Analysis of trust issues in Cloud Technologies

Yagub Sardarov, Orkhan Aghayev

Abstract

This article examines the concept of trust in cloud technologies, which is considered one of the most critical issues in cloud security. To address this, the study explores various disciplines that have studied the concept of trust, sheds light on approaches to ensuring the transparency of clouds and investigates "trust as a service" solutions. The issues found in these trust mechanisms are identified, and recommendations for their resolution are provided.

Keywords: trust, cloud technologies, service level agreement, sybil attacks, reputation-based trust.

One of the factors that have had a significant impact on the development of information technologies is the creation of cloud technologies. Cloud technologies have provided conditions for easy access to resources from remote locations and have facilitated the use of a user-friendly interface. When using cloud technologies, the user's computer plays the role of a connected terminal, and all data is stored on servers called "clouds." the customer receives a large virtual server, and these servers can be physically located far from each other or even in different continents. The main advantages of this technology are the ability to work independently with cloud services and the absence of restrictions on location or time. However, ensuring the security of these technologies is not an easy task. Cloud technologies offer dynamic, collaborative, and agile resources to users via the internet, which are located in information centers outside of the user's organization's infrastructure. However, the extreme lack of transparency and the distributed nature of these technologies pose significant barriers to their success in the market. One of the main issues with cloud technologies is the problem of trust. Numerous approaches to establishing trust have been recommended for the cloud environment. However, the existing approaches rely on cloud providers presenting information relevant to evaluating their trustworthiness to centralized centers. Some cloud providers may alter or filter information before presenting it, thereby casting doubt on the accuracy of the information used

to make trust decisions. This article presents an analysis of reputation-based trust and the methods for ensuring transparency in cloud approaches, along with the investigation of "trust as a service" services. To properly assess a provider's trustworthiness, it is recommended that all trust indicators be checked by third-party professional organizations automatically.

The concept of trust is widely studied by various disciplines such as social psychology, economics, and marketing. While the topic of trust has been extensively researched, there is currently no standard definition of trust. Different sources provide varying definitions of trust. For example, according to y. Wang and j. Vassileva, trust is "the confidence that a subject has in the reliability of another subject based on their own perceptions." this is a sociological definition of trust. However, in the context of cloud technologies, the term trust is often used in reference to information security and privacy.

When cloud technologies emerged in 2007, users had a low level of trust in this technology. According to an analytical report based on a survey of over 3,000 cloud customers in six countries conducted by fujitsu scientific research institute in 2010, 88% of customers did not trust cloud services because they were unsure who would have access to their personal information, and 84% were uncomfortable with where their personal information would be stored. Nevertheless, the adoption of cloud technologies has recently shown a sharp increase. In fact, the revenue generated by the cloud market is predicted to increase from $77 billion in 2010 to $210 billion in 2016, according to the analytical organization gartner. Note that 41.3% of this revenue will be earned through the provision of "Infrastructure As A Service". In addition, by the end of 2016, 50% of the world's 1000 largest organizations planned to store their sensitive customer data in public cloud infrastructures. On the other hand, market research media ltd has estimated the revenue of the cloud market at $270 billion between 2015 and 2020 using a compound annual growth rate (cagr) calculator, which calculates the growth rate of investments over time. Currently, there are numerous trust mechanisms created to determine the reliability of cloud providers. Below is a brief summary of their main categories. Ensuring transparency in clouds is one of the most important issues in determining the reliability of clouds. No cloud is completely transparent, meaning that it is not possible to see the technologies or processes used in the cloud. Transparency is considered a key factor in assessing the credibility of cloud providers. Without transparency, building trust is not possible. Addressing transparency and accountability issues in cloud technologies has always been a focus of international organizations. To determine the transparency of clouds, the cloud security alliance (csa), a leading organization in this field, prepared the security, trust & assurance registry (star) program at the end of 2011. The registry of the cloud security alliance (csa) is available for free on the organization's website. This registry is based on mechanisms for self-evaluation of providers' security levels and consists of two documents:

Consensus assessments initiative questionnaire (caiq): The cloud provider will fill out in response to a series of questions regarding compliance with security requirements this electronic spreadsheet.

Cloud controls matrix (ccm): this is a document consisting of general principles that determine the cloud provider's security level. It assesses the degree to which the cloud provider meets the requirements of csa's 13-part security guidance.

According to information provided by the csa, more than 30 advanced cloud providers have prepared their own star documents to determine their level of transparency. These providers include google, microsoft, verizon and intel among others.

One of the mechanisms that serves the establishment of trust is the cloud trust protocol (ctp), proposed by the computer sciences corporation (csc) in 2009. The protocol is based on a query- response mechanism. Users can send queries to the provider to obtain specific information about transparency elements. These transparency elements include cloud infrastructure configuration, gaps, audit accounts, service management mechanisms, and others. The csa has taken on the responsibility of realizing the protocol in the cloud environment and has added it to its grc (governance, risk management and compliance) document collection in 2011. The purpose of the protocol is to create conditions for users to obtain information about events occurring in the cloud infrastructure. By enabling users to monitor events occurring within the cloud, ctp acts as a mediator between cloud users and providers.

In summary, the csa provides mechanisms such as the caiq and ccm for cloud providers to evaluate and demonstrate their compliance with security requirements, while the ctp protocol allows users to obtain detailed information about the transparency elements of the cloud infrastructure. These mechanisms aim to establish trust between cloud providers and users by providing greater transparency and accountability.

One of the approaches to establishing trust in cloud technologies is the service level agreement (SLA). A SLA is a contract between a service provider and a client that guarantees the quality of service (qos) claimed by the provider and creates conditions for the application of legal penalties in the event of a breach of the contract terms. The SLA comprises multiple indicators, including efficiency (uninterrupted operation time and downtime duration), response time, agility, and other parameters or restrictions.

Service providers (sps) are obliged to adhere to these indicators when providing services. Violations of any of these indicators can result in penalties for the sp, as well as negative feedback from the client. Currently, most large organizations that provide cloud services attempt to provide services that comply with the sla. For example, the sla level for services provided by 3tera, a cloud service provider, is "five nines," meaning that 3tera services provide 99.999% of the requirements specified in the sla. If the level of service falls below 99.999%, compensation is paid to the client. Amazon, on the other hand, declares a 99.95% sla level for its elastic compute cloud (ec2) service, and also compensates clients if the sla level falls below the specified percentage. However, in order to receive compensation, users must provide documented evidence of service interruptions that reflect the downtimes.

Generally, trust models based on the SLA focused on monitoring the indicators promised in the contract. Examples of such monitoring systems include wisla, traverse, and it SLA monitoring systems.

Trust as a service (taas) is a mechanism for determining the level of trust in cloud systems. It involves the provision of trusted third-party services on a query basis, independent of the security service provider. One such mechanism is the cloud trust authority (cta), proposed by emc's rsa division in 2011. The cta serves as a centralized function for managing the security of various service providers. It manages identification, ensuring a unified entry between different cloud providers.

Moreover, this mechanism allows external users to track the security profile of the service provider according to a defined standard, by adhering to normative documents. The rsa philosophy for developing trust is based on the synthesis of transparency and management mechanisms, and typically defines trust as "trust = transparency + management."

Reputation-based trust.

Currently, there is a significant focus on issues related to reputation-based trust in cloud computing. Similar to the concept of trust, the notion of reputation has been extensively researched in various academic disciplines, but a standardized definition has yet to be established. Multiple sources have provided different interpretations of the concept of reputation. For example, one source

defines reputation as the trust one subject has in another subject's abilities, reliability, and integrity based on recommendations received from other subjects. Reputation systems, on the other hand, utilize the ratings provided by individual members of a community regarding a specific object (such as service providers, services, or subjects) to calculate reputation scores for that object.

The concepts of trust and reputation are applicable in various fields, but they are closely related to each other. Both concepts are used to evaluate the degree of reliability of a subject. However, what differentiates them is that trust is a relationship established between two subjects, whereas a subject's reputation is the general opinion of the community towards that subject.

Generally, a subject who has gained trust from a large number of participants in the community will possess a high reputation. In the cloud environment, a subject who wants to make a decision based on trust regarding another subject will evaluate the trust level of the subject based on its reputation. Besides reputation systems, it is also possible to encounter the term "recommendation systems" in various sources. The difference between these systems lies in the fact that reputation systems are based solely on the opinions of participating members within a community, while recommendation systems also take into account opinions provided from outside.

Well-known reputation systems include truster and trustedsource. Currently, many websites such as slashdot, reddit, digg, ebay, etc. Utilize reputation systems. In various e-commerce sites, buyers and sellers evaluate each other after each transaction.

Reputation systems, such as those utilized by online marketplaces like ebay, calculate and display the trustworthiness of a seller or buyer. These reputation systems are widely used for internet security purposes, with trustedsource being one of the most well-known systems. Trustedsource was created by ciphertrust and is currently owned by mcafee. It calculates reputation scores for internet identities such as ip addresses, domains, email content, and web content through the use of data mining and other analytical methods. Internet reputation systems are useful tools in preventing network attacks through email, web, and other protocols.

Reputation systems are also utilized in other areas, such as peer-to-peer systems for identifying trustworthy peers, social news for determining the best news, and web search systems for pagerank. However, reputation systems are weak against certain types of attacks. Enisa has identified 15 attack types that are relevant to reputation systems, with sybil attacks being the most relevant for cloud infrastructure. Sybil attacks are sometimes referred to as pseudospoofing, where a large number of fake identities (sybils) are created to manipulate the subject's reputation score. Reputation systems are important tools for internet security and are used in a variety of applications. However, they are vulnerable to certain types of attacks, such as sybil attacks, which can be used to manipulate reputation scores through the creation of fake identities. The term "sybil" was first used in 1973 by english journalist flora schreiber in her book "sybil." the book discusses the life of shirley ardell mason, a patient in a psychiatric clinic. The name "sybil isabel dorsett" was used to protect mason's anonymity. Due to the nature of the plot, sybil suffers from dissociative identity disorder, which is characterized by the formation of several different personalities in one person's body. After interviews with psychologists, it became apparent that 16 different people were present in dorsett's body. At times, she introduced herself to society under the names of these individuals. John r. Douceur was the first to refer to the detection of multiple identities in information systems as the "sybil attack."considering the importance of information in the modern era, security and trust issues in cloud technologies hinder the widespread adoption of this technology. Otherwise, crucial information may be compromised.

Conclusion

The mechanism by which cloud providers present the necessary information to relevant authorities to assess the trustworthiness of their service is critical in evaluating conflicting reports. However, it is highly likely that some cloud providers may present filtered or altered information, which raises doubts about the accuracy of the decision-making process. Therefore, the automated verification of trust indicators in the cloud environment by third-party professional organizations can facilitate the accurate evaluation of the provider's trust level. This can create opportunities for broad application of cloud technologies. On the other hand, the creation of reputation systems that are constantly under attack by sybil attacks can provide a foundation for the extensive implementation of cloud technologies.

References

[1] Habib S.M., Hauke S., Ries S., Muhlh M. Trust As A Facilitator In Cloud Computing: A Survey // Journal Of Cloud Computing: Advances, Systems And Applications, 2012, Vol. 1, No 19, 33 P.

[2] Alguliev R.M., Abdullayeva F.C. Identity Management Based Security Architecture Of Cloud Computing On Multi-Agent Systems / Proc. Of The Third International Conference On Innovative Computing Technology (INTECH), 2013, Pp. 123–126.

[3] Əliquliyev R.M., Abdullayeva F.C. Bulud Texnologiyalarının Təhlükəsizlik Problemlərinin Tədqiqi Və Analizi // İnformasiya Texnologiyaları Problemləri, 2013, №1, S. 3–14.

[4] Rashidi A., Movahhedinia N. A Model For User Trust In Cloud Computing // International Journal On Cloud Computing: Services And Architecture (IJCCSA), 2012, Vol. 2, No. 2, Pp. 1–8.

[5] Huang J., Nicol D.M. Trust Mechanisms For Cloud Computing // Journal Of Cloud Computing: Advances, Systems And Applications, 2013, Vol. 2, No 9, 14 P.

[6] Heijden V.H., Verhagen T., Creemers M., Creemers M. Understanding Online Purchase Intentions: Contributions From Technology And Trust Perspectives // European Journal Of Information Systems, 2003, Vol. 12, No 1, Pp. 41–48.

[7] Castelfranchi C., Falcone R. Principles Of Trust For MAS: Cognitive Anatomy Social Importance, And Quantication / Proc. Of The IEEE Third International Conference On Multiagent Systems, 1998, Pp. 72–79.

[8] Gambetta D. Can We Trust Trust? Trust: Making And Breaking Cooperative Relations, Basil Blackwell, Oxford, 1990, Chapter 13, Pp. 213–237.

[9] Montaner M., Lopez B., Rosa J.L. Opinion-Based Filtering Through Trust / Proc. Of The 6th International Workshop On Cooperative Information Agents VI, 2002, Pp. 164–178.

[10] Jøsang A., Ismail R., Boyd C. A Survey Of Trust And Reputation Systems For Online Service Provision // Journal Of Decision Support Systems, Vol. 43, No 2, Pp.618–644