2. LITERATURE SURVEY

2.1 INTRODUCTION

Cloud security has recently received widespread attention from experts across domains, having a large number of research projects being undertaken to improve the core issue of trust in the cloud. This chapter provides a discussion of literature being carried out related to trust models specific to cloud computing. Broadly, there are three phases first; trust establishment through the quality of service with its associated metrics are discussed. The means of measurement and QoS parameters like availability of TMP chip and SLA certificates are reviewed through various literature surveys. Next, assuring trustworthiness through attestation policy and the need for third party certification to attest the trust score is an essential evaluation procedure. Finally, a study on Game playing strategy using the cooperative cost-sharing model with its necessity has been discussed.

2.2 TRUST MODELS IN CLOUD COMPUTING

Trust is a complex phenomenon where there is no standardized definitions or model. One of the common definitions of trust, generally adopted is “the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context” [13]. The work substantiates the definition through various properties and characteristics of trust. It emphasizes the accreditation of the trustworthiness by a third party. Trust functions, in general, have been broadly classified into four comparative dimensions [14] as follows.

Subjective and Objective trust: If results or outcome of an event are kept as a benchmark to quantify a specific entity’s dependability is said to be objective trust. On the other hand, if the results are reliant on an individual attention then it is subjective trust.

Transaction and Opinion based trust: The decisions can be taken according to person’s transaction profile or on a person’s opinion.
**Complete and localized trust:** If information’s are gathered from each and every single node, it is called global trust function or complete trust function. However, localized trust deals with an event or data collected from one’s neighbor.

**Relative trust between rank and threshold:** A similar scale of best to worst can be termed as relative trust, and threshold initiated trust has their limit set for taking any logical decisions.

Trust is a multidimensional quantity with conditional transitive. For example, if an agent trusts another agent, who in turn trusts the third one, then the first agent and the third can indeed make a relationship based on certain policies and conditions. Based on willingness to exchange information between each other, one can have confidence towards the other in maintaining a long term relationship. Means of control mechanism could establish trust through objective rules instead of subjective probability. The mechanism works to attain a level of control by forcing quality assurance metrics. This type of enforcement enables entities to abide by tentative agreements, called as control trust. In our research, we use control trust by forcing certain quality of services to be adopted as a policy for progressive interaction. Having gone through briefly the basic characteristics of trust, we now focus our literature survey towards our trusted cloud environments.

Historically, trust revolves around the domain of social interactions, and its entry into digital world has become inevitable because of the complex nature of machines interacting with each other. Currently, researchers have renewed their interest towards the field of computational trust for a secure ecosystem because social communities interacting with machines grow exponentially due to cloud adoption. The growing importance of cloud computing makes it imperative for consumers, providers, and society in general to embrace trust. Establishing confidence with reputation systems has been successfully used since the inceptions of the internet to support users identify reliable service providers.
Numerous surveys and researches have been carried out for different domains, especially on web services, social networking, and grid computing. With respect to web services, trust has been the main focus for services group selection and trust classification [15], [16]. A comprehensive survey has been undertaken to address trust evaluation, trust information collection and trust dissemination in social networks [17]. Trust degree calculation based on subjective logic has been researched for data grids to maintain the integrity of data [18]. Since cloud has evolved on these concepts, all the trust methodologies can be easily adapted to cloud computing also. Nevertheless, cloud-specific trust models have found a stronghold because of implicit security loopholes in it. Hence implementing trust in every system is not a question of choice but a mandatory feature to protect every asset in IT infrastructure.

2.3 BEHAVIORAL TRUST AND QoS FOR TRUSTED CLOUD

Monitoring and managing the behavioural trust of participants in the cloud and their interaction process of how they collaborate or cooperate are essential for trusted cloud. Most of the earlier trust models for behavioural approaches do not concentrate on user specific actions. Changes during the service interaction in the cloud are a challenge that needs to be reviewed.

Trust model by Tian [19] addresses the behaviour of users based on time, abnormality in access, slow-rise of trust value, a rapid decline of non-trustable users. The work assesses the behaviour based on security, authentication, and compliance of contract. It also proposes that AHP could be the best choice for giving weightage to various metrics collected for behaviour. The work focuses only on a study of behaviour models.

An approach for monitoring the participants in a forensic data center environment, to oversee the investigation across jurisdictions was proposed by Thorpe [20]. The author justifies that, assessing the participants of the cloud just for their behavioural pattern alone are not sufficient. Hence we have to evaluate the pattern of the software services which are instantiated at the user’s place. Malware’s and adware’s that keep cropping up unknowingly
and collects information’s from user’s machine, hence checking the behaviour of services for its quality and enforcing it to behave as expected are an essential phenomenon. So to test the quality, we need to assess various QoS parameters. Hence Quality of Service plays a vital role in establishing the trustworthiness of every entity in the cloud atmosphere.

The TR model [21], describes trust as a facilitator in the cloud that integrates Quality of Services (QoS) parameters like compliance, interoperability, customer support, federated identity management, and service deployment. These QoS parameters quite closely map trust affector so as to establish trust in cloud providers. This in turn, assists consumers, to comprehend the capability and competence of service providers prior to interacting with them. This research paper provides a comparison of many trust models based on customization, aggregation and attack resistance with an aim to provide an understanding of various trust models.

Analyzing the objective parameter of cloud services instead of subjective ratings makes the evaluation criterion important. Also, it reflects the exact nature of the delivery status of service. The quality of service characteristics of cloud such as response time, throughput, geographical location, accountability, resource capability and security parameters have been discussed at large for evaluating trust [22], [23].

In another approach [24], QoS of the services is combined with the trust relationship to identify any missing values. The work measures the usability of the service through Jaccard’s Coefficient and the numerical distance by Pearson Correlation Coefficient. Another work in QoS [25], identifies the three key elements of quality namely, efficiency, reliability, and availability, and simulates using CloudSim tool. It is a formal approach with minimal parameters for assessing the trust. The histories of trust are given the least preferences, whereas in our work the centralized trust store is the key agent in providing the values for attestation.

The level of satisfaction on the delivered services, especially the QoS, needs to be initially bounded by an agreement between the end users. This
agreement generally termed as the service level agreements are a necessary component in justifying the quality. For example, every cloud service must address the issue of security and privacy, but providers mislead the users with promises for a certain service. So, the need for an agreement between various cloud stakeholders especially provider and user should be there. A legal contract would bind them to service the customers of what is being assured. A good SLAs can be contributed towards conflict avoidance and facilitate arbitration and resolution of an issue before it could escalate into a major dispute. Hence, SLA verification requires a professional third party to monitor any situations arising out of disagreements. Cloud Standards Consumer Council is one such group under a consortium dedicated to the advocacy of cloud adoption. It provides practical guidelines for cloud service agreements (CSA) to help enterprises and decision makers [26]. The CSA consist of three major artifacts as listed below.

a) **Customer Agreements** – describes the terms of service between the customer and provider

b) **Acceptable Use Policy** – activities that are prohibited by the provider which are considered as improper or illegal.

c) **Service Level Agreements** – specifies the level of thresholds and financial penalties associated with any SLA violations.

To select a trusted cloud provider, the research paper by Alhamad [27] combines the existing SLA requirements into the trust framework. The constituent components include an SLA agent for grouping cloud consumers. The designs of SLA are based on consumer needs and negotiation with providers. Further, it monitors the business activities and SLA parameters. SLA’s at customer, service and multilevel has been discussed along with its impact on trust by Shakeel [28]. It proposes that agreements can be made only after pre-assessment by verifying certain attributes about the providers like knowledge on cloud service, background check, and security objectives.
A framework using Service Measurement Index (SMI) to help the users to evaluate the cloud offering and rank them accordingly was proposed by Saurabh [29] gives a list of cloud Key Performance Indicators (KPI). It also ranks service quality through Analytical Hierarchy Processing (AHP), and provide a computing methodology to relatively compare different services offered by providers. This work helps in creating competition among cloud providers and enables them to satisfy their SLAs and enhance their QoS. A similar work called as Global Trust [30], supports the performance of the cloud through some successful transactions and combines an opinion source model adopted from certain logic [31]. The certain logic is based on subjective trust where the opinions are expressed as $O(x) = (t, c, f)$, which are modeled as a triplet of average ranking, certainty, and initial belief. Both the above works expose the quality metrics in the cloud with their evaluation methodologies. However, an actual implementation of these frameworks is required to prove it.

Another important quality measure taken into consideration in our work are the reputations of the existing provider or the consumer or the service being delivered. Reputation deals with the aggregated opinion of a large number of the users towards an entity based on different criteria. A highly reputed service generally has a trust indicator for that service, hence for choosing trustworthy services the value of reputations are always recommended. A research work by eminent Kai Hwang [32], suggests some basic protection mechanism for IaaS, PaaS and SaaS implemented by industry majors during the early stages of cloud initiatives. It proposes to integrate virtual clusters and datacenters for a trusted data access using the well-known reputation system. In another work by the same author [33], the work proposes to use an overlay network exclusively for trust above the layer of cloud data centers to implement a reputation system. This reputation-based trust management scheme uses the watermarking technique to protect data and software for a dependable cloud. Data coloring techniques are primarily meant for security. Hence, attestation of colored data can further enhance the system.
A trust cloud framework proposed by Abawajy [34], aid a service consumer in assigning a weightage factor for feedbacks given towards a service provider. The work controls the negative feedback rating based on trust levels of the provider. This work focuses on provider and consumer and identifies false feedbacks; it lacks in assessing the software services and purely depends on indirect trust computation. For integration of cloud and sensor networks, a novel approach has been proposed to calculate the reputation [35]. This method identifies the need for security and trust while integrating the two domains. It calculates the cost, trust, reputation score, and performs three main functions, first, it authenticates, then calculates trust and finally helps in choosing the service provider. The work addresses major trust related attacks like good and bad mouthing, collusion and white-washing attacks.

The necessity of trusting a cloud service that is aggregated from vendors by a provider, in a heterogeneous environment, requires the involvement of official bodies, governing councils and even government interventions. At the international level, various committees have been set up to secure cloud infrastructure from possible attacks and mitigate any event of a disaster. One of the pioneering organizations is the Trusted Computing Group [36], involved in the development of trusted computing standards to enable seamless security in support of open security standards. One of the prominent security standards includes the development of Trusted Platform Module (TPM), self-encrypting drives and framework for Trusted Multi-tenant Infrastructure (TMI). Cloud Security Alliance (CSA) promotes best practices for securing the cloud by developing a Security Trust and Assurance Registry (STAR) which documents the security controls being developed [37]. Another body that defends the consumer’s rights is the Cloud Standards Consumer Council (CSCC) [38], which specifies various metric for trust assessment. Finally, NIST’s cloud computing security reference architecture provides a detailed specification of different stalk holders and their responsibilities towards establishing security [39]. The overall objective of all these councils and alliances among the industry and institution is to adopt the TPM as a boot level device for assuring security through trusted boot.
Trusted computing platform is a tamper-resistant embedded security chip that specifies important functions for IT security and focuses chiefly towards providing cloud security through TPM [40]. Key security aspects contributed by TCG are its secure cryptoprocessor, disk encryption, and password protection. It can provide assurance within the cloud by shielding its internal data structure and, consequently, subverting the computations from being intervened by the host system or the system administrator. The module works at the root of hardware, operating system, hypervisor, and applications. Thus the module has launch measurements, hashes, keys in its Platform Configuration Registers (PCR) and boots trustfully by comparing the measurement with good known values.

TPM chips have gained the backing of industry giants like Intel, AMD, Dell, Microsoft, Juniper Network and Cisco with almost every country adopting it as a standard. One of the significant enhancements made on adopting TMP is that Intel has built the specifications in its Xeon processor through Intel’s TXT (Trusted Execution Technology) [41]. Thus, in our proposed work, the role of the module serves as a root of trust for the operating system that runs higher level cloud applications. In our experiments, the TPM-based system plays a vital role for trust and assumes that a host accessing cloud services must indeed connect via a TPM.

2.4 ATTESTATION MODELS FOR TRUST CERTIFICATION

The authenticity of trusted service that is selected through various trusted cloud models which would be in question if it fails to provide the assured trustworthiness. Hence there needs to be a third party cloud auditor responsible for performing a verification process through evidence given by those models. Through a set of standard protocols, the attester can verify the behaviour and certify the users, services, and providers that the trust gained are indeed true. A verification methodology for a cloud hosted web application was implemented using the consistent behavior of object’s reading and write capability [42]. The work proposes a collaborative verification through witness agents who verify the I/O behavior of the web apps. The verifier checks the log information for its consistency of the
predetermined operation using a streaming algorithm. AdapTest [43] aims to project an attestation framework for a multi-tenant cloud system which reduces attestation overheads and shortens detection delays. It provides attestation at runtime dynamically by using the previous attestation results and probabilistic approach.

Based on certain principles [44], researchers have currently focused their security mechanisms in the verification process. The work proposes various principles for attestation process, like key exchange mechanism, measurement attributes, lifetime for any attested resources and its values. On the attestation mechanism called DR@FT [45], a domain-based integrity model for remote attestation, the integrity is measured based on information flow. It classifies high-integrity and low-integrity processes and verifies the latest changes in a target system. Since hardware-based integrity measurement has failed to achieve the required level of trust. An approach called integrity verification proxy (IVP), a service that enforces various integrity requirements to the remote systems has been proposed as an efficient protocol for integrity measurement [46].

Another work by Nuno [47], proposes a model called Excalibur, for building trusted cloud services using hardware protection. It demonstrates a cloud broker security model that uses ARM Trusted Zone technology for hosting mobile apps in the cloud. The difference between Excalibur and our work is that, even though we use a broker for verification, it is purely a software process instead of a hardware inspection. However, we do have stressed the need for TPM modules as the primary root of trust, and so the weightage in evaluating its trust are given the top priority. The need for trusting a service in the cloud and its necessity to verify its ability to guarantee the integrity of contents generated by the users in online applications like cloud software services has been the research carried out by Akshay [48]. The work has considered online games and online messaging system for effectively monitoring the behavior and verifies it. In our model, an image processing application is considered for effectively identifying and testing the integrity of the service.
A Client-Oriented Remote Attestation (CORA) model [49] enables clients to select a node in the cloud at a security level corresponding to their particular needs and dynamically verify the node’s security status. This model has a user defined security which may lead to compromise the provider’s intention to deliver trusted services. In contrast, our model aims at establishing a standardized architecture in accordance with regulations and frameworks set by international bodies like CSCC. An auditing standard for attestation process called SSAE 16 (Statements on Standards for Attestation Engagement) has been followed for our work in identifying trust principles and objective [50].

The process of attestation service to verify the authenticity of the claims made by the trusting agent has found significant research initiatives from various communities. These research activities make any trust model to abide by the common nature of verifying the behavior measurements by a certified evaluator. Strategies

2.5 COALITION STRATEGIES FOR TRUSTED COOPERATION

By engaging cloud players through an experiment of a game, the resultant outcome would be in the form of an empirical value, which can be used as an estimate of trust. Game of trust can be designed to maximize the monetary gain attributed to the cooperation of participants. The participants vary based on the assessment, either for service providers or consumers. It can also be adopted for negotiation, arbitration and vendor identification. The following works identify the necessity of game playing in the cloud.

Predicting the future of resource allocation and its prices to satisfy the budget constraint users has been proposed using game theoretic Nash Equilibrium [51]. They adopt the Bayesian learning mechanism to solve the resource allocation problem and sequential gambling auction for identifying the total sum for equilibrium. Using these methods the model imposes a limit to the bids, else users would attempt to exaggerate the competition and raise the bids without any limit.
Hosting a SaaS onto another provider's infrastructure requires that they both agree to certain SLA contracts. This is because application vendors would like to capitalize on their incomes by decreasing the resources supplied by IaaS provider. Alternatively, IaaS supplier's tries to increase their revenues. So there exist conflicts that can only be solved through the game. Hence a variation of the regular Nash Equilibrium called the Generalized Nash Equilibrium Problem (GNEP) with a payoff function adaptable for each player was proposed [52].

An optimal solution for assigning VMs requires game theory strategies. The bargaining solutions like Nash Bargaining and Raiffa Bargaining are proposed based on the tasks that are known in advance and real-time task arrival respectively. Based on the service provider’s choice of deadline and budget requirements, a novel asymmetric approach was also proposed [53]. The model gives an insight into the bargaining principles of the game and does not concentrate on trust establishment.

Game theory has been considered for efficiently instantiating the VMs, and provides a model for incentive scheme and also penalizes those providers who break away from the coalition [54]. The mechanism ensures that none of the providers gain individually, or break to form another federation. The cost allocation is based on the provider’s market power. Hence, a stable federation can be formed by involving a variety of providers, ranging from the low segment to market leaders, who share a common cloud federation.

Federation formation issue for energy-aware cloud has been addressed through the usage of game theoretic approach for distributed coalition formation [55]. The main objective was to reduce the energy bill of cloud federation and prove that, the cooperation strategy work better in reducing the bill than servicing alone. This approach provides a solution for cost minimization. Selecting an auction winner in the cloud using non-cooperative game through Nash Equilibrium in a multi-user allocation was proposed by Amin [56]. The work aims at finding the equilibrium points, upon which there are no other bids to be offered and avoids any impasses among
the bidders. The work has been simulated in CloudSim and the results are satisfactory for utility sharing among service providers. A cooperative approach for resource allocation through coalition has been studied by Jebalia [57] to maximize the overall revenue. The work concentrates on compensation policy for those who have adopted security aspects. Orchestration and intermediation of cloud services require experienced service brokers, who are responsible for aggregating different demands of customers. One of the major demands of the customers was to find the lowest price for the service. Hence the work demonstrates it as an optimization problem through linear reward-inaction algorithm [58].

Most of the literary work that has been surveyed for the game has provided solutions for resource allocation, scheduling, and bargaining. Only a very few have adopted the idea of using game theoretic concept for establishing trust or identifying cooperation between service providers.

In work proposed by Gokulnath [59], Nash equilibrium enhances the trust evaluation of first-time users and service providers at the boot load level. The paper addresses the issue of cold start and whitewashing in the selection of cloud service providers (CSP). This work focuses only at the initial stages of cloud access and does not deal with the continuous evaluation. For a multimedia application delivery model in the cloud platform, a different approach has been adopted to minimizing the penalties due to the violation of service quality by any untrusted providers. The federation dynamically provides VM instances to users with QoS guarantee and satisfies fairness and stability property [60].

Thus game theory plays a vital role in this dynamic and distributed cloud landscape for an efficient and optimized resource allocation. Apart from that, the game can be adopted for mutual agreement, strategy playing and policy establishing. In our research, we have considered the game for the cooperation of various providers to exercise a mutual agreement for cost sharing.
2.6 SUMMARY

- In this chapter, need for trust as critical evaluators to measure the performance of software services are discussed.

- Various trust models are explained, along with its characteristic and purposes and its influence on identifying trusted entities. The involvement of industry majors and setting up of working groups for trusted cloud computing ascertains the vision of trustworthiness for cloud interaction are reviewed.

- Conventional trust models for recommendation, QoS, Bayesian and game theory have presented their case mainly for assuring trustable service selection from a trustworthy provider. However, these models have not concentrated towards either the user trust or the service trust at runtime. Moreover, with the existing methods in use, trust adaptation and trust through cooperation is a daunting task.

- The review presented offers a vivid picture of behaviour models, attestation method and game theoretic trust evaluation techniques. The shortfalls of the different methods have been dealt with scrupulously. It is against such a background that this thesis proposes to adopt multiple strategic approaches with layers of trust phases for evaluation, assurance and enhancement.