Techniques used for establishing Cloud Service Trustworthiness: A Survey

Poornima A. B.
Computer Science & Engineering
Dayananda Sagar College of Engineering
Bengaluru, India
poornima.dsce@gmail.com

Navneeth Krishna M.
Computer Science & Engineering
Dayananda Sagar College of Engineering
Bengaluru, India
navneeth.padaki15@gmail.com

Nishchala M.
Computer Science & Engineering
Dayananda Sagar College of Engineering
Bengaluru, India
nishchalamkumar12@gmail.com

Oindrila Chakraborti
Computer Science & Engineering
Dayananda Sagar College of Engineering
Bengaluru, India
oindrila2411@gmail.com

***Abstract*— The goal of this survey paper is to review and present a detailed comparison of the current approaches in improving the domain of Cloud Service Selection. Establishing parameters for cloud service trustworthiness is the primary need for Cloud Service Selection. However, limitations such as biases in datasets, lack of standard tests to assess trustworthiness, and minimal flavors of Cloud Service Providers pose a challenge in establishing these parameters which in turn are necessary in assisting Cloud Users choose the service that is most feasible for their requirements. Analytical Hierarchy Process (AHP) is one of the most frequently used procedures to evaluate trustworthiness while other techniques include Multiple Criteria Decision Analysis (MCDA), Naïve-Bayes Classifier, Markov Chains, etc. In these approaches, priority is placed on specific Content Areas (of a Service Level Agreement) in order to define a trustworthiness quotient. We delineate each approach—its features, algorithm(s) used, weight asserted on each Content Area, and relevant characteristics in our survey. In addition to this, we juxtapose the findings of the above methods to effectively learn their efficacies.**

Keywords*— *Cloud Service Selection, Cloud Service Trustworthiness, SLA Content Areas

I. Introduction

Cloud Service Selection has progressed as a cloud computing paradigm of entrusting good faith in a Cloud Service Provider (CSP) for the services with specifications that are legally agreed upon by the involved parties. The procedure of selection narrows down to multiple factors that vary based on a user's needs, the environment(s) in use, the volatility of the service(s) required, and the scale at which the transactions are made. Due to the dynamic and fast-moving nature of a CSP's operability, keeping track of all the factors involved in choosing a reliable cloud service becomes tedious, resource-intensive, and expensive to maintain consistency in the predictions about reliability. Since such detailed moderation is rendered unfeasible, predicting the reciprocation of commitment to the service agreement narrows down to the most important quality of this paradigm known as Cloud Service Trustworthiness.

Trustworthiness can be defined as the ability to be relied on. In terms of cloud computing, it can be defined as the worthiness of a service and its provider when it comes to being trustable. This parameter is ranked as top priority with regards to cloud computing as Cloud Customers (CC) have to entrust their critical data upon the CSPs, which if lost, might incur a huge loss to the CC, both financially and contractually. In addition to this, the service provided by the CSP needs to meet all the requirements and specifications that have been mentioned and agreed upon in the Service Level Agreement (SLA). The requirements and specifications (e.g. performance, scalability, availability, reliability, response time, downtime, etc.) serve as parameters while calculating the trustworthiness quotient. If the required facilities are successfully provided to the CC, while maintaining the confidentiality and security of the CC's data, the CSP is deemed as trustworthy, and therefore, has a high trustworthiness quotient.

The abundance of seemingly similar Cloud Services and the enormous range of customized user preferences and requirements have led to difficulty in choosing the optimal CSP. Some of the main issues faced by CC are lack of trust in service providers with respect to availability, reliability and efficiency of services at their time of need, ambiguity in SLAs, non-compliance with SLA, absence of diversified trust elements, and Quality-of-Service (QoS) guarantee. The changing user preferences also pose as an obstacle for instant assessment of CC requirements in real-time. In existing systems, users don't have freedom to assign weights to their preferred characteristics (like Security, Availability, Reliability, Cost, Latency, etc.) in CSPs. Traditional Cloud Service Selection models use very few attributes in the trust evaluation process which might not be sufficient for CC. Users need transparency, unbiased evaluation of trustworthiness, and reliability in Cloud Service Selection tools before deciding the most suitable service for them.

II. Surveyed Techniques

Among the latest Cloud Service Selection Techniques, we have shortlisted those that provide robust experimentation, structured models, and high ranges of measures of trustworthiness. The approaches are broadly classified under four major survey techniques and are as described:

A. QoS-based approaches

In traditional interpretation, cloud service selection is primarily focused on QoS requirements of an end-user. These requirements in turn help prioritize Content Areas of an SLA. Although QoS parameters vary in each domain, their role meets the common ground with many techniques:

—*Using a Markov Chain.* Keeping in mind the limitation of changing user preferences (UPs) that contribute to the uncertainty in identifying the trustworthiness of a cloud service, F. Nawaz et al. [1] utilize a Markov Chain (MC) to generate a pattern that can establish the priorities of QoS criteria. The MC is also used for identifying transitional patterns present within the changes. QoS priorities effectively rank the services offered by a cloud. Initially, the MC is applied to the required transition matrix and the primary UPs. In each iteration of all the UPs, its relation with the QoS criteria is figured and the best and worst criteria are noted. Based on this, optimal weights are calculated using a method known as the Best-Worst Method; a category of Multiple Criteria Decision Analysis (MCDA) (discussed in *D*). After all the passes, the final QoS weights are computed while considering their relations to user preferences. From the QoS repository, the criteria are matched and then the QoS values are normalized. This helps in finding out the final service ranks. This approach makes comparisons with respect to all available QoS parameters such as performance, price, reliability, and availability. This technique takes into account the possibility of changing user preferences which render it customized and incomparable with most existing techniques. However, when compared after the elimination of the Markov Chain, we learn that most systems, that utilize Analytical Hierarchy Process (AHP) for pairwise comparison, prove inefficient when compared to BWM which is a vector-based algorithm that makes fewer comparisons than matrix-based algorithms (e. g., AHP). The study brings to light the fact that about 80% of the trials to determine weights using BWM are consistent when compared to a meager 60% consistency as displayed by AHP and using further evidence, F. Nawaz et al. gathers that BWM is better than AHP in terms of reliability (not to be confused with QoS criteria). Consistency Ratio (CR) is a measure that graphs the inconsistency of MCDM methods and it gives a measure of the quality of the produced results.

—*Real-Time Global Trust Degree.* Noticing how most models use simple or very few trust-based attributes to calculate trustworthiness of CSPs and reach incorrect outcomes of the overall trust calculation, L. Bao [2] suggests that more trust elements like availability, reliability, security, etc. of resources must be included in the trust evaluation technique of CSPs. These attributes become the deciding factors of evaluation of trust by SLA compliance and QoS guarantee. Two types of Software Agents — Monitoring Agents (MA) and Computing Agents (CA) are used to collect Cloud Service evidence i.e., performance parameters of several attributes over a period of time. The matrix consisting of attribute values or evidence is normalized depending on the expected positive increasing value or expected positive decreasing value over the domain [0,1]. Normalization equations are used for the aforementioned two cases which result in a new matrix called Evaluation Matrix. The model aims at computing real-time Global Trust Degree (GTD) which is governed by historical evidence on the trust attributes of CSPs over certain time slots. Hence, GTD value based on QoS establishes a trust relationship between Cloud Customers (CC) and CSPs and also deals with the dynamic nature of the services provided to the CC. Comparison of this model with other trust evaluation systems like Simple Trust Model (STM) and models that involve Fuzzy Logic suggests that the Mean Absolute Difference (MAD) between the predicted and actual outcome is 9% and 5% less respectively. This relatively lower MAD indicates that L. Bao's [2] model establishes an optimal technique to assess trustworthiness with higher accuracy. The trust system and SLA architecture are embedded with each other which enables the system to provide suitable trustworthy services for CCs at their time of need dynamically. This enables the CSPs to meet their QoS requirements.

— *Linear Regression Model.* The pay-as-you-go feature of many CSPs has enabled enhanced scalability in providing resources based on the requirements of Cloud Customers (CC). Incidentally, scalability introduces a more challenging trust relationship between CSPs and CC as users must depend on the availability of services at the time of need. In addition to scalability, users need an effective system to rank CSPs on their distinct QoS parameters based on specific user purposes. Mahesh K et al. [3] suggest a Linear Regression Model to assess trustworthiness and choose the most optimal candidate among several Cloud Services based on user criteria. Initially, Linear Discriminate Analysis (LDA) technique used for clustering and ranking similar services according to their QoS scores. LDA aims to filter out the services which are not along the lines of QoS attributes specified by calculating the similarity degree between service request and service. After the initial confidence is established using LDA, CC should verify confidence further by observing the adherence to SLA on the grounds of transparency, integrity, compliance, and competency in the past. If SLA verification is carried out by a Cloud Broker (CB) who acts as an intermediary entity between CC and CSPs, then the trust quotient partly depends on confidence between CC and CB. This is known as a reputation-based trust mechanism system. The model analyses different services based on QoS parameters – Response Time, Throughput, Availability, Success ability, and Price in the first step. In the next step, further confidence is checked by computing the trust score and ranking of services – out of nine CSPs in the evaluation process, the best service scored 0.4740 while the worst service scored 0.2724.

B. Approaches based on Standard Organizations

Organizations & Initiatives such as Cloud Security Alliance (CSA), CSA Cloud Controls Matrix (CCM), Consensus Assessments Initiative Questionnaire (CAIQ) form the basis of many entity relationships in a standard representation of any Cloud Service Architecture. Moreover, they also serve as benchmarks and tools for techniques like Clustering and hierarchical prioritization of Content Areas. Several researchers utilize the aforementioned standards in their assessment of Cloud Service Trustworthiness.

—*Entrusted Trust Model.* The limited and non-transparent monitoring of services and unavailability of means for choosing reliable CSP based on CCs' requirements have led to an urgent need to establish an architecture to support the best CSP for their operations after careful deliberation over their QoS attributes and performance measures provided by authentic sources. Existing Trust and Reputation (TR) systems give equal weightage to all sources and feedbacks and neglect that some might not be trustworthy. Hence, S.S. Roy et al. [4] propose the ETM system that uses the Consensus Assessments Initiative Questionnaire (CAIQ) to filter out the unreliable sources to avoid misleading CCs about promised SLA compliance and QoS feedbacks. The average rating of CSPs, the certainty of this rating, and initial expectation associated

with the service are taken into account for calculating the final expectation of performance of services. The ETM system comprises of Registration Manager (RM) – CSPs register in the marketplace through the RM and fill the CAIQ which is sent to the CAIQ Engine and Trust Information (TI), CAIQ Engine – consists of all the questions which are answered by CSPs and further stored in TI, Trust Manager (TM) – takes in user requirements, Trust Semantics Engine (TSE) – converts the requirements into Propositional Logical Terms (PLT) and send the customised PLT to Trust Computation Engine (TCE) which carries out the evaluation of trust value of services, Weight Measurement Engine (WME) collects feedback from trustworthy sources and assigns weights to the attributes based on the level of trust of the source and passes on to Trust Update Engine (TUE) which updates the previously calculated trust of CSPs based on the weights computed by WME. It is assumed that all CSPs should submit legally acceptable answers to CAIQ which are verified by Cloud Security Alliance (CSA) stored in TI. The trust measurement is carried out in three steps: the TSE forms the PLT, feedback from genuine information sources is collected according to CAIQ and the average rating of the service, certainty of the rating and initial expectation are computed, lastly, weights of the information sources are updated and Degree of Conflict (DoC) is used to interpret user behaviour. These updated weights and DoC are used to update the new trust factor of CSPs. It is observed that weights differ after feedback is provided which in turn, affects the overall trust of services.

—*Trust Management System.* S. M. Habib et al. [5] state that the main objective and purpose of their paper is to provide an overview of the Trust Management (TM) System and how it functions for a cloud marketplace. The various technologies that are used to establish trust in the CSPs are elucidated. With respect to SLAs, SLA monitoring and validation schemes are used as a source of quantification of the services offered by a CSP. Cloud providers also use various audit standards, SAS 70 II, FISMA, ISO 27001 to name a few, as proof of the platforms and features offered to their customers. Cloud providers are also rated by their existing customers via rating questionnaires. The Cloud Security Alliance (CSA) proposed an intricate questionnaire to analyse the competence and capabilities of CSPs in terms of different attributes (e.g. compliance, reliability, scalability, performance, etc.) for the purpose of security and transparency. TM models have served their purpose in various decision-making scenarios (e.g. p2p networks, product reviews, e-commerce, etc.) and these systems need to possess some desirable properties to function effectively. This means that TM systems must possess the ability to aggregate and collect data, the data collected must be as diverse as possible and must be collected from numerous sources, the subjective interests specific to each customer must be taken into consideration, knowledge about the complexity and architecture of the subsystems must be known, the trust values need to be transparent and comprehensible, and finally, the TM system needs to be attack-resistant to false modifications.

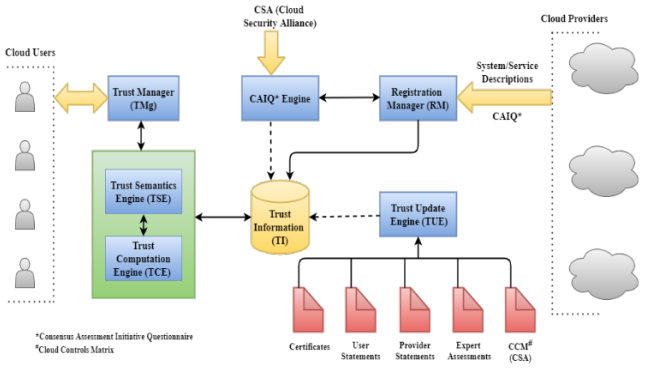

Fig. 1. Architecture Overview of The Trust Management Model proposed by S. M. Habib et al. [5].

S. M. Habib et al. [5] propose a novel architecture of a TM System (Fig. 1.) in the field of Cloud Computing. It consists of a Registration Manager (RM) through which CSPs can register themselves into the cloud marketplace, a Consensus Assessment Initiative Questionnaire (CAIQ) Engine which enables the service providers to fill in the questionnaire via an intuitive graphical user interface (GUI), a Trust Manager that allows the customers to list out their specific requirements, preferences, and opinions while they look at performance scores of CSPs, a Trust Semantic Engine (TSE) which is used to judge the performance of a CSP solely according to a specified attribute, a Trust Computation Engine (TCE) which is closely intertwined with the TSE to compute trust values, and a Trust Update Engine (TUE) which is used to collect opinions about the trustworthiness of CSPs and filter them according to the user's requirements.

—*Cloud Controls Matrix.* CCM is an initiative by CSA that deals with describing control guidelines for a cloud service's provision of security. Under the control guidelines, there are control domains that are further divided into a number of controls. In CCM v3.0.1, we observe 133 controls. According to Kanpariyasoontorn & Senivongse [6], it is pertinent to analyze the feature of each CCM control in order to produce a trustworthiness metric. The method proposes a Cloud Service Trustworthiness Assessment Method (refer Fig. 2.) which initially defines the attributes & sub-attributes of Security and Dependability as Trustworthiness is defined to be a result of them. Sub-characterization of Security & Dependability ensues and the new attributes map associations with the following standards: (1) The NIST SP800-53 Control Standard and (2) AICPA Control Standard both of which map to the CCM. Next, we define a degree of association between every CCM control domain and sub-attribute with a matrix called 'Association Matrix'. To illustrate, a control domain like Application & Interface Security has degrees of 0.75, 1, 0.75, and 0 for the sub-attributes Confidentiality, Integrity, Availability, and Reliability respectively. The assurance weights for the control domains must be calculated because security assurance is one of the two components that influence trustworthiness. With the mathematical product of the assurance weights and the degree of compliance of a service with a given control domain, we establish the capability of a service 'P'. A service capability matrix is constructed by merging all the service capabilities and is multiplied with the Association Matrix to yield the Service Trustworthiness.

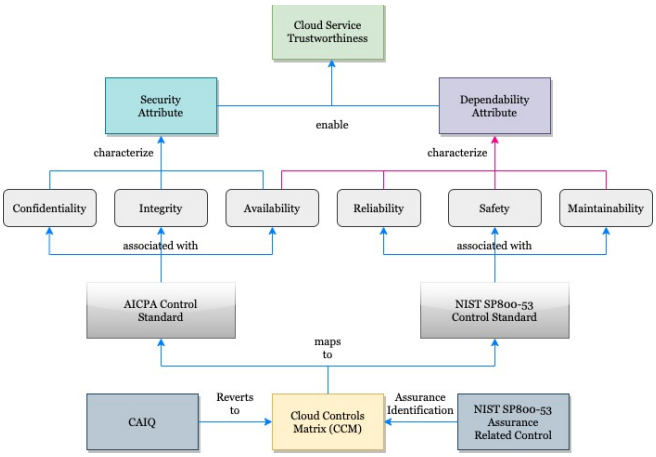

Fig. 2. An overview of Cloud Service Trustworthiness Assessment Method proposed by Kanpariyasoontorn & Senivongse [6].

This technique presented a self-assessment mechanism which clearly raises questions about biases and the validity of the service trustworthiness. A germane observation is that CSA is an esteemed organization whose repute holds value enough to treat Kanpariyasoontorn & Senivongse as a promising methodology for assessing trustworthiness.

C. *Approaches based on Fuzzy Methods*

Fuzzy methods are a type of multiple-valued logic that extends its applications to even Cloud Service analyses. The truth values of the variables in a Fuzzy methodology hold a real-value between 0 and 1 (both inclusive). The topical research in the field of Cloud Service Trustworthiness that makes use of fuzzy methods is described:

—*Evaluation and Comparison via Fuzzy Neural Networks.* Z. Wu and Y. Zhou [7] state that their off-center fuzzy neural network (FNN) handles diversified trust elements for evaluation of the trustworthiness quotient. Neural networks are known to learn from training data. This feature is of paramount importance when it comes to improving the accuracy and credibility of the trustworthiness evaluation. The result/output obtained from FNN can be modified depending upon proper feedback training. To achieve this, an improved back propagation algorithm is used. The structure of FNN is comprised of five layers. The first layer is an input layer where all the chosen trust element data will be categorized and put into a combined and unified format as a data package. The reason behind the requirement of a unified data package is due to the fact that FNN cannot simultaneously compute both qualitative and quantitative data. The second layer involves extraction and transformation of the data packages containing the trust elements into vertices which is contained in six dimensions. This entire procedure is handled by the FNN framework. This step is performed after the first layer completes its entire packaging process. The transformation into vertices is carried out according to the identified trust space. Trust element space is used to establish and more accurately represent the nature of each element under consideration. It can also be used to assort any candidate elements which might appear in future instances. This trust space is multi-dimensional. It consists of six axes which include internal and external axes, subjective and objective axes, and direct and indirect axes. A subjective element can be defined as an element that is based on the judgement (subjective) of a trust evaluator whereas an objective element possesses a measurement for its exact value. A Minimum Coverage Polyhedron (MCP) is then used in the third layer to calculate and calibrate the overall properties of the complete data package where it will be refined as a polyhedron in six dimensions. A histogram table is generated by the algorithm used in MCP which contains the distances between all the trust elements under consideration and a central point in the polyhedron. The central point of the aforementioned polyhedron is obtained by a Graham scanning algorithm. It reduces the six dimensions down to two. The fourth layer comprises of neuron units that use fuzzy representations for single or composite trust element six dimensional values and fuzzy rules which are used in customized trustworthiness evaluation. Thus, this layer is deemed as the multi-criteria analysis layer. The trust elements talked about are obtained from domain information where certain elements might be available only in certain services. These are called special elements and require domain ontology for their recognition. Uncertain and subjective information is handled well due to the fuzzy logic contributing towards the analysis of trustworthiness. The effectiveness of the FNN-based trustworthiness evaluation framework is done by collecting experimental data from cloud-based services. Email service providers, consumer reporting websites, online survey results, online consumer feedback sites, etc. are used for this purpose. The result is used to picture and analyse a group of consumers' observed weights over different features of cloud-based service's trustworthiness.

—*Analysis and Validation using Fuzzy Logic.* Pandey & Daniel [8] make use of Fuzzy Logic for building a Cloud Service Trustworthiness Model (CSTM) whose goal is to provide a fair evaluation of the trustworthiness of cloud services. The design focuses on agents for 'Requestor' and 'Provider' that are stakeholders which participate in the smooth functioning of a cloud service. As and when these stakeholders request or register for a new service, common and special parameters that constitute trustworthiness are involved in a weighting and positioning process. The listed parameters are defined with first and second grade indexes before determining their weight distribution for both indexes. A Level is ascribed to different parameters based on their quality and an evaluation Fuzzy Matrix is constructed for the first-grade index. It denotes the membership degree of a given parameter of a cloud service in specified trustworthiness levels. Processing through the Fuzzy Comprehensive Evaluation Model is a cardinal phase. Here, the overall trustworthiness membership degree of a cloud service is solved for on different levels. The final result brings about an adjective like 'high' and 'low' for trustworthiness levels of individual parameters. This stakeholder-based topology not only evaluates the overall trustworthiness of a cloud service but also the trustworthiness of individual parameters such as Security, Maintainability, and Usability.

D. *Approaches based on Multiple Criteria Decision Analysis*

When there are many parameters in the ingredients of trustworthiness, there arises a possibility of conflict. In order to explicitly evaluate these flavors to make optimal decisions, MCDA provides the necessary system. Some Trustworthiness models incorporate MCDA for constructing schematics:

— *Multi-Dimensional Dynamic Trust Evaluation Scheme (MDTES).* The primary entities in the proposed solution

include CSPs, CCs, Cloud Auditors (CAs), SLA Agents (SLAAs), and Cloud Brokers (CBs). Compliance information attributes of the cloud entities need to be ordered correctly to measure and evaluate trust. A few examples include SERVICE_SLA and SERVICE_INFO. Based on the QoS parameters (reliability, stability, etc.), a compliance report is generated from the information collected from all the cloud entities. Challagidad and Birje [9] describe the steps of MDTES where the first step involves the Compliance Information (CI) to be supplied to the CA which is collected from all cloud entities. The received CI is then sent to PMS which generates the CI report based on QoS parameters after examining it. After the CI report is received from the CA or PMS, the trust evaluation process is initiated after improving the current existing TOPSIS (i.e., Analytic Network Process and Minowski distance). The trust metric is obtained after the evaluation is handed over to MDTES to evaluate the trustworthiness of CSPs and CCs as per the obtained decision. MDTES is dynamic in nature, its robustness is shown when it dynamically changes to accommodate an increased number of CSPs and CCs as per the judgment. This entire processed metric is then transferred to the CA. If either the CC or CSP requires this metric, they can request it from the CA. The trust evaluation mechanism carried out by the MDTES involves the allocation of correct weights to the cloud entities after the CI is obtained. ANP is used to determine the weights. In case of revision, a recently completed service that was offered by a CSP is used to update the trustworthiness quotient via MDTES. CLOUDSIM is the software used for simulating the working of MDTES. For this process, it is assumed that both the CC and CSP have a data center at their premises. MDTES builds trust and evaluates it into three types, namely– trustworthy, untrustworthy, and arbitrary CSPs. CSPs that provide high compliance services based on the discussed QoS parameters build more trust when it comes to their functionality and their trustworthiness quotient almost comes up to 1.

—*Support Factor Clustering, Trust Factor Aggregation, and Minimum Polyhedron Technique.* CCs and CSPs often don't have clear information about each other for cloud service selection. A trustworthy relationship should be established between CCs and CSPs on the basis of the reputation of services as well as suitable trust factors. Due to the unavailability of uniform trust metrics for different kinds of services, L. Wang and Z. Wu. [10] propose a trustworthiness evaluation framework which is made of five sections. The Pre-processing Section collects trust factors (quantitative and qualitative) of CSPs which are categorized and converted to a unified scale using the Trust Factor Management Section. Trust coordinate is used to further categorize them into Subjective trust, Objective trust, Direct trust, Indirect trust, Inflow trust, and Outflow trust. Entropy value is used to define trustworthiness metrics (value between 1 and -1 where 1 is completely trustworthy and -1 is untrustworthy) to measure the uncertainty in trust relationships. These factors are then sent to the Trust Factor Processing Section for further processing like updating of common factors, dealing with special factors with trust ontology alignment approach to formalize the meaning of trust for a clearer understanding for user expectations, and assigning weights to all factors which are then employed in the multi-criteria analysis approach by the Trustworthiness Decision Making Section to measure, rank or sort cloud service candidates. Trust Computation using MCDA is carried out by Support Factor Clustering (based on Support Vector Machines and clustering as per CC requirements), Trust Factor Aggregation (functions of factor addition and multiplication are used to aggregate trust factors of services), and Minimum Polyhedron (finds the minimum polyhedron that covers all trust factors in trust coordinate system). To store the result for referencing it later, the Trustworthiness Record Section is utilized. The accuracy of the results is consistent after three-fold verification is carried out by comparing the outcome with feedbacks, data of revenue, and client growth rate as well as reviews from experts of third-party organizations.

E. More Approaches

In addition to the techniques discussed above, there are prominent methodologies that assess cloud service trustworthiness using unique technologies, algorithms, and specifications. Below, we see many such versions:

—*A Trust Label System.* As the name indicates, a label is associated with trust values. Emeakaroha et al. [11] present a model with knowledge-based trust relationships that are more robust than calculus-based trust relationships. A methodology known as 'Delphi Methodology' is utilized to derive a trust label interface that has (1) the main section and (2) a service level summary. Composite metrics like Data Portability, Data Location, Ownership, etc. primarily work on accumulating trust with the users. Implementing a service monitor framework is based on an average calculating mechanism that is run using a service monitor core. Compared to existing techniques, Emeakaroha et al. offer a considerable augmentation in terms of a means to communicate detailed and real-time information to their users. As this functionality is unique to this research, the Trust Label System fares better than traditional trustworthiness assessment procedures.

—*Compliance-based Trustworthiness Calculation.* The calculation of this mechanism follows the proposed approach that Sidhu and Singh [12] have elucidated where the first step involves negotiation and finalization of a SLA where the CC and CSP negotiate and reach a consensus which specifies the service requirements and performance standards followed by the signing of a contract in agreement to the aforementioned parameters. SLA consists of measurable entities such as reliability, performance, response time, availability, etc. Not keeping up with the decided standards will cause disciplinary action to be taken on that side that does not strictly follow the SLA by the other side. The second step involves monitoring service installation at the user end. These services intend to monitor the QoS parameters as modified by the SLA. Any number of monitoring services can be installed, each responsible for examining a particular parameter. The third step entails the storage of the monitored results from the previous step. The results obtained only for agreed QoS parameters are stored in the database. These will be used further on for compliance checking. The fourth step involves the generation of a compliance report where a specialized set of formulae are used to obtain the compliance which is calculated from parameters that are normalized between 0 and 1. Variables such as services, service providers, parameters, etc. are used in this step for the calculation. In the fifth step, the user can request for compliance reports from specific CSP's peers to know where the performance of that particular CSP stands in the marketplace. Peers opinion is created by compiling all the opinions obtained by the peers. The sixth

step deals with the aggregation of the compliance reports that were received from the peers. It makes use of variables such as compliance (obtained from step four), service providers, peers, etc. The aggregated variable is called Peer Compliance. In step seven, the results from step four and step six, Compliance and Peer Compliance respectively act as weights while computing the trustworthiness of a service provider (TSP). The simulation of this specific model is carried out in MATLAB.

—Using *Decision Trees.* One of the fundamental steps prior to assessing cloud service trustworthiness is assigning weights to SLA content areas. This step is efficiently addressed with hierarchical clustering and other algorithms under the purview of Machine Learning. In Venisha A. & Murali [13], we notice a broker-agent arrangement between the user and the SLA. A Feedback Provider updates the dataset while working with four layers: Broker Layer, Redirection Layer, Validation Layer, and Web Application Layer. At every level, a Decision Tree Algorithm is utilized and is carried out alternatively in various steps until the tree is built completely. When compared with other techniques and their accuracies like T-Broker with 80% accuracy, Multi-layer Perceptron with 92%, and Support Vector Machine with 92.45%, Decision Tree stands at a high accuracy of 95%. Venisha A. & Murali also discuss this methodology as an energy-efficient technique to ranking CSPs based on trustworthiness. Utilization of the CPU is maximized and is highly productive in calculating the trust metric.

—*Threshold and User Preference Clustering.* Existing models for Cloud Service Selection do not take into account the similarity in user preferences which seem personalized and unique for each user. To consider the context information and specific user requirements, as well as interaction, requirement personalization and similarity, QoS diversity, complexity and trustworthiness between service providers and users, Y. Wang et al. [14] propose a Cloud Service Selection method based on Trust and User Preference Clustering which follows a six-step procedure to produce the final measure of trustworthiness. Firstly, all CSPs register to the cloud service registration center. The Cloud Customers' (CCs) requirements are sent to the framework as personalized preferences. Condensed hierarchical clustering method is used to cluster requirements and the distance between these clusters is measured as per user service weight preference similarity, user service attribute score similarity, and user evaluation similarity in the third step. Threshold-based hierarchical clustering algorithm clusters repeatedly based on the similarity of preferences until 'K' clusters are present and their distances are measured. The optimal cluster is obtained by assessing the cluster structure degree. The comprehensive trust, sum of direct trust, and recommended trust are evaluated in the next step. Direct trust is calculated with the help of attribute weights (objective weights are calculated using improved entropy weighting method and subjective weights are calculated using AHP), attenuation time, transaction amount, and penalty factor. In order to prevent false reporting of direct trust by malicious users affecting the CSPs' reputation in the market, recommended trust (intra-domain recommended trust and extra-domain recommended trust) is also calculated. Recommended trust is the measure between a user and an intra-domain/extra-domain recommender of the CSP. Lastly, CSPs are ranked based on their trustworthiness. Based on the user's choice the weights are assigned to direct trust and recommended trust and the final comprehensive trust is computed. This trustworthiness is the deciding factor of the service that is chosen for particular user requests. The improved condensed hierarchical method proves to be better than traditional methods with respect to running time of clustering, iterations taken to cluster, and convergence speed. This method has the lowest Mean Absolute Error and Root Mean Square Error as well as the highest Success Rate for different number of transactions and interactions which vouch for the feasibility and effectiveness of the technique and the capability to identify malicious services and feedback.

—*D-S Evidence Theory-based Fusion Model.* The Dempster-Shafer (D-S) Theory was first proposed by Dempster but formally established later on in 1976 by Shafer. J. Liu et al. [15] states that the belief functions in this theory have been used to combine diverse and conflicting pieces of evidence, to represent and modify uncertainties, and to consolidate information from various sources. The term 'Fusion Model' talks about how due to the absence of any prior knowledge in the field of web service trustworthiness, the trustworthiness metric declared by the Web Service Providers is the only source available initially. However, once a customer starts to use a service, and later scores it according to its performance, the accuracy of the trustworthiness metric will increase, but the information provided by both the users and providers may be fuzzy and subjective up to a certain extent. The service cloud comprises of four entities (sub-agents) namely, the requestor agent, the service agent, the register agent, and the fuse agent. Here, the requestor yields a request to the requestor agent and the provider later forwards its service and delivers it to the service cloud. Thus, the opinions and feedback of the requestors can be easily collected and stored from which trustworthy content can be extracted and trustworthiness can be calculated dynamically. Trustworthiness for the above model can be obtained from various categories, and the procedure for obtaining these categories is deemed as 'Fusion Process'. The first category involves extracting trustworthiness from a Service Provider. It is not possible to be convinced solely by the declarations made by a service provider, therefore, if the particular service's performance can be compared to a similar service whose trustworthiness quotient is believable, then it can be assumed that the service under consideration will deliver average performance as well. The second category involves obtaining trustworthiness from a Service Requestor. Users can throw light on valuable information about the services they have used via tagging, rating, or even grouping the resources/services that are similar. These can be exploited to find web sources which are credible. A few basic recommender systems or rating systems (e.g., Amazon, eBay) already exist which simulate the social recommendation and trust experience for all requestors. The third category involves extracting the trustworthiness component from a Service Agent. It can be calculated using parameters such as usability, reliability, and security. Usability is the degree to which an application or product can be used by certain requestors to achieve personalised and specific goals effectively. Reliability is defined as the ability

that a particular service possesses to complete a specified task in a particular condition and within the given time frame. Security is a parameter that can be offered by the Service Providers according to the requirements and specifications listed by the customers. Guaranteed methods are provided for this parameter. A series of comparisons provided the comparative results that corroborated the practicality and feasibility of the D-S Evidence Theory-based Fusion Model. Thus, it can be justified that through fusion trustworthiness the chances of service discovery increase.

III. OBSERVATIONS

The surveyed techniques focused on establishing a quantitative measure of trustworthiness in order to compare the services as well as the service providers. Different nomenclatures like Trust Metrics/Factors/Elements/Labels were used for the same areas that are the Content Areas of an SLA. The architecture of the model, although having different goals, consists of similar associations (e.g. between CAIQ, Content Areas, Trustworthiness Evaluation, etc.). Matrix-based evaluation is used almost by default in many of the standard techniques. A hierarchy was pivotal wherever clustering was involved.

Decision Trees were the obvious choice for categorizing labels to move the system towards calculating various other metrics that were determined as influential. It was observed that MCDA is the most frequently utilized segregation tool to classify the Content Areas. Approaches tried to build systems/frameworks/models that can function independently or serve a purpose while addressing a limitation or while tackling an existing solution.

We learned that the need & role of each content area must be well-defined and a metric to assess them individually and as a whole form the fundamental truth of trustworthiness. The weights associated with each Content Area must be customized to the user's needs and assuming or predicting user weights must be avoided. This can be met through questionnaires and consumer-friendly user specifications.

QoS was efficient in prioritizing Content Areas that are most relevant in evaluating trustworthiness. Clustering techniques go hand-in-hand with assessing trustworthiness as the vast amount of Content Areas explicate its need. Moreover, Clustering is utilized for categorizing user requirements based on similarities.

Normalization of quantitative figures derived from Content Areas is a requirement to techniques that have to quantify qualitative Content Areas (e. g. Security, Scalability). A few techniques used the minimum polyhedron method in their models.

Standards like CAIQ and CCM predominantly influence the assessment techniques as their definitions are constant for any service provider or the service(s) that are offered. The standards also help better understand the security facilities of a given service.

Fuzzy logic was demonstrated to be an approach whose results are well-founded. Its principle of assuming that humans make decisions based on non-numerical and imprecise information stands true.

We compare the surveyed methodologies based on their Computation, Domain, and Goal in the following table:

TABLE I. COMPARISON OF SURVEYED METHODOLOGIES

Techniques	**Observations**		
	Computation	***Domain***	***Goal***
F. Nawaz et al. [1]	An algorithm based on QoS criteria & changing user preferences	Markov Chain	List of Cloud Service Rankings
L. Bao [2]	Matrix normalization & Calculation of Global Trust Degree (GTD) based on QoS parameters	Real-Time Global Trust Degree	GTD value
Mahesh K et al. [3]	Reputation-based Trust mechanism, Linear Discriminate Analysis used for clustering and ranking of services	Linear Regression Model	Ranks of services
S. S. Roy et al. [4]	Assesses trustworthiness based on uncertainty value, models trust metrics	Entrusted Trust Management (ETM) System	Filter out unreliable sources and evaluate the trustworthiness
S. M. Habib et al. [5]	User-preference, SLA & CAIQ based trust evaluation	Trust Management (TM) System	Overview of the TM System and how it functions for a cloud marketplace
Kanpariyasoontorn & Senivongse [6]	Maps Standards to parameters & constructs CCM Control Domain Association Matrix with Assurance Weights	Cloud Controls Matrix	Trustworthiness Matrix
Z. Wu et al. [7]	Fuzzy Neural Network to deal with trust elements, normalization & Min. Polyhedron technique	Evaluation and Comparison via Fuzzy Neural Networks	Collection of experimental data from cloud-based services to evaluate trust
Pandey & Daniel [8]	A trust model based on security, maintainability, reliability, and usability	Fuzzy Logic	Framework for a fair evaluation of trustworthiness
Challagidad & Birje [9]	Based on compliance and builds an evaluation matrix	Multi-Dimensional Dynamic Trust Evaluation Scheme	Trustworthiness of services and customers
Wang & Wu [10]	Trustworthiness value and Trust factor processing, Multi-criteria analysis, clustering interaction	Support Factor Clustering, Trust Factor Aggregation, and Minimum Polyhedron Technique	Measure, rank, or sort cloud service candidates
Emeakaroha et al. [11]	Delphi methodology, an average calculation mechanism, and service provisioning	Trust Labels	A Cloud Service Monitoring System based on Trust Labels
Sidhu & Singh [12]	Trustworthiness quotient, establishes trustworthiness of CSP in the environment	Compliance-based Trustworthiness Calculation	Generation of compliance & peer-compliance reports for trustworthiness

Techniques	Observations		
	Computation	***Domain***	***Goal***
Venisha A & M. Murali [13]	An Architecture based on Machine Agent, Feedback Provider, and Trust Validation	Decision Trees	High-accuracy prediction from Decision Trees
Y. Wang et al. [14]	Calculates comprehensive trust,User-preference clustering and Threshold-based clustering	Threshold and User Preference Clustering	Comprehensive trust evaluation
J. Liu et al. [15]	Trustworthiness Fusion Model based on web services, fusion formula is used	D-S Evidence Theory based Fusion Model	Trustworthiness calculated through 'Fusion Process'

IV. CONCLUSION

Although Cloud Service Selection is a field that is rapidly evolving, the latest methodologies have very similar cores in their approaches. Conventionally, AHP was believed to be the primary choice to estimate the trustworthiness of a CSP. Novel solutions met other ways to cogently link trustworthiness and associations between Content Areas. These proposed ways are challenging researchers to fundamentally re-assess and write functional algorithms that cater to the changing priorities and preferences. Inherently, no particular approach stands to build a general solution to bridge the gap of uncertainty in cloud service selection. While merging solutions seems a plausible all-encompassing characteristic, trustworthiness remains ever-open to uncertainty as the bounds of computing try to leash it.

ACKNOWLEDGMENT

We would like to convey our gratitude to Dayananda Sagar College of Engineering, Bengaluru for the extended support. The faculty of the Department of Computer Science & Engineering encouraged us with ample resources and opportunities to make this survey possible.

REFERENCES

[1] Falak Nawaz, Mehdi Rajabi Asadabadi, Naeem Khalid Janjua, Omar Khadeer Hussain, Elizabeth Chang, Morteza Saberi, An MCDM method for cloud service selection using a Markov chain and the best-worst method, Knowledge-Based Systems, Volume 159, 2018, pp. 120-131.

[2] L. Bao, "QoS-based Trust Computing Scheme for SLA Guarantee in Cloud Computing System," 2017 International Conference on Computing Intelligence and Information System (CIIS), Nanjing, 2017, pp. 236-240.

[3] Mahesh K, Dr. M. Laxmaiah, Dr. Yogesh Kumar Sharma, "Predict Trustworthiness of Cloud Services Using Linear Regression Model", IJAST, vol. 29, no. 04, 2020, pp. 5737-5745.

[4] Sudipta Singha Roy, Tamjid Haque Sarker, and M. M. A. Hashem, "A novel trust measurement system for cloud-based marketplace," 2015 2nd International Conference on Electrical Information and Communication Technologies (EICT), Khulna, 2015, pp. 49-54.

[5] S. M. Habib, S. Ries, and M. Muhlhauser, "Towards a Trust Management System for Cloud Computing," 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, Changsha, 2011, pp. 933-939.

[6] J. Kanpariyasoontorn and T. Senivongse, "Cloud service trustworthiness assessment based on cloud controls matrix," 2017 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, 2017, pp. 291-297.

[7] Z. Wu and Y. Zhou, "Customized Cloud Service Trustworthiness Evaluation and Comparison Using Fuzzy Neural Networks," in 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, GA, USA, 2016, pp. 433-442.

[8] S. Pandey and A. K. Daniel, "Fuzzy logic based cloud service trustworthiness model," 2016 IEEE International Conference on Engineering and Technology (ICETECH), Coimbatore, 2016, pp. 73-78.

[9] P. S. Challagidad and M. N. Birje, "Determination of Trustworthiness of Cloud Service Provider and Cloud Customer," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2019, pp. 839-843.

[10] L. Wang and Z. Wu, "A Trustworthiness Evaluation Framework in Cloud Computing for Service Selection," in 2014 IEEE 6th International Conference on Cloud Computing Technology and Science (CloudCom), Singapore, Singapore, 2014, pp. 101-106.

[11] V. C. Emeakaroha, K. Fatema, L. v. d. Werff, P. Healy, T. Lynn, and J. P. Morrison, "A Trust Label System for Communicating Trust in Cloud Services," in IEEE Transactions on Services Computing, vol. 10, no. 5, pp. 689-700.

[12] Jagpreet Sidhu, Sarbjeet Singh, "Compliance based trustworthiness calculation mechanism in cloud environment," in International Workshop on Intelligent Techniques in Distributed Systems (ITDS-2014), pp. 439-446.

[13] Venisha A., M. Murali, "Discovering The Trustworthy Cloud Service Provider In Collaborative Cloud Environment," in International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8, Issue-2S2, 2019.

[14] Y. Wang, J. Wen, W. Zhou, B. Tao, Q. Wu and Z. Tao, "A Cloud Service Selection Method Based on Trust and User Preference Clustering," in IEEE Access, vol. 7, 2019, pp. 110279-110292.

[15] J. Liu, X. Liu, and R. Hu, "A Trustworthiness Fusion Model for Service Cloud Platform Based on D-S Evidence Theory," in Cluster Computing and the Grid, IEEE International Symposium on, Newport Beach, California USA, 2011 pp. 566-571.