encryption) technique.

8- DC will receive the file and decrypt it is utilizing his private key.

RESULTS AND DISCUSSIONS

A. Introduction

In this paper, four main sets of experiments have been conducted to develop the proposed security model separately. After that, the four modules, the calculated time and accuracy were integrated. Then the total time taken for the four modules to calculate the availability of SCaaS were calculated. The first set of experiments is developed to evaluate the prevention systems. Data were taken from Information Security Forum (ISF) [27] have been utilized to train the prevention system. Eighteen signatures categories were trained and evaluated in the first experiment. The second experiment is conducted to evaluate the proposed methodology for sandboxing to know behaviors of day zero attacks and least privilege. The third experiments are conducted to evaluate and ensure the data confidentiality. After all, all these systems were integrated together to make the security framework. This chapter presents details about these experiments and the proposed system evaluation.

B. Access Control

The authentication method utilized is dual factor authentication. username and password are first factor while second factor is a digital certificate. Request userid and password. Hash password Retrieve stored user-id and hashed password the Compare after that Make a function call to a network-based authentication service. System Stores User-ids and Passwords. Passwords stored in a database table. User-id stored in plaintext Password stored hashed. Centralized management of access controls. LDAP Active Directory, Microsoft's LDAP. Access Control system tested against Attacks Intruders will try to bypass, trick access controls, defeat to spoil their targets. Attack objectives were found to guess credentials malfunction of access controls or Bypass access controls or Replay known good logins. To avoid Password Cracking frequent password changes, controls on hashed password files, salting hash. To avoid Malicious Code, anti-virus and anti-spyware were utilized. For Spoofing and Masquerading, the firewall to drop forged packets were configured.

C. Evaluation of sandboxing

The proposed sandboxing was tested using different numbers of engines at the same time, when enabling the 12 machines like the researches in [21] made it takes about 78% of the processing memory. Other experiments were made by enable one engine ant a time then the time and processor performance were calculated. Many experiments were made until we found that running five programs at the same time gives the optimum outputs. The below table shows Detection rate for five common antivirus programs as a role of the age of the malware samples as shown in figure 4.

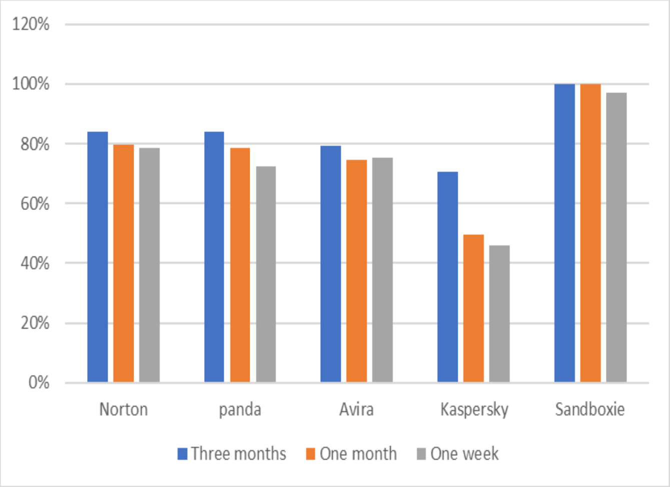

Figure 4. Detection rate over malware samples

After that the accuracy of the proposed sandbox was calculated over three-month malware samples as shown in figure 5

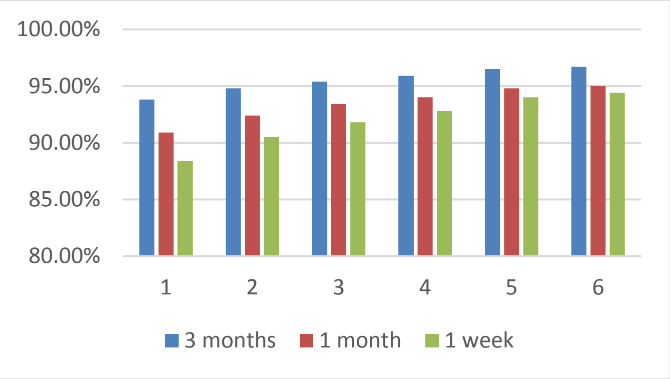

Figure 5. the accuracy of proposed sandbox over 3-months

D. Evaluation of Prevention Systems

In the literature review, prevention systems are utilized to know the behaviors of the traffic comes to the cloud. All the cloud providers must insert prevention systems. Prevention systems evaluated for intrusion prevention systems and malware prevention systems. In Intrusion prevention systems each threat is required to train system before utilizing it by performing some training samples. Then this trained system was put in the framework. Second evaluations are for malware prevention system. the same tests Were made but with different datasets. The accuracy of different datasets was then tested. Predefined datasets were utilized [4] consists of 188 samples for different malware. Training and testing data are collected from many users over different days. In Malware prevention system the evaluation is done on dataset. Experiments, training and testing data are collected from different users over different days. IPS and the time taken were evaluated to scan the traffic against the number of signatures. False Positive FPs or False Negative FNs happen to IPS were analyzed as shown in figure 6 and 7, Malware prevention and sandbox with real traffic and investigates their frequencies at all FPs and FNs. attack types were classified, and the most 19 attack which affects the cloud like DDoS, buffer overflow, Web attack, scan.

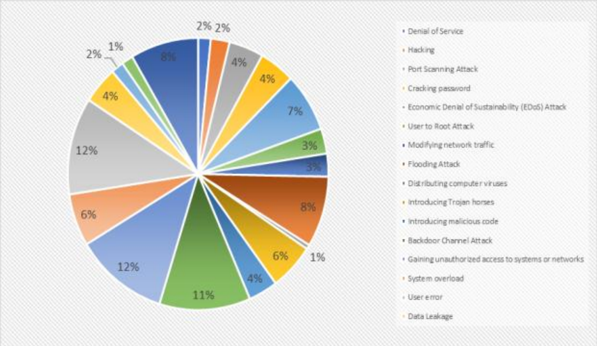

Figure 6. Attack Ranking on FP

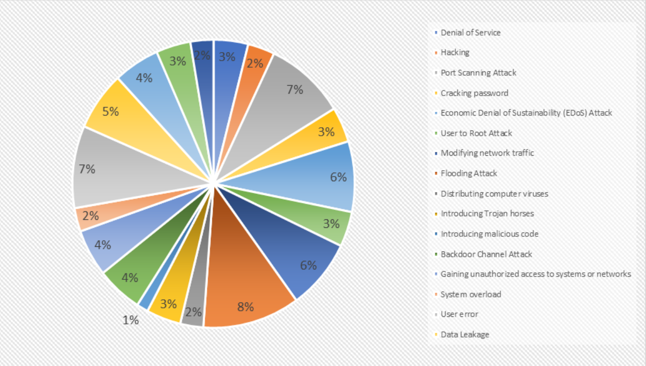

Figure 7. Attack Ranking FN

After implementing the above prevention systems, the time taken was calculated to measure the availability. After doing many experiments found that enable all the signatures in the system will impact the performance and all the signatures in the prevention system will affect the time. many experiments were made to enable only the most threat that has higher hit count and the ones that affect the cloud as summarized in table 1.

Table 1. comparison between no of signatures and time took

Number of Signatures	Time taken in Minutes
30070	10
20010	8.6
10342	6.6
5043	3.8
1276	3
908	2.5
200	1.5
0	1

IPS, the malware prevention and sandboxing were disabled. This is considered as the optimum time the file taken to upload and save to the file storage system. After that all the signatures were enabled which are 30070 it takes 600 seconds which is 10 minutes, the signatures were filtered according to the kind of operating system work on SCaaS (windows) and the kind of software component uploaded, and the kind of files uploaded. And after all, the result from this filtration was 908 signatures will optimum because it fulfills all the categories in 150 seconds.

SECURITY POLICY APPROACHES:

- *Balanced security and availability 908 signature* It is an optimal policy regarding security and availability. This policy has around 908 rules enabled, some of them only generate events whereas others generate events as well as drop the traffic.
- *Security over availability 20010 signature* security over availability was prioritized, which increases the number of enabled rules which will affect the response time of the cloud.
- *Availability of security 200 signature* If the priority is that the response time of the cloud is important rather than security, availability of security policy then could be chosen. which will reduce the number of enabled rules.
- *No Rule Active* This option disables all rules.

The first approach which is “Balanced security and availability” was chosen so 908 rules were applied over the dataset with different sizes. After testing each system separately, all these systems were integrated to propose the security framework the time was calculated for each step separately to calculate the availability time. For system performance evaluation, 708 software components 320 malware and 388 clean codes and 908 threats are utilized. The results are obtained utilizing a 10-fold cross-validation technique in each system. The system detects accuracy by 90.67% while recognizes threats behaviors with 81.25% accuracy. The purpose of the experimentations is to prove the effectiveness of the whole security framework. Time for every subsystem is calculated to which will be compared to availability as shown in table 2. The experiments run a simulation, the features of the machine are as follows: First server for LDAP and Certificate authority server, Second server webserver. The third server is for prevention systems it consists of 2 virtual machines one for IPS and Malware second for sandboxing.

Table 2. Average time verses apply 908 signature availabilities

Data size	Access Control	Prevention system	PBRE	The system available after	The system available after
<5K	57 sec.	150 sec.	45 sec.	252 sec.	4.2 min
5 – 10 K	57 sec.	150 sec.	61.7 sec.	268.7 sec.	4.47 min
>10K	57 sec.	150 sec.	66.8 sec.	273.8 sec.	4.56 min

CONCLUSION

In this paper, a security model was implemented to secure utilizing software component on cloud computing. Security model was divided into four sub-modules which are access control, prevention system, sandboxing and finaly proxy broadcast encryption. each module was implemented unaccompanied and assessed it. In addition, the time consumed by each module was calculate. Finally, all the systems and calculate the total time consumed was integrated. The time taken will impact the availability of the cloud. To know the accuracy of the system, all the signatures were disabled and calculate the time. afterward many signatures according to its relative correspondence were enabled and disabled, and its hit counts. And compare it with the non-security approach. After many experiments, it is recognized that enabling 908 signature which had the highest hit count (After applying the security checks) led to that the system became slower by 68 % in comparison to non-applying of any security modules. balanced security and availability were applied which has 908 signatures.

REFERENCES

[1] Mahmoud M. Elkhouly, 2016, Pages: 45-51Software Component as a Service (SCaaS), Australian Journal of Basic and Applied Sciences, 10(16) November

[2] Rola Motawie, Mahmoud M. Elkhouly, Samir A. El-Seoud, 18-10-Nov 2016 Security Problems in Cloud Computing, BUE ACE

[3] Mahmoud M. Elkhouly, Rola Motawie, Maged Huessien, January 2016, Addressing security issues in cloud computing, European Journal of Scientific Research 138(2) ·

[4] https://github.com/marcoramilli/MalwareTrainingSets/tree/master/trainingSets . [Accessed: 21-Sept-2017].

[5] Popovic, O.; Jovanovic, Z.; Jovanovic, N.; Popovic, R. Nis, Serbia, 5–8 October 2011; Volume 2, pp. 632–634, A comparison and security analysis of the cloud computing software platforms. In Proceedings of the 2011 10th International Conference on Telecommunication in Modern Satellite Cable and Broadcasting Services (TELSIKS),.

[6] Holloway, I.; Todres, L. 2013, 3, 345–357, The status of the method: Flexibility, consistency, and coherence. Qual. Res..

[7] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, 79-88, 2006, "Searchable symmetric encryption: improved definitions and efficient constructions," pp..

[8] I. Foster, Y. Z. Y. Zhao, I. Raicu, and S. Lu, 2016, “Cloud Computing and Grid Computing 360- Degree Compared,” 2016 Grid Comput. Environ. Work.,.

[9] P. Mell and T. Grance, 2015, “The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology,”.

[10] D. F. Ferraiolo, D. R. Kuhn, R. Sandhu, S. Gavrila, and R. Chandramouli, 2001 vol. 4, no. 3. pp. 224–274, “Proposed NIST standard for role-based access control,” ACM Transactions on Information and System Security,

[11] L. Youseff, M. Butrico, and D. Da Silva, 2008. GCE ’08, pp. 1–10, 2008 “Toward a Unified Ontology of Cloud Computing: Grid Computing Environments Workshop, 2008. GCE ’08,” Grid Comput. Environ. Work..

[12] D. Catteddu and G. Hogben, 2009 “Cloud Computing: Benefits, risks, and recommendations for information security,” ENISA,.

[13] Nishit Mishra, Tarun Kumar Sharma, Varun Sharma First Online: 25 November 2017Secure Framework for Data Security in Cloud Computing Conference paper Advances in Intelligent Systems and Computing book series (AISC, volume 583)

[14] Amit Sanghi, Sunita Chaudhary, Meenu Dave, First Online: 31 December 2017 Enhance the Data Security in Cloud Computing by Text Steganography Part of the Lecture Notes in Networks and Systems book series (LNNS, volume 18)

[15] Geeta C M, Raghavendra S, Rajkumar Buyya, Venugopal K R, S S Iyengar, L M Patnaik Directions 2018 Vol 28, No 1, Data Auditing And Security In Cloud Computing: Issues, Challenges And Future, International Journal of Computer C M

[16] Bakshi A, Yogesh, B. 2010: pp. 260–4 Securing cloud from DDOS attacks utilizing intrusion detection system in a virtual machine. In: Second international conference on communication software and networks;.

[17] Mazzariello C, Bifulco R, Canonoco R. 2010; pp. 265–70, Integrating a network IDS into an open source cloud computing. In: Sixth international conference on information assurance and security (IAS);.

[18] Lo CC, Huang CC, Ku J. Cooperative 2008: pp. 280–4 Intrusion detection system framework for cloud computing networks. In: First IEEE International Conference on UbiMedia Computing;.

[19] Dutkevyach T, Piskozub A, Tymoshyk, 2017. IDAACS 2007: 2007: pp. 599–602 N. Real-time intrusion prevention and anomaly analyze the system for company networks. In: Fourth IEEE workshop on intelligent data acquisition and advanced computing systems: technology and applications,

[20] Jon Oberheide, Evan Cooke, Farnam Jahanian Published 2008 CloudAV: N-Version Antivirus in the Network Cloud

[21] Zhengbing H, Jun S, Shirochin VP. 2007. IDAACS; 2007: pp. 647–51 An intelligent lightweight intrusion detection system with forensic technique. In: 4th IEEE workshop on intelligent data acquisition and advanced computingsystems: technology and applications,.

[22] R. Curtmola, J.A. Garay, S. Kamara, R. Ostrovsky, 2006, pp. 79–88. Searchable symmetric encryption: improved definitions and efficient constructions,

[23] M. Chase, S. Kamara, 2010, pp. 577–594 Structured encryption and controlled disclosure,.

[24] S. Kamara, C. Papamanthou, T. Roeder, 2012, pp. 965–976 Dynamic, searchable symmetric encryption,.

[25] K. Kurosawa, Y. Ohtaki, UC-Secure 2012, pp. 285–298 Searchable Symmetric Encryption,.

[26] https://github.com/woanware/LogViewer Last access 1-5-2018

[27] Information Security Forum (ISF), “Information risk analysis methodology (IRAM),” 2010. [Online]. Available: https://www.securityforum.org/products-services/risk-manager/. [Accessed: 24-Oct-2017]