Trust and its Influence on Technology

Krishna Kambhampaty, Maryam A Maryam Alruwaythi, Kendall E. Nygard
Computer Science Department
North Dakota State University
Fargo, ND 58102
{k.kambhampaty, maryam.alruwayti, kendall.nygard}@ndsu.edu

Md Minhaz Chowdhury
East Stroudsburg University
mchowdhur1@esu.edu

Abstract

Trust is a central component in human interaction. In the area of computer science, the word 'trust' is a widely used term. The definition of trust differs among researchers and application areas. Trust is one of the most influencing factors when it comes to human interaction. Without trust, the survival is difficult for families, houses, politics, friendships, relationships, markets etc. Trust can be considered as social glue that enables us to interact with one another. Humans cope with uncertainty using the trust mechanism.

Human trust with machines and Artificial Intelligence might not be that much different from trusting humans. In the AI context, there might be some reasons as to why trust has become popular. Lives saved in the military as a result, of robots replacing humans in a highly risky situations or autonomous driving vehicles etc. Trust plays a key role in the adoption of technology and the products. It continues its impact on businesses and economic behavior such as digital assistants like Amazon Alexa, Google assistant etc. Our paper talks about trust and its relationship with technology. We also suggest ways to improve trust towards technology. Finally, we conclude that trust can be built with machines and technology just as with humans.

1. Introduction

Trust is defined as [1] 'confidence in or reliance on some quality or attribute of a person or thing, or the truth in a statement'. Trust management was introduced by Blaze. M in 1996. This was first implemented in cloud computing environment as a way of solving security problems. The word 'trust' is a complex and an abstract word. It is hard to pin point what comprises of trust as it is multi-dimensional and multi-faceted. Trust is often built upon past or historical experiences of an individual.

Recent study has described trust as fundamental construct for understanding users perception of technology. Initial trust formation is essential in overcoming the perceptions of risk and uncertainty before using a novel technology.

There are three levels of trust [2]. *Inductive trust, Social trust* and *Moral trust*. *Inductive trust* is derived from the person's past experiences. A person trusts something or someone as they have acted as expected. Inductive trust is the simplest of the trusts and is easy to formalize. The second kind of trust is *Social trust*. This trust is dependent on the encounter between machines and humans. Machines have their own of set of goals just as humans. To trust or not depends on the reasoning of humans. The third kind of trust is *Moral trust*. This trust is based on sense of what is morally right. This kind of trust is hard to interpret and is the least explored area with in AI.

2. Relationship of Trust with Technology

Trust factors can also be utilized to improve the cyber security. Both the public and private sectors fall prey of cyber-attacks. Cybercrimes have costed the world nearly $3 trillion in 2015. This figure is expected to raise to $6 trillion by 2021 [3]. The cyber-crimes range from damage to data, loss of productivity etc. [4].

Security measures to tighten the cyber incidents only overwhelm the users. One of the studies from [5], there is a resistance from users in changing passwords. A survey comprised of 571 respondents from various walks of in life in the campus. Some were undergraduate students, graduate students, staff, researchers, faculty and administrators at Virginia Tech. When the passwords were required to be changed, only a portion of the individuals changed the password. In addition, the resistance to change password, changed from 'rather not resistant' to 'strongly resistant'. Researchers of the study found that the even when the passwords were changed, it was perceived as unnecessary interruptions and were intentionally delayed. Study also found that password breach can attribute to security risks, it did not affect their attitude.

Raking up cyber security measures requires actions at many levels, starting from the design of the technology till its implementation and maintenance. Behavioral science can address the cyber security issues. [6] suggested that security systems need an understanding of behavioral science. This prevents users from being the weakest link. Shari et al have done a survey on how behavioral science can impact the cyber security [7]. They describe that incorporating behavioral science into cyber security can yield to effective security system. They have focused their survey on two aspects: cognitive load and bias. Their survey suggests that including human behavior can lead to potential improvements in the cyber security system.

3. Trust in Information Technology

Trust is emerging as a central aspect in the acceptance of Information Technology. The importance of trust in IT is more important than ever. IT has become center of our lives. We rely so much on the IT. For instance, an online reservation system, communication, hospital management, online shopping etc. all rely on IT. The trust in IT is not very different with the trust in people [8]. Trusting in humans means is belief in a person's capability to fulfill a task or a responsibility. Trusting in Information Technology means, it is understood as the system is functionally capable to complete a task to be done. Differences come in the aspects of integrity, morality. These are harder to be described in IT. There are several advantages of trusting in IT.

Trust in IT influences the adoption or change to new technology and secondly it may affect risks, beliefs and attitudes to using a technology. Trust in digital environment is called as ‘e-trust’.

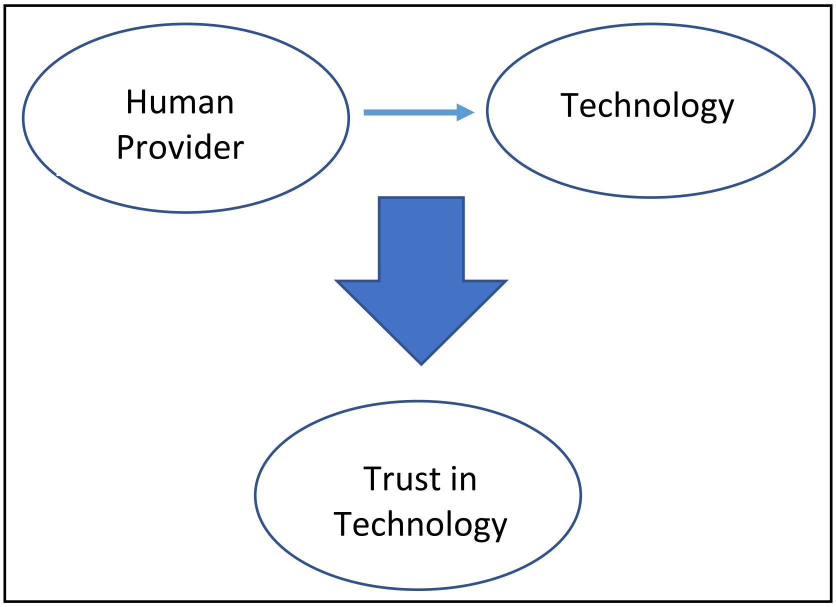

Figure 1: Trust in Technology

4. Trust in the Cloud Computing Environment

Cloud computing provisions shared computing resources. Resources like storage space, servers etc. This is widely used in several industries such as healthcare, banking and education [9]. However, general public still do not have complete confidence and trust in the cloud computing. This is a might not seem as much of a problem at a first glance. This problem can manifest into multiple folds. Industries are gradually getting more reliant on the cloud services for cost effective measures.

Cloud computing provides different types of services, such as Infrastructure as a Service (IaaS), Software as a Service (SaaS), Platform as a Service (PaaS) etc. Cloud Service Providers (CSP) offer these resources to users. The CSP’s infrastructure is more powerful than the personal computing platforms. Though is true, cloud computing environment constantly faces security challenges. Some of them are Amazon S3 unavailability (https://status.aws.amazon.com/s3-20080720.html), iPad breach of personal data (https://techcrunch.com/2010/06/15/ipad-breach-personal-data/), President Obama’s Twitter hack etc.

With the users not trusting the cloud, might affect the industries. This could also affect the cloud service provider industry. This user concern might have emerged from either misconceptions or lack of understanding of the technology. This misunderstanding on the cloud could have negative effects on the trusting the cloud. It might also be due to the security concerns of the data. If the understanding is that data is stored on a third party's hard disk , users would be worried about the encryption of the data or that someone can access the personal or confidential files [10]. In addition, the thought of relying on the cloud for data retrieval might seem like a problem to many. This could arise due the unreliable internet connection one might face. When users see the value for their money, the perception towards cloud computing might drastically improve. In addition, users have serious concerns over security and privacy of cloud computing.

5. Trust in Artificial Intelligence (AI) and Machine Learning

Artificial Intelligence has become ubiquitous in our lives. It is a common site among online shoppers to notice 'recommendations' from the website. Some of the online shopping sites such as Amazon, Google, Walmart have employed techniques like AI and Machine Learning to better understand the user requirements and entice them with the available products. Airline ticketing sites, ride sharing services like Uber, personal digital assistants like Siri, Alexa, Google have relied on AI and Machine Learning technology to improve on the quality of service.

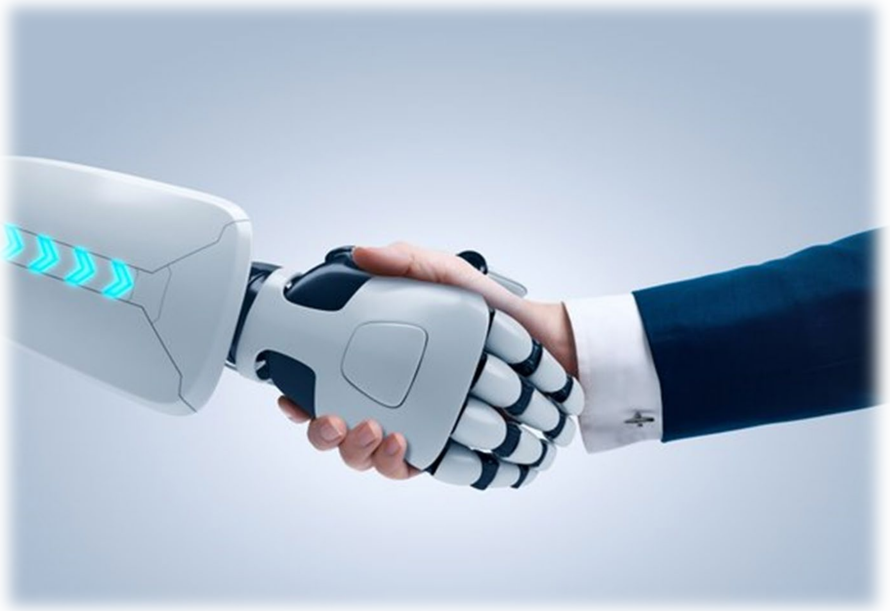

Figure 2: Trust and Technology go hand in hand
Source: Getty Images

AI is a software dominant technology and hence is prone to vulnerabilities. With this fact in hand, how much should the users be trusting on the outcomes generated by AI? [11]. Autonomous cars are equipped with auto-pilot capabilities. This system can adhere to the rules of the road. One of the Tesla car has reportedly saved the driver during his regular commute. The driver upon realizing he had myocardial infarction, changed the destination to the nearest hospital. The autonomous car has efficiently maneuvered in the traffic and has safely brought the driver to the hospital. Upon arrival, driver was rescued by the hospital personnel. This scenario builds trust in autonomous vehicles and more specially in AI. However, in another scenario, a driver was killed in an autonomous car. Evidence suggests that the visual and radar systems have encountered a glitch, as a result, causing the death of the driver. In this scenario AI based system turned deadly.

John Launchbury, director of DARPA's Information Innovation Office, credits statistical learning as a second wave of Artificial Intelligence. This kind of learning has strong suite of learning but lacks in the ability to reason. The outcomes are sometimes skewed. This stresses on the testing of machine learning to ensure the code running behind is flawless. John Launchbury suggests that the AI still needs to be perfected [11].

6. Build and Improve Trust

So, the question that remains is, how do we replicate the human to human trust to human to machines. Peter et al suggests that Explainable AI can play a key role in establishing an initial trust on machines. This could also repair the trust relationships. When a machine such as an autonomous vehicle is providing explanation of its actions, humans can slowly gain trust as it reduces the perception of risk. This is key especially in the early stages of building trust. An explainable trust can also repair the broken trust. If an explanation is provided as to what caused the system to fail the expectations of its user, can also repair the trust.

The relation between explanation and trust [12] has been analysed by Wolter Pieters. This analysis was accomplished using system theory and actor-network theory. Pieters made a clear distinction between trust and confidence. Confidence can be high, but the trust could be low. For instance, when the government announces that voting machines are secure, it builds confidence but might gain trust from people. There is also a distinction between explanation in Information Security versus explanation in AI. Pieters findings confirm that the explanation and trust especially e-trust are critical in the digital environment.

The next question that arises is how this explanation needs to be given. An explanation that could be understood by humans is required. As an example, people request for an explanation of decisions made by others. A series of verbal or pictorial explanation can easily make one understand. Machines need to closely follow this style of explanation.

7. Conclusion

In this paper we have discussed the importance of trust in technology. Trust can play a key role in addressing the cyber-security concerns. Making improvements to the software right from design to development is one of improving security. However, if an element, behavior is added as well, it can very well improve the overall security of cyber systems.

Trust influences the adoption of newer technology. We suggest that an explanation of actions by the systems in an understandable way can help build or improve trust. As a result, adoption newer technology would seem less risky. This can benefit the business and overall economy improvement.

References

[1] S. Furman, "Building Trust," 6 Nov 2018. [Online]. Available: https://www.usability.gov/get-involved/blog/2009/09/building-trust.html.

[2] L. E. G. T. A. H. R. L. K. M. P. C. P. J. P. S. T. P. Peter Andras, "Trusting Intelligent Machines," IEEE Technology and Society, pp. 76-83, 2018.

[3] P. Paganini, "Cost of cybercrime will grow from $3 trillion (2015) to $6 trillion by 2021Security Affairs," [Online]. Available: http://securityaffairs.co/wordpress/50680/cyber-crime/global-cost-of-cybercrime.html.

[4] M. M. C. K. K. a. P. K. Kendall E. Nygard, "Cybersecurity Materials for K-12 Education," Midwest Instruction and Computing Symposium, 2018.

[5] Pamplin, "When Users Resist: How to change management and user resistance to password security," March 2019. [Online]. Available: https://www.magazine.pamplin.vt.edu/fall11/passwordsecurity.html.

[6] M. A. a. I. F. Sasse, "Usable Security: Why Do We Need It? How Do We Get It?," Security and Usability, pp. 13-30, 2005.

[7] D. D. C. Shari Lawrence Pfleeger, "Leveraging Behavioral Science to Mitigate Cyber Security Risk".

[8] H. M. Knight, "Trust in Information Technology," pp. 329-331, 2005.

[9] K. K. K. E. N. Maryam Alruwaythi, "User Behavior Trust Modeling in Cloud Security," IEEE Computational Science and Engineering, 2019.

[10] F. Landman, "ReadWrite," 03 April 2019. [Online]. Available: Why the Public Still Doesn’t Fully Trust Cloud Computing.

[11] G. Hurlburt, "How Much to Trust Artificial Intelligence," IEEE Computer Society, 2017.

[12] W. Pieters, "Explanation and trust: what to tell the user in security and AI?," Springer, pp. 53-64, 2010.