International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 02 | Feb 2020 www.irjet.net p-ISSN: 2395-0072

A Joint Optimization Approach to Security and Insurance Management System

D. Vetriselvi[1], A. Abinayaa[2], S. Akshara[3]

[1]Assistant Professor, Dept. of Computer Science and Engineering, Jeppiaar SRR Engineering College, Chennai.
[2,3] Final year Student, Dept of Computer Science and Engineering, Jeppiaar SRR Engineering College, Chennai.

Abstract - *The main aim of this paper is a combined approach to security and the cyber insurance provisioning in the cloud based resources. Using a stochastic optimization, optimally provisioning both services within the face of uncertainty regarding future pricing, incoming traffic and cyber attacks is presented. Thus, an application may guard against attacks by provisioning security services from providers such as Avast and Trend Micro. These services may take various forms, such as secure data storage, and intrusion detection services to screen incoming traffic. And then cyber insurance is employed to provide explicit cover within the event that malicious activity results in loss. Insurance coverage may be first- or third-party with such as theft of money and digital assets, business interruption, and cyber extortion, privacy breaches, loss of third-party data.*

***Key Words*: Security services, Cyber Insurance, Stochastic Optimization, Cloud, Intrusion Detection**.

1. INTRODUCTION

Computing services are increasingly cloud-based, resources are invested in cloud based security measures. The Security-as-a-Service (SECaaS) allows customers to provide security to the cloud, through the subscription fee. However, no security system is bulletproof. So, one successful attack can result in the loss of data and revenue worth millions of dollars. To compensate the loss, customers may also purchase cyber insurance. It uses a stochastic optimization model to optimally provision security, and insurance services in the cloud. The accurate estimation of damages caused by cyber attacks is one of the key challenges in cyber insurance.. The model designed may be a mixed integer problem we also introduce a partial Lagrange multiplier algorithm that takes advantage of the entire unimodularity property to unravel the answer in polynomial time. In this application run on customer machine that we assume to be Internet-accessible, either on a cloud service like 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're correctly detected by security services, or unhandled if they're not successfully processed. These unhandled packets will cause damage, which incurs costs to the customer will refund the quantity to insurance firm . And then IMP will refund the particular data cost to customer.

2. RELATED WORKS

There are two aspects to the system model which we propose during this paper. One is the matter of Security Service allocation, and thus the second is cyber insurance provisioning. Recent add security within the paper titled Will Cyber-Insurance Improve Network Security? Has illustrated that solutions aimed toward detection and elimination of security threats alone are unlikely to end in a strong cyberspace. As an orthogonal approach in mitigating security problems, some have pursued the utilization of cyber-insurance as an appropriate risk management technique. Such an approach has the potential to jointly align with the incentives of security vendors, cyber-insurers, cloud providers, and network users (individuals and organizations), successively paving the way for comprehensive and robust cyber-security mechanisms. To the present end, during this work, we are motivated by the subsequent important question: can cyber-insurance really improve the safety during a network? To deal with this question, we adopt a market-based approach. This fact also emphasizes the necessity for designing mechanisms that incentivize the insurer to permanently be a part of the market.

With the implementation of cloud platforms in mobile system, within the paper titled Security in Mobile Cloud Computing by Prashant Pranav the storage of bulk data by client has become easier. IT Industries also are exploiting the advantages of cloud computing by producing more and more smart phones that take full advantage of the features of clouds. Because the use of smart phones by the users is increasing rapidly, the difficulty of security associated with use of cloud computing technique in mobile computing environment has emerged together of the most important challenges during this regard. Security with regard to mobile cloud computing is often addressed at three levels viz. mobile terminal, mobile network security, and cloud storage. Although many attempts are made in developing a model which ensures privacy and security of knowledge in mobile cloud system, no model is free from malicious attacks. During this review paper, we have focused on few models which are aimed toward giving security and privacy of knowledge in mobile cloud.

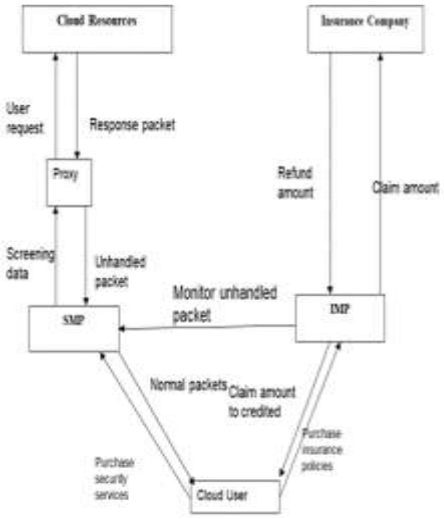
A comparative study of a different cloud service, cloud security issues and cloud providers help in choosing the right cloud service. Cloud computing is the most emerging field in the field of computing. In this various cloud services along

with the cloud security issues has been analyzed. Also, the comparison of three major cloud service providers namely Amazon AWS, windows Azure and Google App Engine have been carried out in the terms of security and security issues. It will help the consumers of cloud services to choose the right cloud provider according to their requirements and needs.

3. PROPOSED SYSTEM

In this paper, we present SECaaS in firewall-style to provide a security policy enforcement and monitoring infrastructure for network traffic which focuses on network traffic analysis like IDS (Intrusion Detection System) implementations to identify attack behaviors. And then relationship between cyber insurance and SECaaS provisioning, contains a customer who uses applications, which receive Internet traffics in the form of packets. These packets are scanned by security services, provisioned by a subscription management process (SMP). In this application run on customer machine that we assume to be Internet-accessible, either on a cloud service like Amazon. Applications receive data packets in accordance with their operating purpose. 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. These unhandled packets will cause damage, which incurs costs to the customer will refund the amount to insurance company. And then IMP(insurance management process) will refund the particular data cost to customer.

4. PROPOSED ARCHITECTURE



5. PROPOSED METHODOLOGY

In this paper, Lagrange multiplier algorithm and banking interface is used.

5.1. Lagrange Multiplier Algorithm

The model designed may be a mixed integer problem we introduce a partial Lagrange multiplier algorithm that takes advantage of the entire unimodularity property to identify the answer in the polynomial time. The mixed integer programming deterministic equivalent formulation is an effective way of identifying the optimum solution to the stochastic optimization, but suffers from tractability problems, as we would normally use a way like branch-and-bound, which has exponential computational complexity. Both the Artificial Intelligence (AI) community, and therefore, the research (OR) community have an interest in developing techniques for solving hard combinatorial problems. Furthermore, there's an excellent deal of overlap in research on local search and meta-heuristics by both communities. However, if we will convert our problem to a linear program (LP) without loss of precision, we will solve it in polynomial time. The partial Lagrange multiplier method will always converge to the optimal solution.

5.2. Banking Interface

In this banking is interfaced for the financial transactions. With the help of this, amount could be debited and credited.

6. MODULES AND DESCRIPTION

6.1. Purchase the Security services

In this module user first register the cloud site and provide the user details. And then login the user credential details. Then user will purchase Security Service in cloud. In this Security Service has a various control and price, validity. User will choose our system performance based services then immediately transfer amount to security management. Once got the service, will protect the customer application and system to particular time periods.

6.2. Cloud service

In this module, user register the cloud service supported user credential details then login the cloud resource. Once enter the cloud site or application to utilize the location. If your application could also be social network to share your post and chat with our friends. Users can also upload their pictures into the social networking site. While uploading, user provides tags for the image. At equivalent time security system will protect the appliance to every and each request to cloud then way of securing cloud-based data.

6.3. Screening Data traffic

In our security model, service managed by the customer applications 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 utilized in cyber attacks are called unsafe packets. Unsafe packets are deemed to be handled if they are correctly detected by security services, or unhandled if they are not successfully processed. These unhandled packets incur costs to the customer. So SECaaS to be noted on user packet size. At an equivalent time service will redirect to the insurance management process(IMP).

6.4. Claim Insurance

In this module IMP will check whether the user is a customer or not. And then check the customer current premium data and evaluate the present unhandled data size to calculate the particular per-packet, price, duration, and maximum number of packets affected. We introduce a partial Lagrange multiplier algorithm to find the optimal solution in a parameter change to calculate the amount to data size. And then refund the amount to particular customer. The price for insurance purchased beforehand is charged at a rate referred to as a future premium. The IMP purchases insurance policies, which incorporates the premium, sorts of risks covered, indemnity value, and policy duration.

7. CONCLUSION

In this paper, we've presented a combined approach to security and the cyber insurance provisioning within the cloud. It provides an experimental evaluation derived by running real traffic data through an Intrusion Detection System. Lagrange multiplier method exploits the total unimodularity property to guarantee integer solutions. This problem is solved iteratively employing a sub gradient method, which we prove converges to the optimal solution in at the worst polynomial time. The main challenge of cyber insurance is that the ability to detect cyber attacks, estimate accurate damages, and successfully make insurance claims.

8. REFERENCES

[1] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Will cyber-insurance improve network security? A market analysis," in Proc. IEEE INFOCOM 2014 - IEEE Conf. Comput. Commun., Apr. 2014, pp. 235–243.

[2] S. Chaisiri, R. K. L. Ko, and D. Niyato, "A joint optimization approach to security-as-a-service allocation and cyber insurance management," in Proc. Trustcom. Big Data SE/ISPA, 2015, pp. 426–433.

[3] Kai Hwang, Deyi Li, Trusted Cloud Computing with Secure Resources and Data Coloring in IEEE Internet computing ,2010.

[4] A. Holder, Parametric Linear Programming, March 3, 2010.

[5]C. P. Gomes, "Structure, duality, and randomization: Common themes in AI and OR," in Proc. 17th National Conf. Artif. Intell. 12th Conf. Innovative Appl. Artif. Intell., 2000, pp. 1152–1158.

[6] Satish Kumar, Vishal Thakur, Ashok Kumar Kashyap, A Comparative study of different cloud services, Cloud security issues and Cloud Providers in IJLTET in 2016.