

# Examining Organizational Culture Values and Acceptance of Biometric Identity Authentication Systems

*Emergent Research Forum (ERF) Paper*

**Babita Gupta**

California State University Monterey Bay  
bgupta@csumb.edu

**Subhasish Dasgupta**

George Washington University  
dasgupta@gwu.edu

**Mini Purushothaman**

IT Services Consultant  
mbhushans@hotmail.com

## Abstract

Identity authentication systems such as biometrics can enable organizations to implement identity authentication and security with greater reliability and accountability. Adoption of these systems is a complex and costly endeavor and susceptible to failure when not aligned to the organization's culture. We examine this adoption behavior utilizing the Unified Theory of Acceptance and Use of Technology (UTAUT) that provides a unified view of user acceptance. In this research, we investigate how espoused organizational culture values influence users' acceptance and use of biometrics technology by considering cultural values as antecedents to the UTAUT model. We conducted an empirical study on the acceptance of a biometric identity authentication system and found that espoused organizational culture values have a significant effect on the UTAUT variables. Facilitating conditions, social influence, and anxiety affect the use of biometric identity authentication systems. Our research contributes to the literature on espoused organizational culture, biometrics, and technology acceptance.

## Keywords

Identity authentication systems, Biometrics, Organization culture, UTAUT, PLS analysis.

## Introduction

Security of physical, financial, and information assets is emerging as a critical issue for organizations. Lapses in security such as unauthorized personnel gaining access to critical infrastructure can have serious consequences that extend beyond the organization. Organizations need to have an absolute belief in the identity of employees, customers, contractors and partners they interact with, that they are really who they say they are.

Authenticating legitimate identity in organizations generally involve using systems that rely on what a legitimate user knows (for example, passwords) or what a legitimate user possesses (for example, ID cards or keys). Identity authentication systems such as biometrics can be used to secure facilities, workstations, cellular phones, smart cards, online transactions, and communication networks. Market research estimates that by 2022 over 3.3 billion users will be benefiting from biometric authentication (Market researchers forecast, 2017) with the biometrics market size expected to be about USD 32 billion by 2022 (marketsandmarkets.com, 2016). While technological advances in the field of biometrics and its rapid commercialization are enabling its adoption among wide array of applications, organizations have been slow to adopt biometrics technology for authentication and identity management and have relied mostly on non-biometrics systems such as user ID, passwords, smartcards for authentication (Goode, 2016). However, these systems are susceptible to fraud and security threats as these do not identify the person but simply identify the information that is provided by that person. Identity authentication systems such as biometrics technology offer a solution to these vulnerabilities and provides a level of confidence needed for dependence on information systems and its legitimate users in an organization. Current work on biometrics acceptance focuses on individuals without the organizational context (Carpenter, McLeod, Hicks, &

Maasberg, 2018; Miltgen, Popovič, & Oliveira, 2013; Ngugi, Kamis, & Tremaine, 2011). Based on the literature review, we did not find any study that focused on understanding the role of organization culture that can catalyze the adoption of identity authentication systems such as biometrics in organizations.

In the following sections we present the summary of literature review in biometrics, UTAUT and organizational culture values. Then we propose our research model and hypothesis and methodology followed by the results. We then discuss the results, our contribution, and future research.

## **Literature Review**

### ***Identity Authentication System: Biometrics***

Biometrics refers to the automatic identification and verification (authentication) of a living person based on her unique physiological or behavioral distinguishing, measurable traits offering the promise of greater security to organizations (Gupta, 2008; Rigelsford, 2003). Advancements in biometrics sensors and matching algorithms have led to the deployment of biometrics authentication in large number of civilian applications such as ATMs, grocery stores, airport kiosks, and driver's licenses to prevent unauthorized access (Jain and Ross, 2004). It has been widely used in applications ranging from managing time attendance of field workers in agriculture fields to forensics applications by FBI for criminal identification. Biometrics technology is used in e-commerce and e-banking with applications in hospitality industry including hotels (Ko and Yu, 2015), smartphones (Meng, Wong, and Kwok, 2014), and in education industry with e-learners identity management applications (Levy, Ramim, Furnell, and Clarke, 2011). In automobiles, biometrics can replace keys for providing secure key-less entry and key-less ignition. Due to increased security threats, many countries have started using biometrics for border control and national ID cards (Jain and Ross, 2004; Jain and Kumar, 2010; Ross, Prabhakar and Jain, 2005), registered traveler biometric systems such as the Global Entry system by Transportation Security Administration (TSA) in the U.S. (Morosan, 2013), in banking industry (Usman and Shah, 2013), and for facilitating and monitoring of labor participation in job-search and training activities (Robalino and Weber, 2013). Various types of biometrics technologies and their applications use fingerprint, hand geometry, iris, retina, face, voice, gait, and signature (Agnvall, 2007; Chandra and Calderon, 2003; Freschi, 2007; Hope-Tindall, 2004; Kleist, 2007) and can be in used in organization for authorizing legitimate users access to secure facilities, for managing time attendance, and for verifying users in financial transactions to reduce fraud (Gupta, 2008).

### ***Organizational Culture***

While there is no consensus on one single definition of culture, it refers to totality of values, thought characteristics, socially transmitted behavior, and beliefs of individuals within a unit such as a nation, organization, profession, or team (Ein-Dor, Segev, & Orgad, 1993). Organizational culture refers to common values and beliefs and a pattern of shared set of basic assumptions that individuals within an organization learned as it adapted to external and internal integration (Punnett & Ricks, 1990; Schein, 1985). There are many studies in the information systems literature that examine the role of national culture (Choe, 2004; Couger, 1986; Ein-Dor et al., 1993; Hoehle, Zhang, & Venkatesh, 2015; Kappos & Rivard, 2008; Srite & Karahanna, 2006; Straub, Keil, & Brenner, 1997) but very few that consider the role of organizational culture on the adoption of information systems. Warkentin, Charles-Pauvers, & Chau (2015) pointed out the significance of considering cultural values at the individual level in the adoption and use of IS such as biometrics in organizations. Culture influences values of all individuals in the organization and these are manifested through the degree to which an individual embraces the values of her organizational culture, called *espoused cultural values* (Srite and Karahanna, 2006). These are the espoused cultural values that we focus on in this study. Denison and Mishra (1995) provided measures of organizational culture values emphasizing cultural traits and espoused values associated with effectiveness using four dimensions of organizational culture values embraced by individuals in the organization: adaptability, involvement, mission, and consistency. We describe these in research model section.

### ***The Unified Theory for the Acceptance and Use of Technology (UTAUT)***

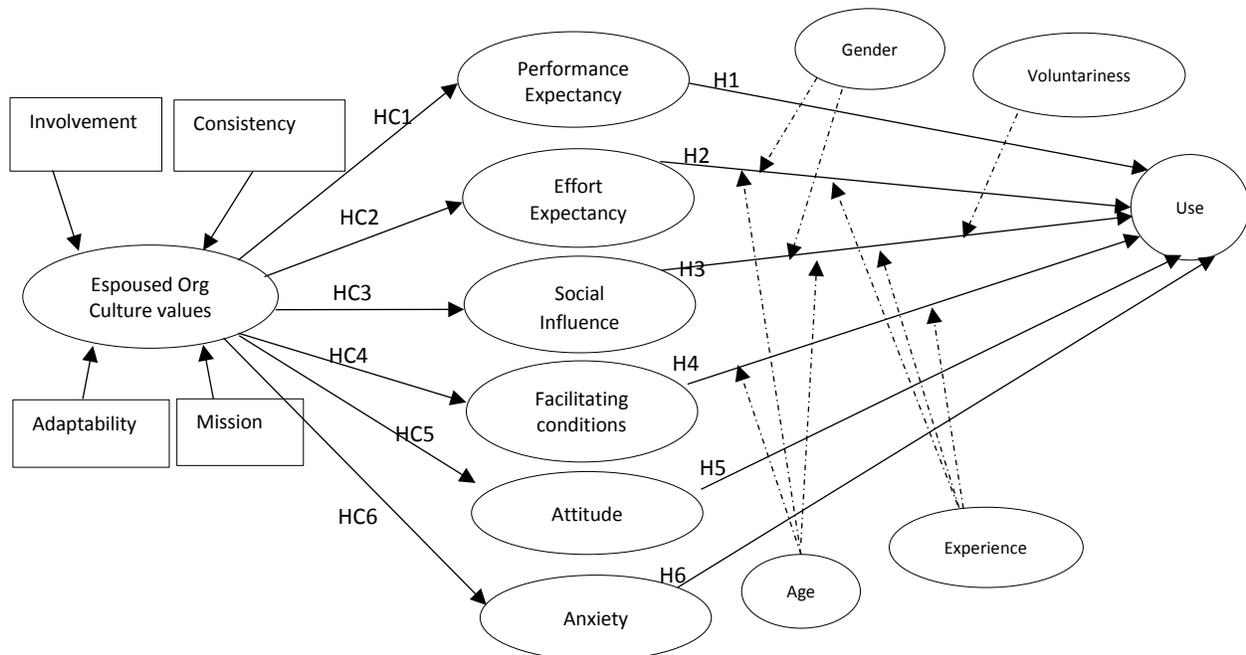
After using the Technology Acceptance Model (TAM) to examine individual use, information technology researchers proposed a few variations and extensions of the model (Petter, Straub, & Rai, 2007; Venkatesh, 2000; Venkatesh & Davis, 2000). These variations as well as some of the earlier models such as the Theory of Reasoned Action and Theory of Planned Behavior were then integrated into a single model called UTAUT (Venkatesh et al., 2003). The UTAUT model has been replicated and validated in different technological

contexts such as the use of mobile devices and services (Carlsson, Carlsson, Hyvonen, Puhakainen, & Walden, 2006; Ho, Hung, & Chen, 2013), information kiosks (Wang & Shih, 2009), biometrics privacy concerns (Carpenter et al., 2018; Miltgen et al., 2013; Ngugi et al., 2011), and community weblogs (Li & Kishore, 2006). Researchers have expanded or enhanced UTAUT by identifying factors that serve as antecedents to the model. Antecedents include personality traits (Wang & Yang, 2005), charismatic leadership (Neufeld, Dong, & Higgins, 2007), and local and cultural environments (Chiu & Hofer, 2015), to name a few. While studies have examined the roles of several organizational and individual factors, so far only one study has considered the role of organizational culture on information technology adoption (Dasgupta and Gupta, 2019). Venkatesh et al. (2016) recommended the study of organizational factors such as organization culture as an area of future research in UTAUT. We therefore use UTAUT for adoption of biometrics system in an organization for identity management with organizational culture values as an antecedent to UTAUT. We use four traits as second order constructs for organizational culture (described later in the following section). This study fills the gap in literature in the area of organizational culture and identity authentication system adoption in organizations.

### Research Model and Hypotheses

In this section we present the model for biometrics system acceptance using UTAUT (Venkatesh et al., 2003) with organizational culture values as an antecedent (Figure 1). The UTAUT identified various factors that influence use of information technology: performance expectancy, effort expectancy, and attitude toward using technology, social influence, facilitating conditions, attitude towards technology, and anxiety. Performance expectancy is the degree to which an individual believes that using biometrics will help her to attain gains in job performance; effort expectancy is the degree of ease associated with the use of biometric system; social influence is the degree to which an individual perceives that important others believe she should use the new system; facilitating conditions refer to the degree to which an individual believes that an organizational and technical infrastructure exists to support use of biometrics; attitude is the individual’s positive or negative feelings about performing the desired behavior, in this case, use of biometrics; anxiety is evoking anxious or emotional reactions when it comes to using biometric system.

**Figure 1: Research Model for the Espoused Organizational Culture and the UTAUT Model**



We modified the model to examine actual use, and not the intention to use since the technology was already implemented in the organization. Denison and Mishra (1995) operationalized organization culture traits as: *involvement* is the extent of participation, *consistency* is the implicit control system based on the internal values of organization, *adaptability* is the capacity for internal change in response to external

conditions, and *mission* provides purpose, meaning, and long-term vision. Recent study suggests that adoption of internet technology is influenced by espoused organization culture (Dasgupta and Gupta, 2019). We therefore propose that espoused organizational culture values of involvement, consistency, adaptability and mission will impact the UTAUT variables, such as, performance expectancy, effort expectancy, social influence, facilitating conditions, attitude and anxiety. The hypotheses are stated below and identified in Figure 1.

**HC1-HC6:** Espoused organizational cultural values influence performance expectancy, effort expectancy, social influence, facilitating conditions, attitude and anxiety.

(Sub-hypotheses for HC above are not listed due to space limitations)

**H1:** Performance expectancy will influence biometric system use.

**H2:** The influence of effort expectancy on use will be moderated by gender, age, and experience.

**H3:** The influence of social influence on use will be moderated by gender, age, experience and voluntariness.

**H4:** The influence of facilitating conditions on use will be moderated by age and experience.

**H5:** Attitude will influence biometric system use.

**H6:** Anxiety towards biometrics will influence biometric system use.

## Sample and Data Collection

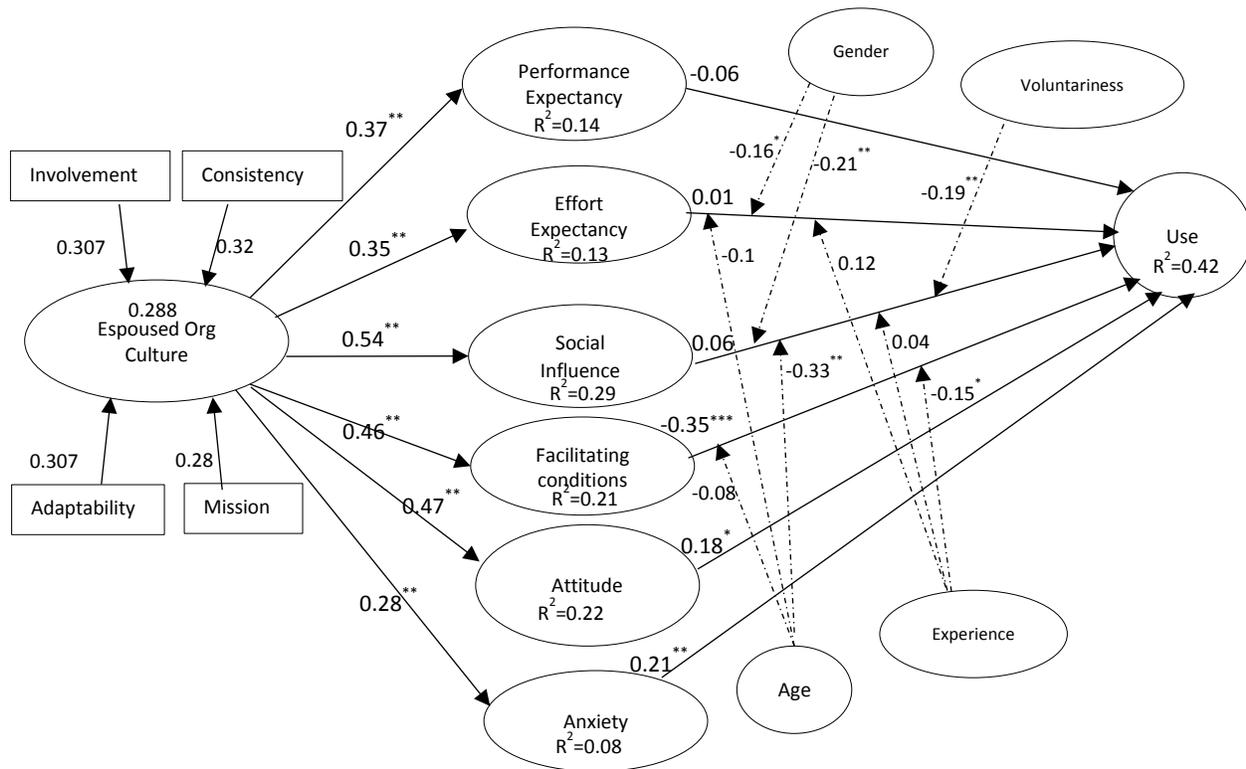
Data for this study was collected from a large public university which implemented iris scanners, a biometric authentication system for identity authentication of faculty, staff, and students to secure access to their labs. In their study of espoused cultural values and their effect on Internet technology adoption Dasgupta and Gupta (2019) used a questionnaire to collect data. We adapted this questionnaire for our study. We first removed items that were not relevant to our study and modified others to reflect the use of biometric authentication systems. We conducted a pilot study of eight users of a biometric authentication system in another organization. We then refined the questionnaire based on comments received from pilot study participants.

Our sample consisted of 150 people who used the organization's biometric identity authentication system. We randomly selected the employees and administered our survey instrument. We received 72 complete responses. Exactly 50 percent of the respondents were 26 to 35 years old, 28 percent were over 35 years old, and 22 percent were 18 to 25 years old. The sample consisted of 17 percent female and 83 percent male users of the biometric identity authentication system.

## Results

We ran a Partial Least Squares (PLS) regression analysis to test our hypotheses. Our model had espoused organizational culture variables as antecedents of the UTAUT model as shown in Figure 1. For the UTAUT, biometric identity authentication system use (or Use) was the dependent variable, and all the independent variables proposed in the UTAUT model: performance expectancy, effort expectancy, facilitating conditions, social influence, attitude, and anxiety. Some of these relationships were moderated by gender, voluntariness, experience, and age (Figure 1).

The results of PLS regression analysis show that the overall model is significant (see Figure 2). Hypotheses HC1 to HC6 which examined the influence of espoused organizational culture variables on performance expectancy, effort expectancy, social influence, facilitating conditions, attitude, and anxiety were found to be significant. In the UTAUT, we found support for hypotheses H4, H5, and H6 which suggest that facilitating conditions, attitude, and anxiety have a significant effect on biometric identity authentication system use. Figure 2 shows the results of PLS analysis. The impact of facilitating conditions on use is moderated by experience (Hypothesis H4). Attitude influences biometric identity authentication system use (Hypothesis H5), and anxiety also has a significant effect on use (Hypothesis H6). We did not find support for Hypotheses H1, H2 and H3. Our results show that performance expectancy, effort expectancy, and social influence do not have a significant impact on use of the biometrics system.

**Figure 2: PLS Regression Results**

\*p-value<0.1, \*\*p-value<0.05, \*\*\*p-value<0.01

## Discussion and Status of Research

Our results show that espoused organizational culture values have a significant impact on all the UTAUT variables, performance expectancy, effort expectancy, social influence, facilitating conditions, attitude, and anxiety. Facilitating conditions, attitude towards biometrics, and anxiety significantly affect use of biometric identity authentication systems, whereas the main UTAUT variables such as performance expectancy, effort expectancy, and social influence had no effect on the use of biometric system. This result is not surprising given the uniqueness of a biometric system. UTAUT and technology acceptance models have examined adoption of information systems that are essentially work related (Venkatesh et al. 2003). Individuals using these work-related technologies expect an improvement in job performance. This was not case in the technology we considered. A biometric identity authentication systems was a security oriented technology that did not claim to improve performance. Effort had no impact on use because the effort to use biometrics was minimal, and expected to be so. So, none of the “traditional” UTAUT variables could explain the use of biometric systems except for the individual’s attitude towards the biometric system.

We are currently working on different parts of this research. There is more work to be done in the justification of our hypotheses, explanation of the results, limitations, and future directions. We believe we are making a contribution to the literature on espoused organizational culture values and biometrics identity management technology acceptance.

## References

Not included due to space limitations. Available upon request.