1. INTRODUCTION

Convergence of distributed and service-oriented computing has created a strong capability towards access of web services everywhere. Performances of computing technology have improved enormously due to multi-core servers, virtualization technologies, high-speed networks, and a wide range of open source platforms. The confluence has led the computing, a paradigm shift towards accessing computational resources through multi-tenant architecture by procuring IT services on-demand. This pay-for-use model known as Cloud Computing, offers scalable and customizable resources with highest availability and cost efficiency. Adoption of cloud services by Small and Medium Business (SMB) enterprises, who contribute around 50% of global economy, has been phenomenal during the past few years. Almost 94% of SMB have used cloud services, and 64% have already adopted cloud-based software for their business processing [1]. The raising level of cloud adoption is proof that this technology is the platform for next generation computing.

1.1 COMPUTING IN THE CLOUD

The underlying technologies and infrastructures that make things work in the cloud environment are an amalgamation of, diverse computing paradigms that have evolved through the time of internet computing. The most important technologies are Virtualization of High-Performance Computing (HPC), where the underlying hardware are virtualized to enable a multi-client resource sharing environment, and Service Oriented Architecture (SOA), that provides a rule-based service delivery model on the internet. These backbone infrastructures enable the cloud computing to scale its storage and computational resources on-demand, rapidly. Even though cloud depends on the distributed environment; it can precisely monitor every resource consumed by a user. This combination of technology delivers multiple services online namely the three widely adopted service models for software, platform, and infrastructure.
Software as a Service (SaaS) model provides user interface delivery, on a subscription basis. The user accesses the service provider’s application deployed in remote servers through a web browser. The scalability feature of cloud applications reduces operational cost and software maintenance and hence, from enterprises to individuals SaaS is the most preferred choice.

Platform as a Service (PaaS) model enables the consumers to design, develop, test and deploy applications onto a virtualized cloud platform. PaaS provides customization of developer tools according to the needs for performing business intelligence, database integration, and workflow management.

Infrastructure as a Service (IaaS) model provisions together servers, storages and other fundamental computing resources like computation, networking, and bandwidth. Some of the examples include building an enterprise infrastructure, virtual data centers, and content delivery network.

Deployment of the above services requires them to be highly coupled and dependent on each other. For example, IaaS forms the base of all the services in the cloud, providing infrastructure resources virtually. PaaS built on the foundation of IaaS, abstract the operating system and middleware to provide a development environment. Finally, SaaS deployment on top of PaaS helps to provision applications to users.

Figure 1.1: Cloud services and application access
The functioning of the cloud lies in how a user accesses the required services with a simple request and response. Consider the use case scenario depicted in Figure 1.1, where the cloud facilitates a customer to consume an image processing application from multiple cloud service providers. These applications deployed on a web server suitable for that service, are built inside a virtualized infrastructure which is hosted in a remote data center. The availability of the Virtual Machines (VM) in the data center is based on the installed capacity of the bare-metal hardware, which in turn decides the number of users accessing that service.

The major benefits of cloud services are that the users are totally abstracted from the underlying layers and can concentrate only on utilizing the functionality of the services. For example, a SaaS user need not care about the version, compatibility, configuration of the host system or the data storage. Similarly, on PaaS, developers can just request and get the necessary tools and databases as a service and does not worry about the computational complexity of the underlying hardware. Again an IaaS consumer need not think about how and where the virtualized data centers are located or even worry about the reliability and availability of the VMs.

Apart from these well-established and standard services, there are several other services for security, communication, backup storage and mobile backend which can generally be termed as XaaS. Along with this, the scope of the proposed work helps to build two other services namely Trust as a Service (TaaS) and Attestation as a Service (AaaS). TaaS would offer various trust models to choose that can help to monitor a group of connected systems or services under surveillance. AaaS would offer verification and certification as a service, where multiple agencies coordinate to offer rule engines, to meet the certification standards for attesting an entity. The scopes of attestation services are very much in the initial stage of development, with numerous research activities and government agencies working towards it [2].

Deployments of the above services are classified into Public, Private, Hybrid and Community clouds. Public clouds can be accessed by any
individual or organization from anywhere. Services in the public cloud are owned and operated by third party service providers across various data centers. *Private* clouds, on the other hand, are deployed on-premises by a particular organization, to share the resources in confined boundaries. These types of cloud setup are adopted by large enterprises for which agility and efficiency are more important than cost factor.

*Hybrid* cloud deployment combines the benefits of private and public, primarily to extending the limits of resources. Critical and non-critical business could effectively be migrating between private and public for higher flexibility and cost efficiency. *Community* cloud, on the other hand, requires a different set of organizations to share the resources, either internally or externally for the benefits of resource utilization. Software applications make use of these deployment models to improve the adoption rate, however, security issues challenge it, in terms of frequent outages and attacks.

### 1.2 CLOUD SECURITY ISSUES AND CHALLENGES

Information Technology research analyst firms like Gartner, Forrester, and IDC have been predicting during the later stages of the last decade that, ‘*computing in the cloud would be the future of IT industry*’ [3]. This prediction has proved appropriate, and now the focus has now shifted towards market share of various cloud services and its impact on other industries. Therefore, adoption of cloud has largely seen as a changeover to the traditional model of computing around the globe. Such huge migrations towards cloud are due to its affordability, optimal utilization of available resources, On-demand scaling and less maintainability [4]. Though these factors are nurturing the growth of cloud, more concerns and issues are still persistent.

In an organizational perspective, one of the most significant decisions to identify the cloud service provider for hosting their application and infrastructure are *security, privacy, and trust*. These concerns are the major roadblock to full adoption of cloud. A recent survey [5] suggests the following as the most valuable use cases for prevention, detection, and response to threats.
- Assessing risk
- Identifying suspicious or malicious user behaviors
- Compliance monitoring or management
- Detecting external malware-based threats
- Increasing visibility into network and endpoint behaviors
- Detecting insider threats
- Baselining systems for exception-based monitoring
- Identifying compromised credentials
- Detecting policy violations and reducing false positives
- Creating fraud detection baselines
- Finding new or unknown threats

Moreover, organizations that have faced an attack are estimated to have lost thousands of dollars and faced immediate threats from unknown sources causing disruption of service [6]. Every year a major portion of the operational expenditure is spent towards mitigating these attacks for building security infrastructure, adoption of analytics, behavior pattern identification, and implementing security intelligence mechanisms [7].

1.2.1 Security, privacy, and trust

Cloud leverages many new technologies to make itself a massive resource pooling architecture; however, it also inherits their risk and issues. Apart from traditional issues, cloud computing poses new vulnerabilities whose impact might create a full-fledged crisis if left unnoticed. Earlier, the server-based computing has proven its resistance toward attacks through business level security policies and best practices. However, the changes towards service-based computing have eroded these well-established standard practices, making the entire cloud offering vulnerable to every type of security breaches. The vision of building a secure cloud requires the developers to design security, privacy, and trust at all levels of deployment.

Security is concerned with the preservation of Confidentiality, Availability, and Integrity (CIA) of the information. In simple terms, the information should not be disclosed or made available to unauthorized
entities. Enforcement of data protection using encryption and decryption establishes security in any system.

Privacy, on the other hand, involves safeguarding unlawful intrusion into personal information and rightfully disclosing it with the consent of the owner. Though privacy overlaps with security regarding protection, privacy essentially deals with handling mechanism of personal data while security deals with protection mechanism of data.

Trust revolves around control over visibility to assure that the information will be processed and will behave in the reliable and expected way. Trust and security have a complex relationship, for example, the absence of the safety in a system can be perceived by the user to have less trust in that system. Similarly, breach of privacy over personal data means that the system deviates from the commitment, leading to a lack of trust in that system. Considering this relationship, trust can be defined as a tuple involving reliability, security, and privacy as shown in equation 1.1.

\[
\text{Trust} = \langle \text{Security, Privacy, Reliability} \rangle
\]  

"Trust is a consequence of reliable security and privacy objectives."

The Figure 1.2, observes that enabling proper security through protection and assuring privacy through preservation can lead to trust in any system. Accordingly, a heterogeneous system like cloud computing must be capable enough to have all the privacy, security and trust objectives, to meet the challenges ahead [8], [9]. The following subsection identifies the need for trust in cloud based on performance and belief.
1.2.2 Trust in cloud environment

Trust is the degree of confidence and reliance towards something, which is expected to deliver as promised. This expectation leads to devotion towards an assurance of ‘what is being promised would be delivered.’ This devotion of trust can ensure any environment to be safe and secure. Trust spins around the certification and certainty that individuals, information, elements, data or procedures will work or act in expected ways. It is a critical factor, aided by reputation and behavioural analysis, facilitating dependability on various cloud computing services. In this context, trust can be defined as ‘the belief the trusting agent has in the service provider’s willingness and capability to deliver a mutually-agreed service in a given context and in a given time slot’ [10]. Trust can be of two types given the expectancy of trustor’s, first, trust in performance, and second, trust in belief [11].

A trust in performance can be expressed as in equation (1.2).

\[ T_p(T_t, T_e, P, C) \equiv \text{made by } (T_e, C) \supset \text{believe } (T_t, C \supset P) \]  

(1.2)

Here the trustee’s performances \( T_p \) are described through \( T_t \), the trustor’s trust; \( P \) is the performance of trustee \( T_e \), in a particular context \( C \). This association means that if \( P \) is prepared by \( T_e \) in context \( C \), and then \( T_t \) can believe \( P \) in that particular context \( C \).

A trust in belief is about what the trustee believes \( T_b \), equation 1.3 represent that trustor \( T_t \) trusts trustee \( T_e \) regarding its belief of the performance \( P \) in context \( C \).

\[ T_b(T_t, T_e, P, C) \equiv \text{believe } (T_e, C \supset P) \supset \text{believe } (T_t, C \supset P) \]  

(1.3)

It implies that if \( T_e \) believes \( P \) in context \( C \), then \( T_t \) likewise believes \( P \) in that connection. Trust in belief is transitive, trust in performance is not, however, trust in performance can be propagated through trust in belief. Hence the research work focuses mainly towards trust in performance, based on the objective parameters.
The choice of performance-based evaluation can increase the level of accuracy in trust evaluation. Though performance can judge the capabilities of trust, it is the belief that motivates the need for trust. Therefore, in an uncertain situation and precarious environment, it becomes necessary to take a calculated risk and believe in it. Hence, trust and risk are the two sides of the same coin, where trust can be the outcome of the accepted risk. The level of accepted risk depends on how well the trust relationships are established. Therefore, trust must be properly gauged with the level of risk, and estimate risk tolerance for good practices.

Thus computing in the cloud makes it vital for consumers, providers, and society in general to establish trust. Hence, a significant challenge lies ahead for a superior trustworthy cloud computing model. More specifically trust in software services becomes an essential factor for the cloud consumers.

1.2.3 Trust in software services

Software as a service has already emerged as a well-established delivery model for IT services. It delivers applications through centralized control, where the tenants are given a protected view of their implementation. VMs isolates the view from other tenants, and each tenant can have their metadata, using which customization for their users are carried out. The internal boundaries of SaaS consist of user data, presentation, and Application Programming Interfaces (API). Entry level security, version control, usage control and privacy coordination are its external boundary. Beyond this level, SaaS has virtually got no other controls over its underlying platform or the hardware infrastructure as shown in Figure 1.3.

In comparison, the traditional in-house application has better control and visibility, and the user has the right to view or modify his environment under any circumstances of system failure or attack. Therefore, it is natural to trust the in-house services. On the other hand, the cloud applications have virtually no access to its environment and hence trusting it is a risk with belief. Hence establishing a trust for SaaS is critical and challenging.
For securing a SaaS application, there are certain mitigation strategies to be addressed.

- First, the application must be built with an engineered approach, which must include and review the trustworthy capabilities at each phase of development (Architecture, design, and coding phases).

- Next, application vulnerability assessment regarding attack resistance capability, availability and accuracy must be judged.

- Finally, a third party SaaS security assessment for governance and compliance are ensured while the service is in operation.

So to have trust in SaaS model, our research gathers effective strategies and protocols to identify the trusted behaviour of the system through Cloud Brokers (CB) and Cloud Auditors (CA).
1.3 MOTIVATION

Cloud services have gained momentous ground in several domains like government agencies, healthcare, education, science and technology. However, despite its significance, the software services deployed in public cloud are most vulnerable to insider attacks, policy violations, and malware. Hence creating low-risk applications through trusted computing based on performance and behaviour analysis can justify the research focus.

Traditional security systems rely on signature and cryptographic techniques for data protection, which take its time to detect any changes in the environment. Hence a rapid detection and response mechanism must be in place to assess and monitor the events. Therefore the top most priority must be to identify any deviations in the system at the earliest stage through behaviour monitoring and analysis. Hence, evaluation of trust through evidence using QoS parameters would justify the purpose of monitoring the behaviour of the system [12]. Effective evaluation algorithms need to be proposed to address the challenges in evaluating the trust among entities.

Consumers expect a level of assurance for trustworthiness through the certification process. Therefore, an independent auditing mechanism can verify and certify the claims made by a cloud entity during service interaction. Thus an attestation process must be modelled to justify and satisfy the consumer’s expectancy.

Threats like collusion attacks have gained prominence in this competitive business-oriented cloud environment. Therefore a system strategy must be modelled and enforced among the entities by forming a coalition among cooperative players.

Many earlier approaches have proposed to evaluate trust separately, from certification process and its governance. Hence, there needs to be a comprehensive model that can provide a reliable solution for trusted services right from provisioning to dynamic adaptation. Therefore, the aim of the work is to create a novel trust model in this cloud ecosystem.
1.4 RESEARCH OBJECTIVE

Based on the motivations to assure trustworthiness in the cloud environment, the objectives of the thesis are as follows.

- To maximize the usability and acceptance of the cloud applications by developing a novel Trusted Cloud Attestation Model (TCAM) in a layered approach.
  - Monitor and assess the behavioural pattern of cloud entities through direct evidence of QoS attributes for uncertainty.
  - Assure the trustworthiness, by re-examining and certifying through a third party attestation process for building confidence and transparency.
  - Establish cooperation and goodwill among the stakeholders for a trusted relationship by having a strategic enforcement policy through cooperative game theoretic principles.

- Provide adaptation policies to address the untrusted entities, and assure to increase trust for greater adoption of cloud service deployment.

- Validate the trust model for its feasibility and practicability by implementing it using industry standard practices.

1.5 SCOPE OF THE RESEARCH

Trust is a special case of cloud security requiring multiple factors that must be observed in evaluating trust score. One of the most important factors in the assessment process is the collection of evidences for measurement. The present work aims to provide a trusted system that is adaptive in nature and validated in a heterogeneous environment with cloud users from various domains of knowledge.
The proposed trust model formulates trust for the three major cloud entities namely, the Cloud Service (CS), the Cloud Consumers (CC), the Cloud Service Providers (CSP). Though IaaS and PaaS indeed require trust models, they are not in the scope of our research work.

The trust evaluation approach is made for an image processing application deployed in a hybrid cloud with around 250 users accessing the service. Considering the network bandwidth, the service is built with only the required filters and processing capabilities.

The attestation system, functions at a remote location, instead of being at the provider’s location, to be considered it as a third party. The attestation process is carried out by a cloud auditor who independently functions based on the predefined protocols.

The work adopts the game theoretical principles especially the cooperative game strategies and policies for effectively identifying those who are having trusted interactions, and those who are maliciously avoiding interactions.

The evaluation methodology for the research adopts NIST cloud specifications and other international guidelines for designing the qualities of entities.

The model helps the tenants to choose the most trusted CSPs based on the trust score they have gained through evidences that are assessed through novel algorithms.

The proposed work helps in preventing attacks from malicious CSPs by forming a coalition of only trusted CSPs by defining a proper payoff characteristic function through cooperative trust, and thereby helps the providers to improve the capabilities of detecting attacks.

The trusted cloud management techniques are significantly improved in this work with an intent to employ software services for maximum serviceability and security for trusted components.
1.6 RESEARCH CONTRIBUTIONS

In this section, summary of major contribution of the research work is presented. The dissertation contributes to trust evaluation and enhancement based on the important characteristics of trust namely behaviour, compliance, transparency, relationship, and reputation. These trust features are developed into a trust model.

The novel Trusted Cloud Attestation Model (TCAM) identifies the trustworthy cloud entities based on three essential phases. The first phase identifies the behavioural characteristics of trust based on Behaviour Trust Model (BTM). The second phase assures compliance and transparency through Attestation Process Model (APM) and finally, the trust relationship and reputation features using Cooperative Trust Model (CTM).

1.6.1 Behaviour monitoring using BTM

In this work, a dynamic and efficient method is suggested based on QoS of the service and consumers trustworthy features, by collecting the evidence through direct observation.

- In this model, to judge the trusted configuration of the system, TCAM Client Capability algorithm (TCC) is proposed. Also to efficiently identify the trust value for the services and the clients, the work proposes a TCAM Trusted Services Evaluation algorithm (TTSE) and TCAM Trusted Client Evaluation algorithm (TTCE).

- An enforcement behaviour policy for login attempts is developed through a trial and error approach, which contributes to the research immensely. This approach identifies vulnerable cloud user who has the ability to gain authorization for malicious activity.

- A novel trust categorization based on the trust value is suggested for classifying the trusted entities. These zones of trust help to make adaptive strategies for enhancement.
• Our results demonstrate that the algorithms developed for TCAM effectively identifies malware injection attack, malicious insiders and runtime failures.

1.6.2 Trust compliance using APM

To assure the compliance and transparency of trust and to preserve the goodwill and confidence of the stakeholders, the research proposed the Attestation Process Model.

• In this proposed strategy, cross-examination of the trust score earned in the earlier BTM is verified with good known values for effectiveness using TCAM Cloud Attestation Protocol (TCAP).

• The transparency of the model is accomplished by enabling the model to work at a remote location administered by a third party auditor. By having this approach, all the stakeholders can share the information with the auditor through audit logs stored for the entire event.

• The work contributes to the faithfulness of the trust score by making all the entity to share the information based on the attestation principles. Hence compliance of the policy assures the users to trust the environment.

• Our experimental results deployed in a real-time OpenStack cloud environment have shown to have a minimum overhead with better availability.

1.6.3 Trust relationship using CTM

Establishing a relationship in an environment is a key factor to influence the trustworthiness. Many of the existing trust models focused on non-cooperative game theoretic principles for establishing equilibrium for service selection. Whereas, our proposed model uses cooperation principles create a coalition of trusted entities.
• A novel Strategic Enforcement Policy Monitoring System (SEPMS), implemented by the CTM enhances the trusted behaviour of the service providers through coalition formation.

• Recommends solutions to mitigate collusion attack and insider attacks through a strategy of cost sharing and an even playing field for all the service providers.

• CTM proposed to handle the adaptation of entities by having an adaptation policy that contributes towards improving the trust score by providing alternative choices based on where the entities are placed in the trusted zone.

• Comparative results have proved the undecidability and accuracy of the services with better performance.

Overall the research work contributes to improving the trustworthiness of cloud entities by enabling the cloud user to select trustworthy software resources and the cloud service providers to be assured good reputation.

1.7 ORGANIZATION OF THE DISSERTATION

The thesis has been organized into eight chapters. Chapter 2 presents a literature review of various types of trust models. Survey on behavioural trust and how QoS attributes have defined the trust evaluation are carried out. Existing usages of attestation and its governing principles by various researchers for establishing trust are clearly described in this section. The need for a coalition and how cooperative game theoretic principles have effectively identified trust in the cloud are surveyed. The drawbacks of these models are pointed out for effectively sorting it out in our proposed work.

In Chapter 3, a brief introduction on the proposed architecture of the Trusted Cloud Attestation Model, with various phases is illustrated as an algorithm. An essential element of QoS attributes for evidence-based behavioural trust analysis and security attributes are discussed. The need for priority ranking using AHP for all the QoS metrics is elucidated.
In Chapter 4, the BTM with its evaluation process to estimate the trust value for the two cloud entities namely, the service, and the user are calculated. The implementation and results of the model are given to validate the functionality of the proposed work.

The need for auditing by a third party auditor who verifies the authenticity of the evaluation using benchmark standards and attests the services and users of the cloud are presented in Chapter 5. Cloud attestation protocol and its algorithms that follow a pre-defined principle of attestation are explained through implementation steps.

The necessity for coordinating in the cloud requires a trustful cooperation among the participants are emphasized in Chapter 6. To achieve this cooperation, the requirements of a rational game play using a game theoretic approach have been modeled. Descriptions of CTM with its proof with different cases for cost sharing coalition policy are defined.

Chapter 7 demonstrates the implementation of TCAM using OpenStack cloud platform for a hybrid cloud environment. Comparative results regarding qualitative and quantitative are illustrated.

The conclusion and potential future areas of work that could be carried out in continuation of this research are presented in Chapter 8.