IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 40-43

A Joint Optimization Approach To Security And Insurance Management System

S.Gomathi[1], Mr.R.Prem Kumar[2]
[1](CSE, Sri Venkateswara College of Engineering and Technology, India)
[2](CSE, Sri Venkateswara College of Engineering and Technology, India)

Abstract: *In this paper we have presented a joint approach to security and cyber insurance provisioning in the cloud. Using a stochastic optimization, we have presented a method of optimally provisioning both services in the face of uncertainty regarding future pricing, incoming traffic and cyber attacks. 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, identity and access management (IAM), 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- or third-party with such as theft of money and digital assets, business interruption, and cyber extortion, privacy breaches, loss of third-party data.*

I. Introduction

As computing services are increasingly cloud-based, corporations are investing in cloud-based security measures. The Security-asa- Service (SECaaS) paradigm allows customers to outsource security to the cloud, through the payment of a subscription fee.

However, no security system is bulletproof, and even one successful attack can result in the loss of data and revenue worth millions of dollars. To guard against this eventuality, customers may also purchase cyber insuranceto receive recompense in the case of loss.

To achieve cost effectiveness, it is necessary to balance provisioning of security and insurance, even when future costs and risks are uncertain. To this end, we introduce a stochastic optimization model to optimally provision security and insurance services in the cloud.

Since the model we design is a mixed integer problem, we also introduce a partial Lagrange multiplier algorithm that takes advantage of the total unimodularity property to find the solution in polynomial time. We also apply sensitivity analysis to find the exact tolerance of decision variables to parameter changes.

We show the effectiveness of these techniques using numerical results based on real attack data to demonstrate a realistic testing environment, and find that security and insurance are interdependent.

II. Implementation Techniques

III. Literature Survey

3.1 Ti Job Dispatching and Scheduling for Heterogeneous Clusters – a Case Study on the Billing Subsystem of CHT Telecommunication

Many enterprises or institutes are building private clouds within their own data centers. Data centers may have different batches of physical machines due to annual upgrades, but the number of machines is fixed most of the time. Consequently it is crucial to schedule jobs with different resource requirements and characteristics to meet different job timing constraints, in such heterogeneous yet most of the time static environments.

This framework makes decisions according to specified policies, and the framework provides four default policies for system administrators to choose to fit their specific needs. The framework is designed to be componentpluggable. The components of the framework can be hotswapped, i.e., replaced without shutting down the services.

3.2 Mobility Aware Task Allocation for Mobile Cloud Computing

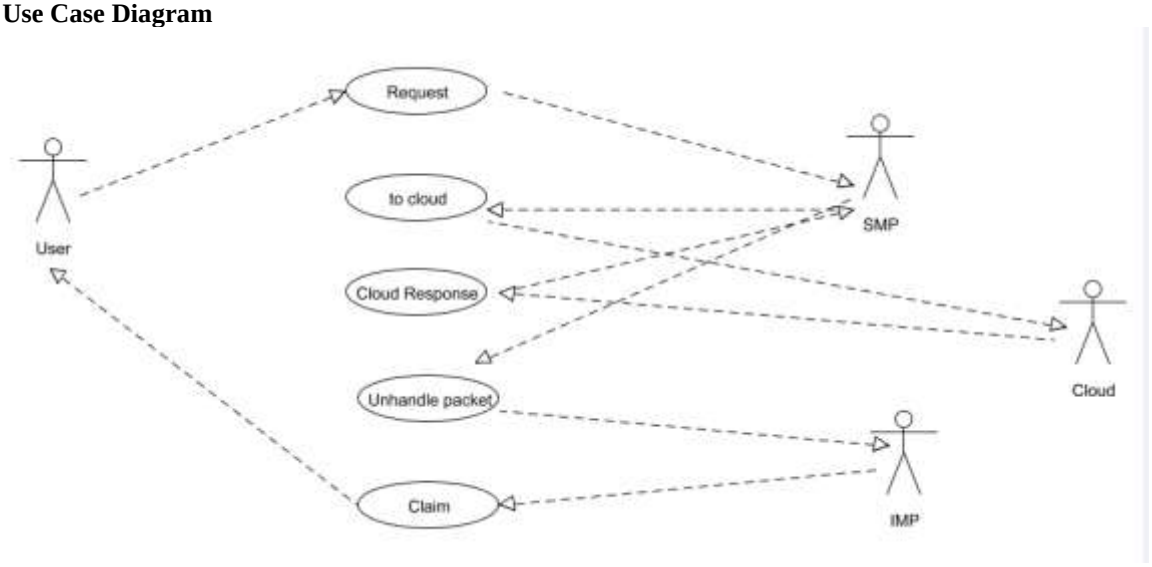
The Mobile Cloud Computing is a promising technology that has provided a way to overcome the limitations of the mobile devices. The advancement of mobile devices technology has made the applications of

these devices more complex and resource famished. Mobile cloud computing has created opportunities to execute these applications on the mobile devices by migrating the compute intensive task to the cloud.

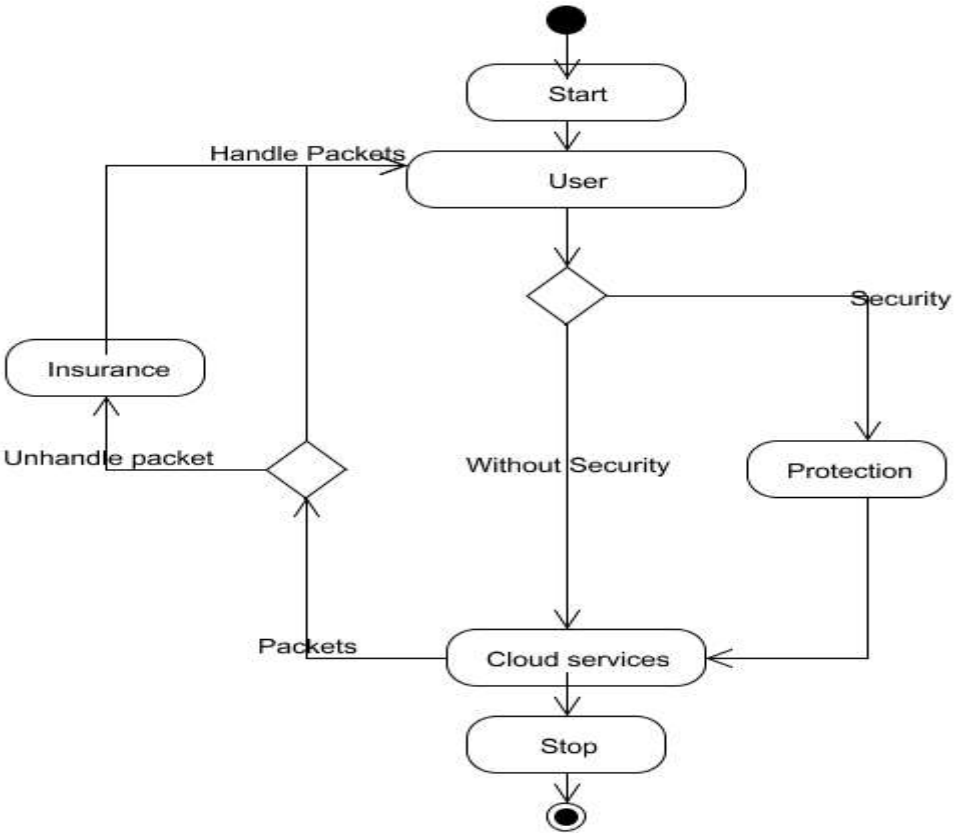
This migration of task to the cloud is not an easy task. The connectivity of the devices and the cloud is affected by the network inconsistency of wireless network. The servers on the cloud are heterogeneous in nature. Furthermore, the users are most of the time in mobile state which results in frequent change in association to access points. All of these make the selection of an optimal server to offload the task in cloud into a challenging work. In this paper, a comparative survey is provided for allocating task on the cloud along with their limitation.

IV. System Design

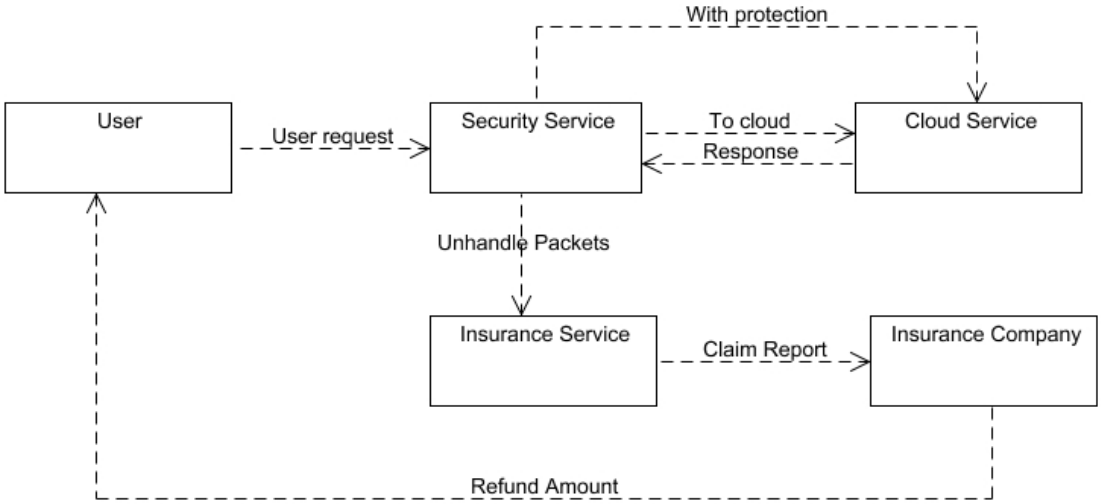
4.1 Use Case Diagram



4.2 Activity Diagram



4.3 Collaboration Diagram



V. Module Description

5.1 Purchase the Security services.

In this module user first register the cloud site and the provide user details (Name, password, email, mobile, dob) .And then login the user credential details like username, password. Once user name and password is valid open the user profile screen will be display. After login user will purchase the outsource security service in cloud. In the security service has a various control and price, validity. User will choose our system performance based services and then immediately transfer amount to security management.
Once got the service, that will protect the customer application and system to particular time periods.

5.2 Cloud service.

In the module, user register the cloud service based on user credential details and then login the cloud resource. Once enter the cloud site or application to utilize the site. If your application may be social network, share your post and chat with our friends. Users will upload their pictures into the social networking site. While uploading, user provides tags for the picture at the same time security system will protect the application to each and every request to cloud and then way of securing cloud-based data.

5.3 Screening Data traffic.

In our security model, service managed by the customer applications and then monitors the traffic flow and screening incoming data packets in accordance with their operating purpose e.g. email data or financial transactions, WebPages 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. so SECaaS to noted on user packet size. At the same time service will redirect to insurance management process (IMP).

5.4 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 maximum number of packets affected. we introduce a partial Lagrange multiplier algorithm to find the optimal solution in parameter change to calculate the amount to data size .And then refund the amount to particular customer. After 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.

VI. Conclusion

We have presented a combined approach to security and cyber insurance provisioning in the cloud. Using a stochastic optimization, we have presented a method of optimally provisioning both services in the face of uncer- tainty regarding future pricing, incoming traffic and cyber attacks. Finally we provide an experimental evaluation of our contributions using realistic traffic and attack data derived by running real traffic data through an Intrusion Detection System. The main challenge of cyber insurance is the number of assump- tions that must be made, for example, the ability to detect cyber attacks.

Acknowledgements

References

[1]. McAfee, "Net Losses: Estimating the Global Cost of Cybercrime," Center for Strategic and International Studies, Economic Impact of Cybercrime II, Jun. 2014.
[2]. (2016) Identity theft resource center data breach reports. [Online]. Available: http://www.idtheftcenter.org/2016databreaches.html
[3]. (2016) A bold approach to cyber risk management. [Online]. Available: http://www.mas.gov.sg/News-and-Publications/Speechesand-Monetary-Policy-Statements/Speeches/2016/A-Bold-Approach-to-Cyber-Risk-Management.aspx
[4]. (2016) Insurance 2020 beyond: Reaping the dividends of cyber resilience. [Online].Available: http://www.pwc.com/gx/en/industries/financialservices/insurance/publications/insurance-2020-cyber.html
[5]. (2016) Mcafee security-as-a-service solutions. [Online]. Available: https://www.mcafeeasap.com/MarketingContent/Products/ProductsLanding.aspx
[6]. (2016) Deep security as a service. [Online]. Available: http://www.trendmicro.com/us/business/saas/deep-security-as-a-service/#usage-based-pricing
[7]. B. Delamore and R. K. L. Ko, "Chapter 9 - security as a service (secaas)an overview," in The Cloud Security Ecosystem, R. K. L. Ko and K.-K. R. Choo, Eds. Boston: Syngress, 2015, pp. 187 –203. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780128015957000094
[8]. (2016) Allianz cyber protect. [Online]. Available: http://www.agcs.allianz.com/services/financial-lines/cyber-insurance/
[9]. (2016) Cyber and data security. [Online]. Available: http://www.qbeeurope.com/professional-financial/cyber-liability.asp
[10]. M. Clark. (2014) Timeline of target's data breach and aftermath: How cybertheft snowballed for the giant retailer. [Online]. Available: http://www.ibtimes.com/timeline-targets-data-breachaftermath.