International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

Trust Management Techniques, Models and Attacks in Cloud

Mahantesh N. Birje, Vijay L. Hallappanavar

Abstract*: Cloud computing is a technology that promises resilient and flexible computing resources to the growing business. Along with many benefits of Cloud computing, there are various complex problems such as security and privacy of data that exists on Cloud. Trust is one of the key obstacles in the adoption of Cloud by the growing market due to absence of any reliable and efficient trust evaluation mechanism. It is difficult task for Cloud consumers to choose trustworthy provider among various service providers who provide similar type of services. There is a need to have - proper techniques/methods to establish trust; proper trust based models to evaluate the trust; and awareness of various possible attacks to know the robustness of the models. Hence this paper discusses existing state of the art trust management techniques, models and attacks, to help research community interested in designing trust based schemes in Cloud environment.

***Keywords*: Attacks, Cloud, Privacy, Security, Trust Management techniques, Trust models**

I. INTRODUCTION

Cloud computing is gaining a great scope towards IT industries, academics and individual users because of its ease of use, on-demand access to network resources, minimal management effort and reduced cost (Mahantesh N. Birje et.al., 2017). The adoption of this Cloud has high influence on business world with important changes to the IT infrastructure (Akashdeep Bharadwaj et.al,. 2019). The Cloud computing supports many services even with smart phones like back up of contacts or executing complex tasks without burdening the computation. The problem of constrained resources is avoided with the answer provided by Cloud computing by low price for services and guarantee of quality. The services are offered by resource sharing in Cloud computing and this is possible with the conformance by the platform that it is able to handle security threats or attacks which hinder its performance and dependability (Minhaj Ahmad Khan, 2016). Security and Privacy are the major obstacles that hold back the adoption of Cloud computing although there are many benefits of it. For any organization to put data over Cloud environment, data confidentiality, data privacy and trust establishment are the important security parameters (Ayesha Kanwal, 2013).

Uncertainty of data security and losing of control over information are the key points in the decreasing level of trust on Cloud service providers.

Thus there is a need to establish trust on service provider to guarantee security of data and gain conformance regarding Cloud performance and activities. As trust is a subjective and depends on context, it is one of the critical issues in choosing Cloud service provider whom we can trust in Cloud environment. Various trust management techniques need to be considered so that a trust can be established between Cloud entities. It becomes necessary to calculate the trust value of Cloud service provider before sending important business information on Cloud by any company. Various trust models have been designed to evaluate trust, which differ in their own way supporting different characteristics and calculating Cloud services using different parameters and needs. A trust model is a coded execution which depends on theory of trust to give a trust value for the members of the Cloud. Depending on this trust value the interactions with that member are constrained and limited. As a result, to choose and implement a particular trust model that best suits the requirements of an organization is a complex task. The security and Quality of Service requirements differ from one Cloud user to another in Cloud environment because one user wants data integrity and safety given by service provider while the other user requires service with good bandwidth and less delay. But every trust model does not incorporate and provides security, control and Quality of Service features Ayesha Kanwal, 2013), making it tougher to select a particular trust model to use while service provisioning in the Cloud. This paper discusses (1) various techniques to establish trust; (2) trust based models to evaluate the trust; and (3) various possible attacks on the trust models.

Rest of the paper is organized as follows: Section 2 describes the taxonomy and comparative analysis of various trust management techniques. Section 3 discusses the taxonomy and comparison of different trust models. Section 4 describes the taxonomy and comparative analysis of various types of attacks in Cloud. In section 5, the conclusion of the paper is discussed along with few research directions .

II. TRUST MANAGEMENT TECHNIQUES

It is difficult for the Cloud service consumers to identify the reliable service providers whom they can believe and trust that the service providers will not behave maliciously (Jagpreet Sidhu and Sarbjeet Singh, 2014). Hence it is essential to establish a trust between service consumers and providers before any service is obtained or offered.

Manuscript published on November 30, 2019.
* Correspondence Author
Mahantesh N. Birje*, Center for Post Graduate Studies, VTU, Belagavi, Karnataka, India, Email: mnbirje@yahoo.com
Vijay L. Hallappanavar*, ECE department, KLECET, Chikodi, Karnataka, India, Email: vijayhall@gmail.com

This section presents taxonomy of various trust management techniques and compares them.

A. Types of Trust Management techniques

There are different types of trust management techniques to support the consumers in selecting trustworthy Cloud providers. The taxonomy of trust management techniques is as given below in figure 1.

- Traditional methods

(i) Audits

Various audit standards are used by Cloud providers to make users believe about the services and platforms offered by them (Sheikh Mahbub Habib et.al., 2014). For example, Google apps are provided with the Google listed Statement on Auditing Standards 70 II and Federal Information Security Management Act certification to show users the security and privacy solutions. The former includes only the operational performance and depends on more exact set of end results and standards. But these are not enough to boost the user's security concerns and there is no transparency as Cloud service providers are not ready to share their audit reports (Sheikh Mahbub Habib et.al., 2012).

(ii) Measuring & Ratings

To help Cloud users to know the reliable service providers, a webservice known as Cloud marketplace is available (Sheikh Mahbub Habib et.al., 2014). These service providers are given rates through a questionnaire which is filled in by Cloud consumers. The user feedback will be combined with technical data in the future which is aim of Cloud Commons, so that the trustworthiness of providers is computed and compared. SpotCloud is another marketplace which gives opportunity for the Cloud users to select appropriate service provider depending on cost, quality and location. In this web service, the provider's ratings are given as star interface similar to Amazon where the information on rating computation is not available (Sheikh Mahbub Habib et.al., 2012) (Gaurav Raj et.al., 2014).

(iii) Self-Assessment Questionnaires

Consensus Assessment Initiative Questionnaire is the detailed questionnaire given by Cloud Security Alliance to make sure the transparency of Cloud provider's which is security controlled. This technique evaluates the abilities and proficiency of service providers considering different features such as compliance, information security and governance.

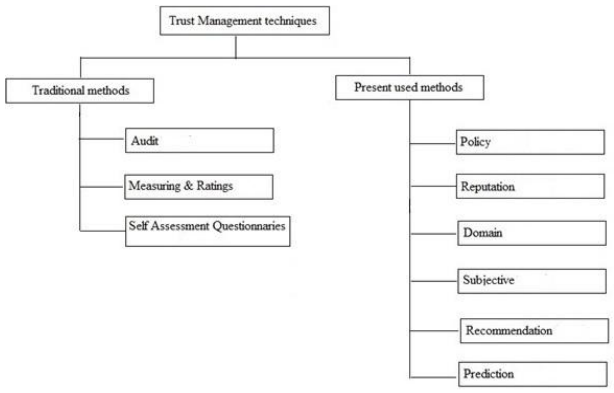

Fig. 1 Taxonomy of trust management techniques

Depending on the answered assessment questionnaire, the potential service provider is identified. But the Cloud security alliance has not made any attempt to prepare a system to compute CAIQ. Also the content present in the STAR database can be verified with Cloud control matrix which gives information of the compliance of service providers with the security standards, audits and control fraeworks of industry (Sheikh Mahbub Habib et.al., 2012) (Gaurav Raj et.al., 2014).

- Present used methods

(i) Policy based trust management technique

By fulfilling SLAs trust can be established on service provider. A service level agreement (SLA) is an agreement between a Cloud user and a Cloud service provider which is legal (Sheikh Mahbub Habib et.al 2014). To know what a service provider is giving and which promises are being kept, SLA validation and monitoring schemes are needed. The Cloud users need to monitor SLA violations in Cloud computing framework and claim providers for compensation. But the clauses of compensation in SLAs are framed by service providers which provide no advantage to the Cloud users. This problem is due to lack of standardized SLAs for the service providers in the Cloud market Sheikh Mahbub Habib et.al., 2012) (Syed Asad Hussain et.al., 2016).

To solve the above problem, Public Key Infrastructure (PKI) concept is used with SLA to support digital signature, key certification and validation, as well as attribute certification and validation. A public key certificate along with binding of public key with subject, it consists of certificate policy extension. In context of public key certificate given to certification authority, it consists of certified public key which is related to specific Cloud service provider. Trust in a CA which includes giving and managing valid public key certificates depends on the conformance of certification authorities with definite certificate policies. This mechanism is known as policy based trust management technique (Huang and Nicol, 2013).

(ii) Reputation based trust management technique

The reputation of a Cloud entity can be defined as the collective belief of all the entities in the Cloud environment towards that entity. As a result in the Cloud environment an entity with high reputation is the one trusted by all the entities. Hence the reputation of a particular entity is used to derive an opinion on that entity by a trustor to compute the trust value. The reputation of a service provider is used to select a Cloud service among various service providers by the Cloud user (Huang and Nicol, 2013). This technique calculates the trust on Cloud services by collecting the feedback and opinions from various service providers. The feedback collected involves information regarding various qualities of service and security parameters given by service providers. The service provider who provides all the needed quality of service and security features to its customers is the most trusted and reliable provider (Ayesha Kanwal, 2013). The reputation based trust management technique is being adopted by Google and Amazon and using this technique it becomes easier for the Cloud users to identify trustworthy service provider to perform online business transactions with confidence and high security (Paul Manuel, 2015).

(iiii) Domain based trust management technique

This technique is used for grid computing but can also be used for Cloud computing.

In this technique the

Cloud environment is divided into several independent domains and classified them into two types - within domain and inter-domain trust relationships. The trust value is obtained from direct and recommended trust tables respectively.

The trust value in within domain involves the transactions between the entities which are in the same domain. The entity calculates the trust value of another entity by checking the direct trust table and if this value is not found then it checks the recommended trust table (Ayesha Kanwal, 2013).

(iv) Subjective based trust management technique

In this technique the trust is divided into different subclasses such as authority trust, code trust, and execution trust in Cloud environment. To allot the values and evaluate the individual subclasses of trust, probabilistic or fuzzy theory algorithms are employed. Probability set theory and fuzzy set theory are the major techniques to calculate the trust information about particular service provider and the offered services (Ayesha Kanwal, 2013).

(v) Recommendation based trust management technique

In this technique the two entities, the trustor and the trustee does not have prior interaction background with each other. In this situation, when the Cloud user has no information about the particular service provider, the trust relationship is established by recommendation of another entity, usually a Cloud auditor (Flavio Corradini et.al., 2015). Cloud users can establish trust in this way by evaluating services (Talal H. Noor et.al., 2011).

(vi) Prediction based trust management technique

The similarity of the capabilities and interests between two providers are the two key factors on which this technique depends. So if the entities have similar features, then there is more chance of trusting each other. Cosine Similarity, one of the similarity measurements is used to calculate this value. To find the trust between each other, a trust threshold is used. This technique is also used to improve the trust feedbacks and is extremely helpful in case of no prior information about the previous interactions of Cloud services (Merrihan B. Monir et.al., 2015).

- Comparison of the trust management techniques

The following table I provides the description of traditional methods of trust management techniques. Table II provides the description of present used methods of trust management techniques.

Table- I: Traditional methods of trust management techniques

Sl. No.	Trust Management technique	Features / Attributes	Intended for	Functions	Drawbacks
i)	Audits	Different audit standards	CSPs	Make users believe about the services and platforms offered by them by different audit standards	includes only the operational performance
ii)	Measuring & Ratings	Service providers are given rates through a questionnaire which is filled in by Cloud consumers	CSPs	for evaluating and comparing the trustworthiness of CPs	information on rating computation is not available
iii)	Self Assessment Questionnaires	means for evaluating the abilities of Cloud service provider	CSPs	detailed questionnaire given to make sure the transparency of Cloud provider's which is security controlled	Absence of system to assess CAIQ

Table-II : Present used methods of trust management techniques

Sl. No.	Trust Management technique	Features / Attributes	Intended for	Functions	Drawbacks
i)	Policy	Uses set of credentials and policies	Systems which need strong protection	Access control decisions	Complexity in issuing and maintaining keys
ii)	Reputation	Uses recommendations and experiences of users	Distributed networks	1.To model and compute trust 2.to retrieve data for trust computation	Malicious users input false data
iii)	Domain	Uses direct and recommendations	Grid computing	To make sure security and interoperability of within and inter domain Cloud	Overhead of implementing trust tables and domain agents
iv)	Subjective	Uses probability or fuzzy logic	Distributed networks	Calculates trust by probabilistic and fuzzy set theory	More complex implementation

v)	Recommendation	Use prior experiences	Distributed networks	To improve security and reliability	no previous interaction background
vi)	Prediction	Uses direct and recommendation trust table	Distributed network	To predict future behavior of a partner	--

III. TRUST MODELS

Trust management is one of the important tools in finding a reliable Cloud entity where lack of prior information about the system would put Cloud users into tricky situations as users do not know each other. While the trust management techniques are highly effective in aiding the Cloud user to select the most trustworthy entity to have interaction with and indirectly avoiding the selection of malicious entity, the trust model help the user to know the trust value of that entity(Felix and Gregoria, 2009) (Eleni and Tsalgatidou, 2012). It serves as a standard for the providers to know the disadvantages and improvement areas of a Cloud service (Rizwana Shaikh and Sasikumar, 2015).

A. Different types of trust models

Providing security in a distributed environment is a critical issue. Traditional security methods cannot always be used in this type of environment where entities can become a participant in the system or opt out, with their wish. As a result trust models help in achieving fix level of security and assurance between entities. The following section discusses the different types of trust models which are classified based on Bayesian network, fuzzy logic, biological and analytical (Mohamed Firdhous et.al., 2011) (Ferry Hendrikx et.al., 2014). The following figure 2 shows the taxonomy of the trust models.

- Bayesian network based trust model

(i) Bayesian Network Based Trust Management (BNBTM)

This model takes multidimensional trust values and using a single Bayesian network individual dimension is computed. Beta probability distribution functions are used to represent the allocation of trust values based on transaction information (Bo Jin et.al 2011) (Audun Jøsang et.al., 2007).

- Fuzzy logic based trust model

(i) Patrol-F (comPrehensive reputAtion-based TRust mOdeL- Fuzzy)

This model works on the theory of fuzzy logic. It uses fuzzy logic to classify the user depending on trust level good or better and bad or worse. It consists of -- direct experiences, reputation values, trustworthiness, loss of information depending on time, first impressions and user reputation calculation by system hierarchy (Supriya M and G K Patra 2012) (Enas F. Rawashdeh t. al., 2018) .

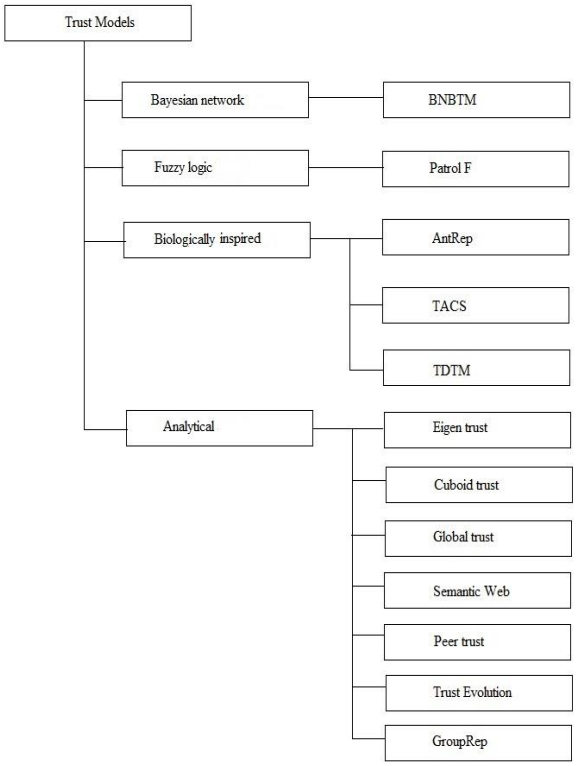

Fig. 2. Taxonomy of the trust models

- Biologically inspired based trust model

(i) AntRep

This model is based on bio inspired swarm intelligence algorithm. A reputation table is maintained by each user which provides reputation of 'x' number of users present in the system. The reputation table consists of reputation of the users and this value is used as criteria for choosing the user. Two kinds of ants, forward and backward ants find the reputation values of the users and to circulate this value in the system. A entity with the highest reputation value from the reputation table is chosen and unicast ant is transmitted to that entity for transaction. And if there are no highest values present in the table then broadcast ants are sent to all the entities. After the transaction is completed, a backward ant is sent to update the reputation values of the all the entities.

(ii) Trust Ant Colony System (TACS)

This model depends on the ant colony system. In this model based on the pheromone traces on the way, the node with high trustworthiness is chosen for requesting service. Each path is linked with pheromone value indicating the trust among the peers. The most trustworthy server is found out by the ants which travel along every path depositing pheromone.

(iii) Time based Dynamic Trust Model (TDTM)

This model is based on ant colony that finds the pheromone, the trust, the heuristic and the distance between two nodes. Depending on the number of interactions, this model computes the trust value. The trust value boosts with more interactions and decreases with less number of interactions.

- Analytical based trust model

(i) EigenTrust

This model deals with file sharing. The model computes the trust in the entity and the trust in the dependability of the resource (Somesh Kumar et.al 2013).

The computation of local trust is represented by the number of file downloading which are satisfactory defined as Sij = sat(i,j) − unsat(i,j), where sat(i,j) represents the file downloads by i from j and unsat(i,j) is the downloads which are not satisfactory.

(ii) CuboidTrust

This model finds the reputation value given by entities trustworthiness with four relations. A cuboid denoted by Px,y,z is formed by having points (x,y,z) where z – quality of resource, y – service requested entity and x – the peer providing feedback of the resource. The rating is binary. Global trust for each peer is computed using power iteration formula (Heba Kurdi et, al., 2018).

(iii) Global trust

This model calculates global trust value of an entity by integrating local trust values instead of focusing on local trust value of an entity.

(iv) Semantic Web

This trust model is used for multi agent system. The trust value of the path that connects the two agents is calculated through addition of the trust of individual edges and later multiplication of corresponding weights associated with each edge is performed.

(v) Peer trust

This model is basically a reputation-based trust model. The trust is calculated using three key factors - interaction number, trustworthiness of the entity and the feedback a entity receives from other entities.

(vi) Trust Evolution

This model involves two types of trust which are direct trust and recommendation from other entities. The trust value is context dependent. And the value of the trust is in the interval [0,1].

(vii) GroupRep

This model indicates the trust among group members. The model consist of 3 levels of trust - trust between groups, trust developed between groups and entities, and only between entities.

B. Strengths and weaknesses of the trust models

After describing various types of trust models, it is necessary to highlight strengths and weaknesses of these models. The below table 3 lists the strengths and weaknesses of the Bayesian network based trust models, table 4 lists the strengths and weaknesses of the Fuzzy logic based trust models, table 5 lists the strengths and weaknesses of the Biology inspired based trust models and table 6 lists the strengths and weaknesses of the Analytical based trust models.

Table – III. Strengths and weaknesses of the bayesian network based trust models

Sl. No	Trust Model	Strength	Weakness
i)	PATROLF	Finds the trustworthiness of a entity perfectly during provision of service and when providing recommendations about other entities	---

Table- IV. Strengths and weaknesses of the fuzzy logic based trust models

Sl.No	Trust Model	Strength	Weakness
i)	BNBTM	Aggregated view of trustworthiness of a entity is got by collecting trust value from various contexts	Handles a interaction with only three discrete calculation

Table - V. Strengths and weaknesses of biologically inspired trust models

Sl.No	Trust Model	Strength	Weakness
i)	ANTRep	This model is able to become accustomed to the changing topologies of various networks without difficulty	This model gives a method to share the reputation evidences but fails to evaluate those evidences
ii)	TACS	This model provides better result for given situations	The model demands every node to have the knowledge of the topology of the system at each situation which is not possible at all times
iii)	TDTM	This model changes to situation correctly to rapid changes in the topology of the network	The model considers the concept of PKI in the system

Table - VI. Strengths and weaknesses of analytical based trust models

Sl.No	Trust Model	Strength	Weakness
i)	Eigen trust	• The model provides better results in calculation of local trust • This model handles collusion and Sybil attack	This model takes into account the pretrusted peers which is not possible at all times as peers cannot be trusted by default before establishing community
ii)	Cubiod trust	• The model provides better results in calculation of trust value • This model handles collusion attack	• The model does not give separate treatment for the direct trust • The model considers discrete values than continuous values in the range [-1, 1]

iii)	Global trust	• The model differentiates among direct and indirect trust • It differentiates among the trust value provided by a peer as a service provider and as a recommender	The model has some scalability issues when trying to find every path which is used to connect two agents
iv)	Semantic web	• The model differentiates among direct and indirect trust • It differentiates among the trust value provided by a peer as a service provider and as a recommender	The model has some scalability issues when trying to find every path which is used to connect two agents
v)	Peer trust	• The model provides better results in calculation of trust value • This model handles collusion attack • The model consists of a context factor to make distinction between the trust of a entity for different transactions	The model fails to make distinction between confidence put on a peer during service provision and when providing recommendations about other entities
vi)	Trust evolution	The model clearly makes distinction between confidence put on a peer during service provision and when providing recommendations about other entities	----
vii)	GroupRep	The model gives the differentiation among trust between groups of peers, between groups and peers, and only between peers	The model fails to calculate the global trust

IV. ATTACKS IN CLOUD

As the server devices are internally connected to the network, there is an attack on the system in the form of delay in communication or failure to reach the network. Attacks on VMs and hypervisors lead to security violation for unlawful reasons. Similarly, Cloud services which include software are prone to hacks and security attacks which break data protection leading to theft of data and service or denial of services for all the peers (Wu Chunming et.al., 2017) (Minhaj Ahmad Khan, 2016).

A. Types of attacks in Cloud

In the Cloud environment, attackers utilize the vulnerable components of the service models - Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) models (Xiaonian Wu et.al., 2013) to conduct attacks. For instance, attacks based on network loopholes could bring about communication latency or connection failure; attacks based on storage loopholes could cause data exposure or destroy; and attacks based on VM, hypervisor and application loopholes are able to compromise Cloud security in many ways. Generally, the Cloud platform mainly includes high efficiency networks, high speed storage devices, high powered servers, and applications (Wu Chunming et.al., 2017). Its weakness depends on the components: network, virtual machines, storage and applications, using which attacks are categorized (Chirag Modi et.al., 2013). The following figure 3 provides the taxonomy of attacks in Cloud.

- Network based attacks

The Cloud devices present in the Cloud environment are linked by a network which also links the devices outside the Cloud environment. An attacker may attack the system through its network which leads to worsen the Cloud services quality and also risking data privacy (Minhaj Ahmad Khan, 2016). The QoS gets worse because along with target server, co-hosted virtual servers, network devices and service providers get affected (Gaurav Somani et.al., 2016). Network based attacks may be classified as below.

(a) Port scanning

A port on a server is checked to know the condition of a service running on the target device. This attack needs permission to enter the network which is connected to the target device. It is done to understand the weakness of the

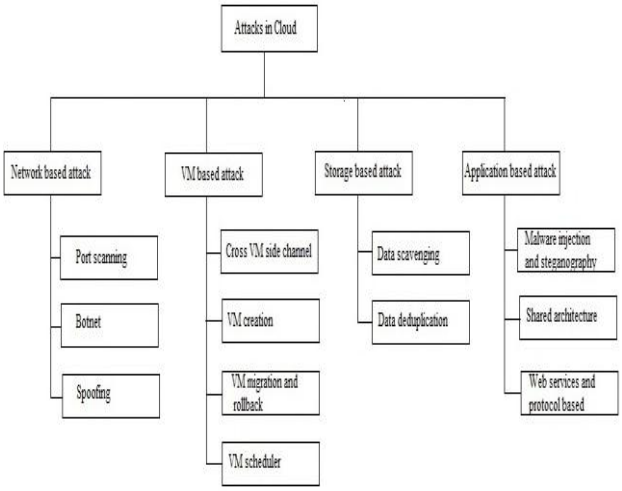

Fig. 3. Taxonomy of the attacks in Cloud

device leading in the denial-of-service (DoS) (Blesson Varghese and Rajumar Buyya, 2018). (Gaurav Somani et.al., 2016) (Mahbub Ahmed and Yang Xiang, 2011).

(b) Botnets

A botnet is used for theft of data from the host device and pass it to a bot-master. A command and control system is set with a bot-master and many machines connected to it steal confidential data. Many examples have shown using Clouds as command and control servers.

(c) Spoofing attacks

Spoofing attack in the system pretends to be the intended user for unlawful works. The IP address of a packet is replaced with fake IP address in an IP spoofing attack. The network traffic can be redirected to a malicious users system using DNS spoofing attack where DNS server is made to return an incorrect IP address. The attacker can access victims virtual machines using ARP spoofing attack which is done on virtual network (Umme Habiba et.al., 2014) (B.Sumitra et.al., 2014).

- Virtual Machine (VM) based attacks

In the Cloud environment, these types of attacks use the loop holes of the virtual machines to break data protection and disturb the Cloud services.

There are many virtual machines installed in the system and these are prone to lot of security risks(Mohammad Equebal Hussain et. al., 2019). Also different levels of virtual machine management may be employed to initiate huge number of Cloud attacks (Hefei Jia et.al., 2019). VM based attacks may be classified as below (Minhaj Ahmad Khan, 2016) (Azeem Sarwar et.al., 2013).

(a) Cross VM side channel attacks

This type of attack takes data related to information on amenity, secret keys and other related data from a victim virtual machine located on the same physical machine where attacker virtual machine is present. The timing related data from the resources such as cache memory may be extracted by these attacks (Umme Habiba et.al., 2014).

(b) VM creation attacks

In the virtual machine image a malicious code can be put so that it gets replicated while generating virtual machines.

(c) VM migration and roll back attacks

During migration of working virtual machine from the host device to another device, the information of the virtual machine files get susceptible to different attacks. Example – the history of execution status kept to use it for rollback may get exploited during migration.

(d) VM scheduler based attacks

The loopholes of scheduler will lead to stealing of data or theft-of-service. Example – A virtual machine is planned to execute later at specified time with keeping the remaining balance of the virtual machine execution time.

- Storage based attacks

The confidential information stored on storage device may be stolen by an external attacker or untrustworthy insider (P. S. Challagidad and M. N. Birje, 2017). As sensitive data is accessible, lot of vulnerabilities can be use to change the data if there is loose monitoring technique. Storage based attacks may be classified as below (Minhaj Ahmad Khan, 2016) (Yuan and Yang, 2011).

(a) Data scavenging

The data does not get completely vanished when erasing data from a storage device. As a result, the vanished data may be recovered by attackers called as data scavenging.

(b) Data deduplication

Storage and bandwidth requirements can be reduced by using data deduplication. But with this technique, the files and their contents get exposed. Also it may lead to communication channel creation for malicious usage.

- Application based attacks

In this type of attack, a code is injected on the applications running in Cloud environment to get information of execution paths which is used for malicious reasons. In the same way, protocols used to give services in the Cloud environment are susceptible to attacks and the applications which are executing may consider them as source of interference. Also the shared architectural components in the Cloud environment may be used by an application to do malicious actions (Minhaj Ahmad Khan, 2016). Application based attacks are classified as below:

(a) Malware injection and steganography attack

In the Cloud environment if an unsafe interface is used for developing application then a malicious code may be introduced into the application. The attackers insert malicious code in the data when sending over the network in a steganography attack. The security systems ignore the sent malicious code considering it as normal file being sent (B.Sumitra et.al., 2014).

(b) Shared architectures attack

The execution path of a user's application can be identified in a shared design. This information may be later utilized to identify the user's activities and capture his account. This attack is also known as Shared technology vulnerability (M.N.Birje et.al., 2015).

(c) Web services & protocol based attack

The data header can be changed to have valid requests in case of several protocols such as SOAP during web services.

B. Comparison of different types of attacks

The following table 7 provides the list of network based attacks where the mechanism, result of attack on the system and the vulnerable component are discussed. Table 8 provides the list of VM based attacks where mechanism, result of attack on the system and the vulnerable component are discussed. Table 9 provides the list of storage based attacks where mechanism, result of attack on the system and the vulnerable component are discussed. Table 10 provides the list of application based attacks where mechanism, result of attack on the system and the vulnerable component are discussed.

Table-VII. Comparative analysis of network based attacks

Sl.No.	Attack type	Mechanism	Result of attack on the system	Vulnerable component
i)	Port scanning attack	Server may be checked to know the condition of the Cloud service	Denial of service	Cloud network
ii)	Botnet attack	command and control servers are set in Cloud environment	Stealing of data from host machine	Cloud network
iii)	Spoofing attack	Change IP address with fake IP address	Change the direction of the network information to an attacker's system. The attacker will be able to get the packet of other virtual machines	Virtual network

Table - VIII. Comparative analysis of virtual machine based attacks

Sl.No.	Attack type	Mechanism	Result of attack on the system	Vulnerable component
i)	Cross VM side channel attack	Loop holes of the virtual machines	Get data of information on amenity, secret keys from a victim virtual machine	Cache memory

ii)	VM creation attack	Unlawful code is put in a virtual machine image	Able to get information	VM image
iii)	VM migration and rollback attack	During migration of information from the host computer to another computer	Information of virtual machine files gets susceptible	Hypervisor and network
iv)	VM scheduler based attack	During VM scheduling	Stealing of data	VM scheduler

Table - IX. Comparative analysis of storage based attacks

Sl.No.	Attack type	Mechanism	Result of attack on the system	Vulnerable component
i)	Data scavenging attack	The vanished information may be retrieved	Extract information	Cloud storage
ii)	Data deduplication attack	During deduplication it is able to know the contents of the files	• Know the files and their content • Makes a communication path for the malicious software	Cloud storage and network

Table - X. Comparative analysis of application based attacks

Sl.No.	Attack type	Mechanism	Result of attack on the system	Vulnerable component
i)	Malware injection and steganography attack	Inserting malicious code in an application and during transmission of data	Service is denied, data is manipulated	Cloud network and storage
ii)	Shared architecture attack	By knowing the execution path of a target application	Identify victim's activities and capture the account	Vulnerable APIs and shared storage

V. CONCLUSION AND RESEARCH DIRECTIONS

Trust management is one of the significant components in Cloud security as Cloud environment consist of different types of Cloud consumers, service providers and intermediary entities. Proper trust management techniques, trust models and awareness of attacks in Cloud will assist the Cloud users to choose the service provider. The paper provides an extensive survey and taxonomy of existing trust management techniques, trust models and attacks in the Cloud. Various trust management techniques exist in the Cloud market which helps the Cloud users in selecting trustworthy service provider. The paper provides the classification of these techniques and gives valuable information of each of these techniques so that customer can select a particular trust management technique depending on his requirements. The paper categorizes the trust models based on the method employed to calculate the trust value which help the users to know the trustworthiness of the Cloud entity and the robustness of the model against security threats that exist in Cloud environment. As Cloud computing is becoming important part of IT market, it is facing security threats. The paper gives extensive analysis of various types of attacks based on the vulnerable components which are prone to attack. This survey paper helps research community to explore more information on trust management and aids in designing trust based schemes for Cloud environment.

The following explanation lists out some of the research directions based on the above survey made.

The first research direction is to device mechanisms for dealing reputation system which encourage users to give feedbacks through secure methods and avoid attacks associated with trust. The second research direction is to develop smart fuzzy system that selects efficient algorithms to calculate trust in different contexts. The third research direction is to provide a cloud user to reflect their perspective in terms of personal preferences in all trust model evaluation processes. There is a need for an effective, reliable and secure trust model that will satisfy the necessary requirements of cloud consumers. The collaboration of cloud service providers benefit the cloud users and also boost the confidence of users. Trust models should function to achieve trust establishment and evaluation in the heterogeneous cloud environment. Trust evaluation based on multiple QoS is still complicated and trust mechanisms should provide methods to handle issues such as integrity and reliability. Real cloud environment has been a challenging factor. Trust models have to be integrated to provide secure environment and this involves mainly mobile trust computation.

REFERENCES

1. Mohammad Equebal Hussain1, Mohammed Qayyum2, Mohammad Rashid Hussain3 and Rashid Hussain4, "Effective and Secure vWSN Applications in a Virtualized Cloud Computing Environment", *International Journal of Communication Networks and Information Security (IJCNIS)*, Vol. 11, No. 2, August 2019, pp 256-261 .
2. Hefei Jia, Xu Liu, Xiaoqiang Di, Hui Qi, Ligang Cong, Jinqing Li and Huamin Yang., "Security Strategy for Virtual Machine Allocation in Cloud Computing", *Procedia Computer Science, Elsevier*, Volume 147, 2019, pp 140–144.
3. Akashdeep Bharadwaj and Sam Goundar, "A framework to define the relationship between cyber security and Cloud performance", *Computer Fraud and Security, Elsevier*, Volume 2019, Issue 2, 2019, pp 12-19.
4. Enas F. Rawashdeh, Inas I . Abukaddam and Amjad A. Hudaib, "Trust Models for services in Cloud Environment: A survey", *IEEE Int. Conf. on Information and Communication Systems*, Irbid, Jordan, 2018, pp 175-180.
5. Heba Kurdi, Bushra Alshayban, Lina Altoaimy and Shada Alsalamah, "TrustyFeer: A Subjective Logic Trust Model for Smart City Peer-to-Peer Federated Clouds", *Wireless Communications and Mobile Computing, Hindawi*, Volume 2, Article ID 1073216, 2018, pp 1-13.
6. Blesson Varghese and Rajumar Buyya, "Next generation cloud computing: New trends and research directions", *Future Generation Computer Systems, Elsevier*, Volume 79, 2018, pp 849-861.
7. Wu Chunming, LIU Qianjun, LI Yuwei, CHENG Qiumei, and ZHOU Haifeng , "A Survey on Cloud Security", *ZTE Communications*, Vol.15, 2017, pp. 42-47.
8. Mahantesh N. Birje, Praveen S. Challagidad, R. H. Goudar and Manisha T. Tapale, "Cloud computing review: concepts, technology, challenges and security", *Int. J. Cloud Computing*, Vol. 6, No. 1, 2017, pp. 32 – 57.

9. P. S. Challagidad and M. N. Birje, "Hierarchical Attribute-based Access Control with Delegation approach in Cloud", *International Conference on Computing for Sustainable Global Development, INDIACom-2017, IEEE Conference*, 2017, pp. 978-982, 2017..
10. Syed Asad Hussain Mehwish Fatima, Atif Saeed, Imran Raza and Raja Khurram Shahzad, "Multilevel classification of security concerns in Cloud computing", *J. of Applied Computing and Informatics, Elsevier*, Volume 13, Issue 1, 2017, pp 57-65.
11. Gaurav Somani, ManojSingh Gaur, Dheeraj Sanghi and Mauro Conti, "DDoS attacks in Cloud computing: Collateral damage to non-targets", *J. of Computer Networks, Elsevier* , Vol. 000, 2016, pp. 1-15.
12. Minhaj Ahmad Khan, "A survey of security issues for Cloud computing", *J. of Network and Computer Applications, Elsevier*, 2016, pp. 11-29.
13. Paul Manuel, "A trust model of Cloud computing based on Quality of Service", *Annals of Operations Research, Springer*, Volume 233, Issue 1, 2015, pp 281–292.
14. Flavio Corradini, Fausto Marcantoni and Fabrizio Ippoliti, "A Survey of Trust Management Models for Cloud Computing", *CLOSER 2015 - 5th Int. Conf. on Cloud Computing and Services Science*, 2015, pp. 155-162.
15. M. N. Birje, Praveen S. Challagidad, R. H. Goudar and Manisha T. Tapale, "Security Issues and Countermeasures in Cloud Computing", *Int. J. of Applied Engineering Research, Research India Publications*, ISSN 0973-4562 Vol. 10 No.86, 2015, pp. 71 – 75.
16. Rizwana Shaikh and Sasikumar, "Trust Model for Measuring Security Strength of Cloud Computing Service", *Int. Conf. on Advanced Computing Technologies and Applications (ICACTA), Elsevier*, Vol. 45, 2015, pp. 380-389.
17. Merrihan B. Monir, Mohammed H. AbdelAzi, AbdelAziz A.AbdelHamid and El-Sayed M. EI-Horbaty, "Trust Management in Cloud Computing: A Survey", *Seventh Int. Conf. on Intelligent Computing and Information Systems, IEEE*, 2015, pp. 231-242.
18. Ferry Hendrikx, Kris Bubendorfe and Ryan Chard, "Reputation systems: A survey and taxonomy", *J. of Parallel and Distributed Computing, Elsevier*, Vol. 75, 2014, pp. 184-197.
19. 19. Umme Habiba, Rahat Masood, Muhammad Awais Shibli and Muaz A Niazi, "Cloud identity management security issues & solutions: a taxonomy", *J. of Complex Adaptive Systems Modeling, Springer*, 2014, pp. 1-37.
20. Jagpreet Sidhu and Sarbjeet Singh, "Compliance based trustworthiness calculation mechanism in Cloud environment", *J. of Procedia Computer Science, Elsevier*, Vol. 37, 2014, pp. 439-446.
21. Gaurav Raj, Mohammed Sarfaraz and Dr. Dheerendra Singh, "Survey on Trust Establishment in Cloud Computing", *Int. Conf. - Confluence The Next Generation Information Technology Summit (Confluence), IEEE*, 2014, pp. 215-220.
22. B.Sumitra, C.R. Pethuru and M.Misbahuddin, "A Survey of Cloud Authentication Attacks and Solution Approaches", *Int. J. of Innovative Research in Computer and Communication Engineering*, Vol. 2, 2014, Issue 10, pp. 6245-6253.
23. Sheikh Mahbub Habib, Sebastian Ries, Max Muhlhauser and Prabhu Varikkattu, "Towards a Trust Management System for Cloud Computing Marketplaces: using CAIQ as a trust information source", *J. of Security and Comm. Networks, John Wiley & Sons Ltd.*, Volume 7, Issue 11, 2014, pp. 2185–2200.
24. Ayesha Kanwal, Rahat Masood, Um E Ghazia, Muhammad Awais Shibli and Abdul Ghafoor Abbasi " Assessment Criteria for Trust Models in Cloud Computing", *IEEE Int. Conf. on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, IEEE*, 2013, pp 254-261.
25. Azeem Sarwar and Muhammad Naeem Ahmed Khan, "A Review of Trust Aspects in Cloud Computing Security", *Int. J. of Cloud Computing and Services Science (IJ-CLOSER)*, Vol.2, No.2, 2013, pp.116-122.
26. Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Avi Patel and Muttukrishnan Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing", *J. of Supercomput, Springer*, Vol. 63, 2013, pp. 561–592.
27. Huang and Nicol, "Trust mechanisms for Cloud computing", *J. of Cloud Computing: Advances, Systems and Applications, Springer*, 2013, pp. 1-14.
28. Somesh Kumar, Suvamoy Changder and Anirban Sarkar , "Trust management model for Cloud computing environment", *ICTACT, J. on Soft Computing*, Vol. 3, Issue 3, 2013, pp. 509-513.
29. Xiaonian Wu, Runlian Zhang, Bing Zeng and Shengyuan Zhou, "Trust evaluation model for Cloud computing", *Int. Conf. on Information Technology and Quantitative Management", Procedia Computer Science, Elsevier*, Vol. 17, 2013, pp. 1170-1177.
30. Supriya M and G K Patra, "Estimating Trust Value for Cloud Service Providers using Fuzzy Logic", *Int. J. of Computer Applications*, Volume 48, 2012, pp. 28-34.
31. Eleni and Tsalgatidou, "Taxonomy of attacks and defense mechanisms in P2P reputation systems", *J. of Computer Science review, Elsevier*, Vol. 6, 2012, pp. 47-70.
32. Sheikh Mahbub Habib, Sascha Hauke, Sebastian Ries and Max Muhlhauser, "Trust as a facilitator in Cloud computing: a survey", *J. of Cloud Computing: Advances, Systems and Applications, Springer*, 2012, pp. 1-18.
33. Bo Jin, Yong Wang, Zhenyan Liu and Jingfeng Xue, "A Trust Model Based on Cloud Model and Bayesian Networks", *J. of Procedia Environmental Sciences 11, Elsevier*, 2011, pp. 452 – 459.
34. Mahbub Ahmed and Yang Xiang, "Trust Ticket Deployment: A Notion of a Data Owner's Trust in Cloud Computing", *Int. Joint Conf. of IEEE TrustCom-11/IEEE ICESS-11/FCST-11, IEEE*, 2011, pp. 111-117.
35. Mohamed Firdhous, Osman Ghazali and Suhaidi Hassa, "Trust Management in Cloud Computing: A Critical Review", *Int. J. on Advances in ICT for Emerging Regions*, Vol. 4, 2011, pp. 24-36.
36. Talal H. Noor and and Quan Z. Sheng, "Trust as a Service: A Framework for Trust Management in Cloud Environments", *WISE, Springer*, 2011, pp. 314–321.
37. Yuan and Yang, "A survey of identity management technology", *IEEE Int. Conf. on Information Theory, and Information Security (ICITIS), IEEE*, 2010, pp. 287-293.
38. Felix Gomez Marmol and Gregorio Martınez Perez, "Security threats scenarios in trust and reputation models for distributed systems", *J. of Computer and Security, Elsevier*, Vol. 28, 2009, pp. 545-556.
39. Audun Jøsang, Roslan Ismail and Colin Boyd "A Survey of Trust and Reputation Systems for Online Service Provision", *J. of Decision Support Systems, Elsevier*, 2007 pp. 618-644.

AUTHORS PROFILE

Dr. Mahantesh N Birje, working as Professor,Master of Computer Application Centre for Post Graduate Studies, VTU, Belagavi, Karnataka, India. His research areas are Distributed computing, Grid computing and Fog computing.

Prof. Vijay L Hallappanavar, working as Assistant Professor, KLE College of Engineering and Technology, Chikodi, Karnataka, India. His is pursuing part time PhD at research centre, VTU, Belagavi. His area of interest are cloud computing, fog computing and trust establishment in cloud and fog computing