IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

A Comprehensive study on Trustworthy Computing

Gulista Khan, Associate Professor,
College of Computing Sciences and Information Technology, Teerthanker Mahaveer University,
Moradabad, Uttar Pradesh, India
Email Id- gulista.khan@gmail.com

ABSTRACT: ***Developing effective commercial connections and determining the acceptance of new technologies both depend on trust. To yet, however, trust in the context of cloud computing has gotten little attention, which has led to a lack of knowledge of the dimensions of trust in cloud services and trust-building antecedents. Although there are a number of conceptual models of trust in the literature for contexts related to cloud computing that may be used as a guide, especially trust in IT outsourcing providers and trust in IT artifacts, the peculiarities of trust in cloud computing necessitate a novel conceptual model of trust. A cloud service is both an IT artifact and a service offered by a business, to start. In this paper, the Microsoft-adopted Trustworthy Computing Security Development Lifecycle also known as the SDL is discussed. This approach is used to create software that can survive hostile attacks. The procedure entails adding a number of security-focused tasks and outputs to each stage of Microsoft's software development cycle***.

KEYWORDS: Computing, Cloud Services, Cloud Computing, Security, Trustworthy.

1. INTRODUCTION

The explosion in connectivity between computers and other devices has also raised serious concerns about cyber security since all devices, whether online or offline, are vulnerable to attack and compromise. This worry is what drew together several of the major players in the computer industry, including AMD, HP, IBM, Intel, and Microsoft in 2007 to form the non-profit organization known as that of the Trusted Computing Group. If all of the capabilities are used, trusted computing with a TPM gives a considerable improvement in platform security. It provides protection against software-based assaults from malicious programs, Trojan horses, viruses, and root kits and, upon request, provides platform configuration data. Its power is in its capacity to evaluate platform components in a manner that prevents programs running with knowledge of the fundamental foundation of trust behind the system's numerous measures from circumventing it. The four pillars of Trustworthy Computing are shown in Figure 1 [1]–[3].

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

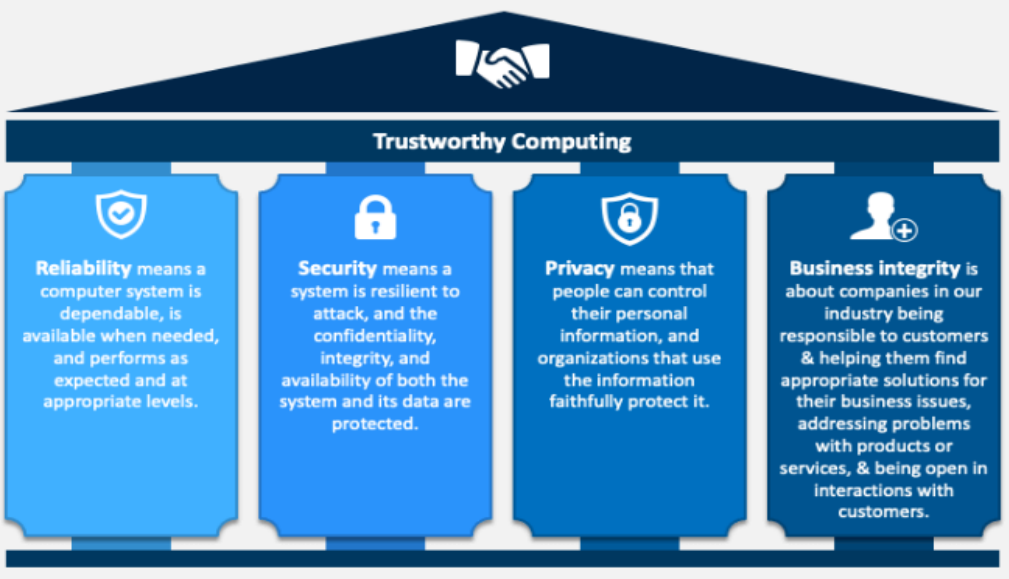

Figure 1: Illustrate the four pillar of the Trustworthy Computing.

A hardware-based "root of trust" on computing platforms is supported by the Trusted Computing Group (TCG), which was established to define, develop, and promote open, vendor-neutral, quality standards that would facilitate improved trustworthiness in information systems. According to the TCG, a component is a root of trust if it "must perform as anticipated since disobedience cannot be discovered." The construction of an integrated circuit that complies with TCG requirements, including those for data portability and backward compatibility, privacy protection, and backward compatibility, became the group's main focus. In light of how quickly the world is changing, trusted computing has become both required and logical. It is also closely related to the growing quantity and variety of security risks. Keeping encryption technology up to date is an ongoing effort since threats are always evolving. Another difficulty has been addressing the criticisms of the balance of security and privacy in trusted computing on a consistent basis.

These problems serve as the foundation for ongoing research and development by organizations that focus on computer technology. Implementing repeatable procedures that consistently provide demonstrably enhanced security is essential for the software sector to fulfill the current demand for it. As a result, software suppliers must adopt a stricter software development methodology that places a larger emphasis on security. Such a procedure aims to reduce the quantity of security flaws that are present in the design, code, and documentation as well as to identify and fix such flaws as early in the development lifecycle as is practical. The requirement for such a procedure is highest for corporate and consumer software that will probably be used to handle inputs from the Internet, manage vulnerable systems, or handle personally identifiable data. Figure 2 depicts the stages that are taken in a reliable process [4]–[6].

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

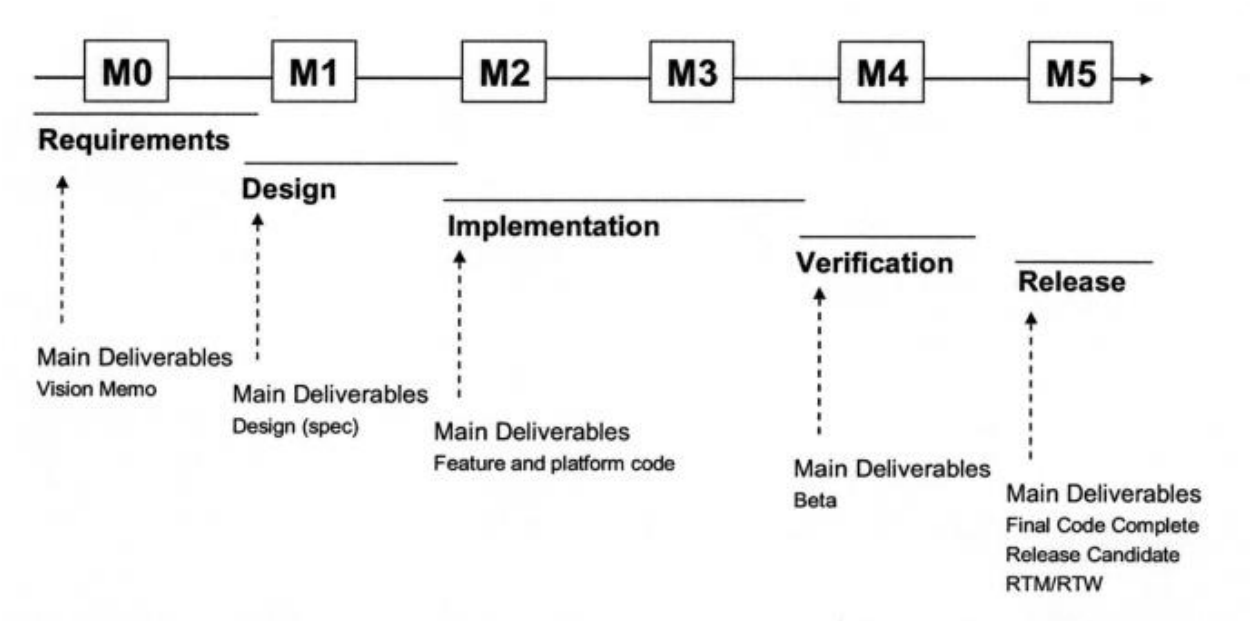

Figure 2: Illustrate the steps which is followed in the trustworthy process.

The underlying assumption behind these problems is that people's faith in computers, online services, and information systems depends on both security and privacy in equal measure. It is the idea that computers and other computing equipment ought to perform as users would expect them to, independent of environmental disturbance, user or operator mistake, or hostile force assault. Even though they don't usually seem like computers, they may be found in our phones, houses, appliances, medical equipment, and even military gear. Additionally, the prevalence is rising. It is a given that consumers would prefer a computer that was completely tied by code to their bank account, for example, particularly in the era of cloud computing. The only scenario where they wouldn't be able to access their money in that instance is if their laptop or PC went lost.

Our military is one of the testing grounds for trusted computing since September 11, 2001, and the complex types of terrorism we have seen. We also need improved confidence for our soldiers who battle abroad. Because designing and manufacturing embedded computing systems for military use are pioneers in the area and whose technology reflects the most recent hardware and software breakthroughs, keeping information secure that is essential to our national security is a must. Microsoft provided figures showing that since the Trusted Computing Group was founded in 2007 and since then, 300 million PCs have been supplied with TPMs. We all get more from the TPM solution as more users share infrastructure, networks, storage, and information. Everyone should be able to engage with a more secure network and benefit from the increased security and privacy guarantees provided by TPM computing.

Whether a trusted system booted the machine, whether it is still operating on the computer, that whether functioning system has been authorized for the program, or whether the system has connection to trusted network services are some of the issues pertinent to a discussion of trusted computing. The only method to demonstrate that a computer system has not been altered or

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

modified is to gather proof. Each of the aforementioned questions may be addressed after the proof has been acquired and confidence has been built. A baseline has to be created in order to do this. The determination of trust is transformed into an assessment of the evidence by comparing a baseline measurement to the measurement collected each time the computer is turned on.

Although the party being trusted lacks control over the other party, which might lead to the trusted party acting opportunistically, trust is crucial in commercial settings that include risk and a reliance on one another. The cloud computing environment makes these need for trust clear. Even though cloud services are based on standardized contracts, not all potential situations are included in the contingencies. In reality, cloud service solutions are designed to be flexible, adaptable, and ever-changing. The same justification also applies to customers' worries about cloud service providers abusing legal gaps. Customers must ultimately feel that suppliers are acting in their best interests. Customers cannot duplicate some characteristics of cloud services, such as quick and (nearly) limitless flexibility. Customers thus rely on outside offered services to varying degrees, depending on how much they utilize cloud services. Users of cloud services may also keep private corporate data on a third-party cloud. Although technological security measures should secure data, there is no assurance that information security won't be compromised. Users must have faith that their cloud provider will properly implement security measures and maintain confidentiality. Given the significance of trust in cloud environments, a thorough understanding of its fundamental aspects and the elements that foster trust is necessary [7]–[11].

2. DISCUSSION

Each and every software provider must handle security risks. Software providers must adhere to strict security standards because of business pressures, the necessity to safeguard vital infrastructures, and the need to maintain public confidence in computers. Making software more safe with fewer patch updates and less onerous security management is a key problem for all software companies. Implementing repeatable procedures that consistently provide demonstrably enhanced security is essential for the software sector to fulfill the current demand for it. As a result, software suppliers must adopt a stricter software development methodology that places a larger emphasis on security. Such a procedure aims to reduce the quantity of security flaws that are present in the design, code, and documentation as well as to identify and fix such flaws as early in the development lifecycle as is practical. The requirement for such a procedure is highest for corporate and consumer software that will probably be used to handle inputs from the Internet, manage vulnerable systems, or handle personally identifiable data. Building better secure software involves three aspects: a repeatable process, engineer education, and metrics and accountability.

While discussing engineer education and providing some broad metrics that demonstrate the effect to date of deployment of a portion of the SDL, this article concentrates on the repeatable process part of the SDL. The adoption of the SDL by other firms shouldn't increase software development expenses excessively, if Microsoft's experience is any indication. According to Microsoft, the advantages of offering more secure software (such as fewer fixes and happier customers) outweigh the disadvantages. In order to increase software security, a software development organization’s procedure must be modified as part of the SDL. The measurements are outlined in this paper along with an explanation of how they fit into a normal software development lifecycle. The goal of

ISSN PRINT 2319 1775 Online 2320 7876
Research paper © 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

these adjustments is to provide clearly defined security checkpoints and security deliverables rather than completely revamp the process. This document makes the assumption that there is a central team within the business (or software development organization) that oversees the creation and advancement of security best practices and procedure enhancements, acts as a resource of knowledge for the entire organization, and conducts an evaluation (the Final Security Review, or FSR), prior to the release of software.

According to Microsoft's experience, the establishment of such a group is essential for both the SDL's implementation and for enhancing software security. While some businesses may think about hiring a contractor or consultant to serve as their "central security team," The approach described in this article, which is frequently used by big software development firms, explains the incorporation of a series of actions meant to enhance software security. As part of its Trustworthy Computing Initiative, Microsoft has created and put these measures into place. Reducing the number and severity of security vulnerabilities in customer-facing software is the aim of these process enhancements. The Trustworthy Computing Software Development Lifecycle is the name given to the enhanced software development method that Microsoft is now using (or simply the SDL). According to Microsoft's experience, the security team has to be accessible for regular contacts throughout the software development process and needs to be trusted with confidential technical and commercial information. For these reasons, creating a security team inside the software development organization is the preferable course of action although it may be appropriate to engage consultants to help build and train the members of the team.

3. CONCLUSION

The use of the cloud presents not only technological and financial difficulties, but also issues with trust. Our paper develops and outlines a conceptual typology comprising five trust components and a framework of four trust antecedents, building on the extensive body of trust literature. We summarize studies on trust in IT outsourcing and confidence in a particular IT artifact using the resultant conceptual model, and we also propose potential areas for future study. The main claims of this article are that, in addition to institution-based trust, experiment on data security in cloud services should also take into account trust in service platform and the cloud ecosystem. This is because trust in cloud services can be divided into two categories: trust in the cloud service provider and believe in the cloud service IT artifact. Trust in cloud services is also significantly influenced by opinions of cloud service provider, cloud service, platform provider, and platform service. This essay aims to be the first step in a thorough investigation of the many dimensions of cloud computing trust. Although it hasn't garnered much attention in the literature so far, the function of trust in cloud computing offers exciting possibilities for future study. We expect that by providing a useful conceptual framework, our conceptual model will motivate other academics to investigate cloud computing trust.

REFERENCES:

[1] L. Hively, F. Sheldon, and A. C. Squicciarini, “Toward scalable trustworthy computing using the human-physiology-immunity metaphor,” *IEEE Secur. Priv.*, 2011, doi: 10.1109/MSP.2010.142.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

[2] C. Huang, L. He, X. Liao, H. Dai, and M. Ji, "Developing a trustworthy computing framework for clouds," *Int. J. Embed. Syst.*, 2016, doi: 10.1504/IJES.2016.073753.

[3] L. M. Hively, F. T. Sheldon, a Squicciarini, and O. Ridge, "A Vision for Scalable Trustworthy Computing," *Ieee Secur. Priv.*, 2010.

[4] T. Holz and D. Hutchison, *Trust and Trustworthy Computing*. 2014.

[5] T. Peters, "A Survey of Trustworthy Computing on Mobile & Wearable Systems," *Tech. Rep. TR2017-823, Dartmouth Comput. Sci.*, 2017.

[6] "Call for Papers - IEEE Transactions on Reliability Special Section on Trustworthy Computing," *IEEE Trans. Reliab.*, 2013, doi: 10.1109/tr.2013.2249011.

[7] N. Asokan *et al.*, "Mobile trusted computing," *Proc. IEEE*, 2014, doi: 10.1109/JPROC.2014.2332007.

[8] M. A. Bouazzouni, E. Conchon, and F. Peyrard, "Trusted mobile computing: An overview of existing solutions," *Futur. Gener. Comput. Syst.*, 2018, doi: 10.1016/j.future.2016.05.033.

[9] S. Nepal, J. Zic, D. Liu, and J. Jang, "A mobile and portable trusted computing platform," *Eurasip J. Wirel. Commun. Netw.*, 2011, doi: 10.1186/1687-1499-2011-75.

[10] E. Gallery and C. J. Mitchell, "Trusted computing: Security and applications," *Cryptologia*, 2009, doi: 10.1080/01611190802231140.

[11] J. Wang *et al.*, "Survey on key technology development and application in trusted computing," *China Commun.*, 2016, doi: 10.1109/CC.2016.7781720.