A Scalable Approach to Joint Cyber Insurance And Security-as-a Service Provisioning in Cloud Computing

ABSTRACT

As computing services are increasingly cloud-based, corporations are investing in cloud-based security measures. The Security-as a- 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 insurance to 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.

EXISTING SYSTEM

In a 2014 report by McAfee it was estimated that financial losses due to cyber risks were between USD 300 billion and USD 1 trillion a year. The Identity Theft Resource Center's 2016 data breach category summary found that as of November, there were 873 recorded breaches in the US with over 29 million records exposed. We devise a stochastic optimization for a customer to jointly provision security services and buy cyber insurance premiums across multiple time periods. We account for uncertainty in traffic quantities and attack frequency, as well as future uncertainty of security service prices and insurance premiums. Due to the tractability problems of integer programming, we introduce a partial Lagrange multiplier algorithm to find the optimal solution in, at worst, polynomial time. We provide proofs of convergence and scalability. We perform a sensitivity analysis, which provides precise values for solution tolerance to parameter change. We then demonstrate the effectiveness of our methods through evaluation of an example scenario, based on analysis of real attack data to provide realistic parameter settings

.Disadvantage

- Millions of credit card details were stolen from Target.
- Security is less.
- The quantification of damage is difficult to define, due to the intangibility of losses.

PROPOSED SYSTEM

In this paper 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 uncertainty regarding future pricing, incoming traffic and cyber attacks. Since our optimization involves solving an integer programming problem, we present the partial Lagrange multiplier method, which exploits the total unimodularity property to guarantee integer solutions, while relaxing the problem to a linear programming problem. This problem is solved iteratively using a subgradient method, which we prove converges to the optimal solution in at worst polynomial time. Using the solution produced by the algorithm, we apply an analytical sensitivity analysis approach that gives precise sensitivity values for individual parameters. 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 assumptions that must be made, for example, the ability to detect cyber attacks, establish accurate damages, and successfully make insurance claims.

Advantages

- It secures cloud-based data through encryption and distribution of data.
- It has the ability to detect cyber attacks, establish accurate damages, and successfully make insurance claims.

SOFTWARE REQUIREMENTS

Front-end	:	JSP
Back-End	:	MySQL
Server	:	Tomcat Server
OS	:	WINDOWS 7/above

HARDWARE REQUIREMENTS

PROCESSOR	:	CORE i3
RAM	:	512MB-2GB
HARD DISK	:	40GB