International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

Cloud-based Optimisation approach to Joint Cyber Security and Insurance Management System

Sujatha E[1], Vignesh D[2], Gokula Krishnan P[3], Siva M[4]

[1,2,3,4] *Department of Computer Science and Engineering,*
Velammal Institute of Technology, "Velammal Knowledge Park", Panchetti, Thiruvallur, Tamilnadu, India

---

Abstract— *The main aim of this paper is to combine the approach to security and cyber insurance provisioning in the cloud-based resources. In cloud computing, the paper deals with binding the security and Insurance Management System (IMS). When a hacker attacks the application deployed in a cloud and tries to inject any malicious code into the application, the proposed system detects the attack and analyze the amount of data lost during that attack. During the estimation process, the quantity of breached data is calculated and sent directly to both the cloud user and Insurance Management System. So that the Insurance Management System can repay the compensation amount immediately to the cloud user with respect to the insurance package subscribed by the user, this activity is done after the attack has been detected and resulted in data breach. If suppose the amount of data breached is huge, then the system ask the cloud user to upgrade their insurance package.*

Keywords— SECaaS, Intrusion Detection System, Subscription Management Process (SMP), Insurance Management Process (IMP).

I. Introduction

In this paper, a joint approach to security and cyber insurance planning in the cloud is proposed. Using a probability optimization, a method of arranging both services in the surface of unpredictability concerning such as future pricing, incoming traffic, and cyber attacks. Thus, an operation may protect against strikes by provisioning security services from providers like Avast and Trend Micro.

These services may take various forms, such as secure data storage, identity management, and intrusion detection services to screen incoming traffic. And then cyber insurance is used to provide explicit cover in the event that malicious activity leads to financial loss. Insurance coverage may be first-party or third-party with such as thievery of money and digital assets, business interruption, and cyber extortion, privacy breaches.

II. Existing System

In the previous systems have been maintaining the security services only. So service should be protecting the user system and information. Sometimes may hacker attack the user assets and data like incidents and disasters such as data breach, data corruption, and business interruption? However, one lucrative attack can bring about the data loss and credit millions of dollars.

In the case of successive malware attack, the data breached is calculated and sent to the insurance system by the user. So loss will be uncertain. We cannot assume that damages can be accurately determined. This may be in various forms, such as a 'ransom' paid. It is important to stabilize provisioning of security and insurance, even when future costs and risks are undetermined.

One of the vital challenges in cyber insurance is the authentic evaluation of ruins generated by cyber attacks.

III. Proposed System

In this paper, SECaaS in firewall-style is proposed to provide security strategy imposition and supervising the network traffic infrastructure. This focuses on network traffic analysis like IDS (Intrusion Detection System) implementations to identify attack behaviors. And the relationship between cyber insurance and SECaaS provisioning, containing a customer who uses applications, which receive Internet traffic in the form of packets. These packets are scanned by services from SECaaS providers, provisioned by a Subscription Management Process (SMP).

In the event that harmful packets elude security, cyber insurers, subscribed to by an insurance management process (IMP), provide compensation for damages incurred. In this application run on customer machine that we assume to be Internet-accessible, either on a cloud service such as Amazon. Applications receive data packets in accordance with their operating purpose, e.g. email data or financial transactions.

Legitimate packets are called safe packets, while packets used in cyber attacks are called unsafe packets. Unsafe packets are deemed handled if they are correctly detected by security services, or unhandled if they are not successfully processed (for example if they are undetected). These unhandled packets will cause damage, which incurs costs to the customer will refund the amount to the insurance company. And then IMP will refund the particular data cost to the customer.

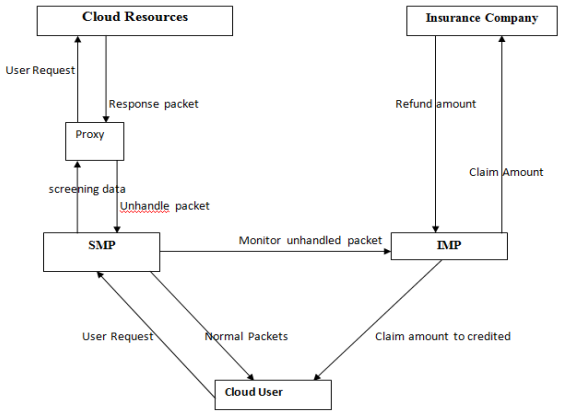

Fig.1: Architecture Diagram

A. Purchase the Security services

In this module user first register the cloud site and provides user details (Name, password, email, mobile, DOB). And then login using the user credentials. Once username and password are valid, then screen of the user's profile will be displayed. After login, user will purchase the outsource security service in the cloud. In the security services have a various control and price, validity.

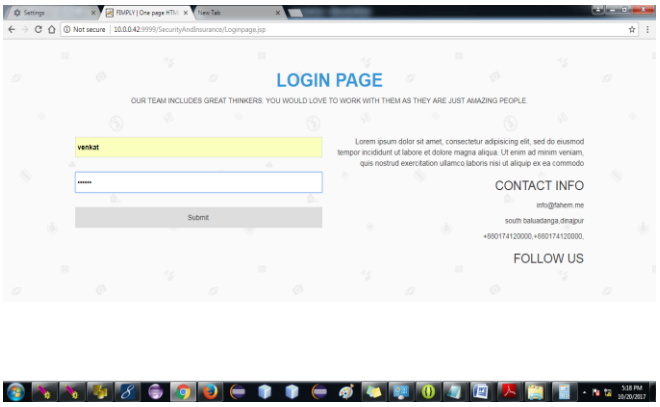

Fig.2:

The user will choose their system performance based services and then immediately transfer amount to security management. Once got the service, the security service will protect the customer application and system to particular time periods.

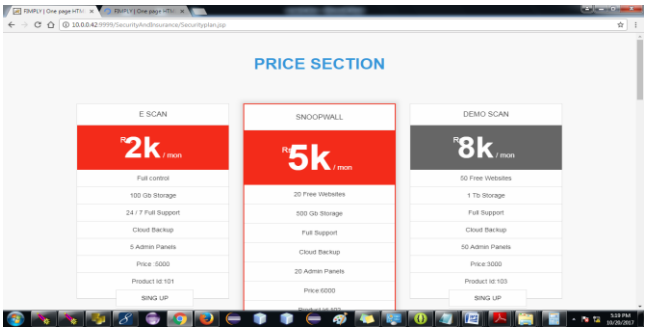

Fig 3:

B. Cloud service

In this module, the user registers the cloud service based on given user credential details and then log in the cloud resource. Once the user enters the cloud site or application, Say suppose, if their application may be a social network to chat with their friends. The user can upload their pictures to the social networking site.

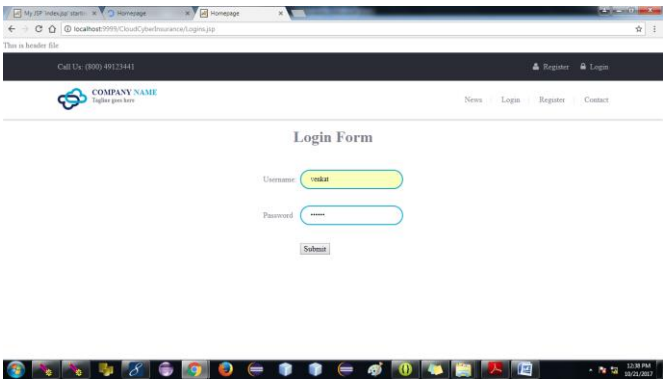

Fig.4:

While uploading, the user provides tags for the picture. Meanwhile the cloud security system will defend the application to each and every demand to cloud as a process of securing the cloud-based data.

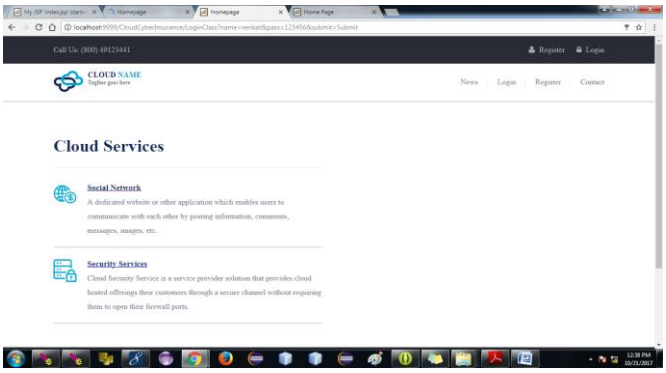

Fig.5:

Fig.6:

C. Screening Data traffic

In our security model, services are managed by the customer applications and then monitor the traffic flow and screening incoming data packets in accordance with their operating purpose, e.g. email data or financial transactions, web pages. Legitimate packets are called safe packets, while packets used in cyber attacks are called unsafe packets.

Unsafe packets are managed only if those unsafe packets are rightly identified by security services, or unhandled if they are not successfully processed (for example if they are undetected). These unhandled packets will cause damage, which incurs costs to the customer. So SECaaS will note on user packet size, and the service will redirect to Insurance Management Process (IMP).

D. Claim Insurance

In this module, IMP will check the user if customer or not. And then check the customer current premium data and evaluate the current unhandled data size to calculate the particular per-packet, price, duration, and a maximum number of packets affected.

A partial Lagrange multiplier algorithm is proposed to find the optimal solution in parameter change for calculating the amount of data. And then refund the amount to the particular customer. After the claim, the customer current premium is low to change the new future premium based on incoming unsafe packets.

The price for insurance purchased in advance is charged at a rate known as a 'future premium'. The IMP purchases insurance policies, which include the premium, types of risks covered indemnity value, and policy duration.

IV. Conclusion

This paper express the trust between the user and insurance management system and the compensation amount in accordance with the insurance subscribed by the user is provided to the user equivalent to the exact data that have been breached in very quick time. Though modern technology has improved so much, security is still a concern for cloud. Even though the security threats by cloud administration are feasible and critical, cloud service providers are concerned about security threat from external attacks rather than internal attacks. This project has presented cloud system architecture in such a way that the current security issues are removed and the cloud security is enhanced.

REFERENCE

[1] McAfee, "Net Losses: Estimating the Global Cost of Cybercrime,"Centre for Strategic and International Studies,Economic Impact of Cybercrime II, Jun. 2017.

[2] L. Zeng, B. Veeravalli, and X. Li, "Saba: A security-aware and budget-aware workflow scheduling strategy in clouds,"Journal of Parallel and Distributed Computing, vol. 75,2016.

[3] A. A. Waskita, H. Suhartanto, P. D. Persadha, and L. T. Handoko,"A simple statistical analysis approach for intrusion detection system," CoRR, vol. abs/1405.7268, 2016.

[4] S. Chaisiri, R. K. L. Ko, and D. Niyato, "A joint optimization approach to security-as-a-service allocation and cyber insurance management," in Trustcom/BigDataSE/ISPA, 2015 IEEE, Aug 2016,pp. 426–433.

[5] C. P. Ram and G. Sreenivaasan, "Security as a service (sass):Securing user data by coprocessor and distributing the data," in Trendz in Information Sciences Computing(TISC2010), Dec 2015.

[6] "Information technology – security techniques – information security management systems – requirements," ISO/IEC 27001,Standard, Jan. 2015.

[7] Y. Sun, S. Nanda, and T. Jaeger, "Security-as-a-service for microservices-based cloud applications," in 2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom), Nov 2015, pp. 50–57.

[8] A survey on security issues in service delivery models of cloud computing.S Subashini, V Kavitha - Journal of network and computer applications, 2011.

[9] A survey of Cloud Computing Security challenges and solutions. Nidal Hassan Hussein, Ahmed Khalid. International Journal of Computer Science and Information Security (IJCSIS), 2016.

[10] Software as a Service (SaaS): Security issues and Solutions. Navneet Singh Patell, Prof. Rekha B.S.2014.