**EXISTING SYSTEM:**

The Existing works consider competitive insurance markets under compulsory insurance, and analyze the effect of insurance on agents’ security expenditures. The authors of consider a competitive market with homogeneous agents, and show that insurance often deteriorates the state of network security as compared to the no-insurance scenario. The existing studies a network of heterogeneous agents and show that the introduction of insurance cannot improve the state of network security. Study the impact of the degree of agents’ interdependence, and show that agents’ investments decreases as the degree of interdependence increases. Study a competitive market under the assumption of voluntary participation by agents, with and without moral hazard. In the absence of moral hazard, the insurer can observe agents’ investments in security, and hence premium discriminates based on the observed investments. They show that such a market can provide incentives for agents to increase their investments in self-protection. However, they show that under moral hazard, the market will not provide an incentive for improving agents’ investments. The impact of insurance on the state of network security in the presence of a monopolistic welfare maximizing insurer has been studied in existing system. In these models, as the insurer’s goal is to maximize social welfare, assuming compulsory insurance, agents are incentivized through premium discrimination, i.e., agents with higher investments in security pay lower premiums. As a result, these studies show that insurance can lead to improvement of network security. An insurance market with a monopolistic profit maximizing insurer, under the assumption of voluntary participation, has been studied in existing work, which shows that in the presence of moral hazard, insurance cannot improve network security as compared to the no-insurance scenario.

**PROPOSED SYSTEM:**

In this paper, we are interested in analyzing the possibility of using cyber-insurance as an incentive for improving network security. We adopt two model assumptions which we believe better capture the current state of cyber insurance markets but differ from the majority of the existing literature; we shall assume a profit maximizing cyber insurer, and voluntary participation, i.e., agents may opt out of purchasing a contract. Under this model, we focus on two features of cyber-insurance: (i) availability of risk assessment for mitigating moral hazard, and (ii) the interdependent nature of security. The first feature is due to the fact that recent advances in Internet measurements combined with machine learning techniques now allow us to perform accurate, quantitative security posture assessments at a firm level. This can be used as a tool to perform an initial security audit, or pre-screening, of a prospective client to mitigate moral hazard by premium discrimination and the design of customized policies. The second distinct feature, the interdependent nature of security, refers to the observation that the security standing of an entity often depends not only on its own effort towards implementing security metrics, but also on the efforts of other entities interacting with it within the eco-system. Such interdependency is crucial for the insurer’s contract design problem, as the insurer will need to offer coverage to each insured for both its losses due to direct breaches, as well as indirect losses caused by breaches of other entities.