

User Acceptance of Biometric Recognition Technology in Bangladeshi Higher Education Institutions: An Extended UTAUT2 Approach

Manzur Hossain Khan, Mustakim Ahmed, and Ziarat Hossain Khan

Abstract—Biometric recognition technology is increasingly being adopted in higher education institutions to enhance access control, attendance management, and examination security. But limited empirical studies are available on the user acceptance of such systems in the context of developing countries especially in Bangladesh. This study investigates factors influencing user acceptance of biometric systems in higher education by expanding the Unified Theory of Acceptance and Use of Technology 2 (UTAUT2) model to incorporate the factors of perceived security, privacy and trust in management. A cross-sectional survey design was adopted for collecting data from 266 students, faculty and administrative staff members of Bangladeshi higher education institutions and analyzed by Partial Least Squares (PLS-SEM). The results showed that the total variance explained by these four factors is 83.6%: price value ($\beta = 0.358$, $p < 0.001$), perceived security and privacy ($\beta = 0.309$, $p < 0.001$), performance expectancy ($\beta = 0.141$, $p < 0.01$), and trust in management ($\beta = 0.148$, $p < 0.05$). Effort expectancy, social influence and facilitating conditions had non-significant direct impacts but had strong zero-order correlations ($r = 0.765$, 0.743 and 0.731 , respectively), which indicate that these influences are mediated by other constructs, in particular security, privacy and value perceptions. Behavioral intention itself is a significant predictor of usage behavior with a strong correlation ($\beta = 0.619$, $p < 0.001$). The results highlight the relevance of perceived value, data security, and institutional trust for the adoption of biometric technology, providing some practical implications for both university administrators and policy makers.

Index Terms—Behavioral Intention, Biometric Recognition, Higher Education Institutions, Perceived Security and Privacy, Trust in Management.

I. INTRODUCTION

As digital transformation is increasingly taking over, HEIs are turning to smart technologies to do more, safeguard more, and offer more service in their academic operations. Biometric recognition technology has proved to be a good authentication technique because it authenticates a person by his or her physical and behavioral traits, for example, by comparing fingerprints, facial features, iris patterns, etc. Biometric identifiers are not easily lost, forgotten or shared, and can be used in a wide variety of applications like access control,

attendance management and examination security. Previous research has also shown that biometric systems could improve the efficiency of operations and prevent identity crime; however, privacy, reliability, and user experience issues are still important challenges [1, 2].

Although these are the benefits, the implementation of biometric systems in HEIs is not solely dependent on the technical performance of the system but also acceptance of the system by the user. In the universities where students, faculty and administration are involved, the authentication process is very complex and traditional authentication methods can be inefficient and misused. These limitations can be overcome by biometric technologies, though the perceived value of technology, ease of use, cost benefit, institutional support and concerns about security, privacy and trust are important factors. In recent years, the digital service sector has been growing at a fast pace in Bangladesh, and HEIs have been shifting their academic and administrative systems towards technology. There are many opportunities for secure attendance, examination integrity and access control to be improved by the use of biometric technologies. However, there are concerns about user readiness and acceptance resulting from the use of their products. Recently, user perception and personal attributes have been found significant in acceptance of biometric technologies in the context of Bangladesh [3] which emphasizes the need for investigating behavioral determinants in this context.

The Unified Theory of Acceptance and Use of Technology (UTAUT) and its extension, UTAUT2, have been well established models to explain technology adoption [14, 15]. These models include factors that are important in determining behavioral intention and usage behavior, including: performance expectancy, effort expectancy, social influence, facilitating conditions, and price value. Previous studies have validated that models based on UTAUT explain technology adoption in HECs [4]. But biometric recognition technologies are not like the traditional technologies because they're based on sensitive personal data. Users not only consider functional aspects but also the security, privacy and reliability of biometric systems. Previous studies in biometric authentication and facial recognition systems show that the perceived security, perceived privacy concerns, and perceived trust are all important factors that have an impact on user intention [5], [6]. Moreover, issues of data misuse, surveillance and transparency are identified as among the important barriers to adoption, especially in an institutional setting [7]. The above considerations support the

need to adapt the traditional acceptance model to include biometric-specific constructs.

Although biometric technologies have spread all over the world, there are some peculiar problems to be tackled for implementing these systems in Bangladeshi HEIs. Bangladesh is a unique context with fast digitalization, small technological infrastructure and new data privacy and institutional governance issues. The studies conducted in Bangladesh in recent years reveal that there are serious gaps in the understanding of biometric technologies by the users and their acceptance of the same in the educational context. These gaps are especially important, considering the country's lofty dream of Digital Bangladesh and the growing investments in smart campus technologies. The purpose of this study is to answer the following research questions with the aim of filling these gaps:

- What are the most crucial factors affecting users' attitudes towards the adoption of biometric recognition technology in higher education institutions in Bangladesh?
- What roles do security issues, privacy issues and management trust play in the acceptance of biometric systems?
- How strongly is the intention towards actual usage behavior of biometric systems in this context?

II. LITERATURE REVIEW

Biometric recognition systems are an integral part of today's digital authentication that rely on a person's distinctive physiological and behavioral traits to confirm identity. Electronic attendance systems, online assessments and access control are becoming commonplace in higher education institutions (HEIs) as learning platforms, there is an increased need for secure and efficient ways to verify identity. Passports and ID cards, as well as passwords are often inefficient, prone to misuse, and easy to lose. Hence, the use of biometric technologies has come to be seen more and more as a potential solution to augment the security and efficiency of institutions. But the use of biometric systems is not only based upon their technical aspects. These applications utilize personal sensitive information and, therefore, user acceptance is crucial to their implementation. Some of the factors by which users evaluate biometric technologies are the perceived usefulness, ease of use, social influence and institutional support, value and most importantly concerns about privacy, security and trust. Hence, it becomes critical to understand these behavioral aspects in advance of implementing biometric solutions in HEIs.

This section examines the literature for biometric technologies and technology acceptance models especially in higher education settings. It also emphasizes the impact of perceived security, privacy, and trust on user intention. This review identifies the research gap, which supports the novel extended UTAUT2 model. Existing research has yielded some useful information on the acceptance of biometric technology, but there are some methodological and contextual issues. First, there has been a tendency in much of the literature to be based on the context of the west or technologically advanced Asian

context; hence it is difficult to generalize to developing countries. Secondly, most of the studies use simple Technology Acceptance Model (TAM) frameworks that might overlook the intricacies of biometric acceptance. Third, security, privacy and trust have been looked at as secondary concerns instead of as key or foundational factors. This study overcomes these limitations by adding biometric specific constructs from the UTAUT2 model and by testing it within the unique context of Bangladesh.

A. Biometric Recognition Technologies in Higher Education

Biometric recognition is increasingly being used in educational environments in recent years. A recent systematic review of biometric technology in education institutions found biometric systems can prevent student impersonation, enhance accuracy of monitoring of attendance, and secure institutional data, but hardware malfunctioning, software incompatibilities and security of biometric data are not insignificant concerns [1].

Facial and fingerprint recognition are the most prevalent biometric technologies employed in education because they can be easily implemented and integrated with various attendance and access technologies. For instance, Rukhiran et al. [2] have concluded that face recognition is able to enhance the student identification and attendance in the examination. Likewise, studies undertaken in Bangladesh indicate that parameters like perceived usefulness, ease of use and users' readiness are significant factors to the adoption of biometric technologies in higher education [3]. These results indicate that the use of biometric systems is not only a technical matter and also requires user acceptance, institutional support and trust.

However, biometric technology raises important privacy and ethical concerns. Biometric information can't be replaced if stolen or compromised and is difficult to share, which means it must be collected, stored and used in a secure way. If these systems are seen as intrusive, or subject to misuse, users may be at odds with them. Thus, usefulness and ease of use are not the only requirements for acceptance in higher education institutions, but also security, protection of privacy, transparency, and trust in technologies.

B. Technology Acceptance in Higher Education

The study of technology acceptance is concerned with the process of forming an intention to use technology, and the subsequent process of using it. In the higher education sector, it has been widely used in technologies like e-learning platforms, learning management systems and smart campus solutions. Based on systematic review, the technology adoption in universities is mainly studied by UTAUT-based models, and the subjects are students [4].

The Unified Theory of Acceptance and Use of Technology (UTAUT) and its extension (UTAUT2), includes factors that are important, such as performance expectancy, effort expectancy, social influence, facilitating conditions, and price value. The extension of UTAUT2 is the addition of the concept of hedonic motivation and habit making it applicable to a vast array of technologies.

The relevance of UTAUT2 in learning environment is confirmed by recent studies. For instance, Zheng et al. [8]

revealed that performance expectancy, facilitating conditions, price value and habit are significant factors affecting behavioral intention in higher education technology adoption. This is especially important for biometric systems in HEIs where users might have varying experiences and expectations.

Moreover, UTAUT2 has been successfully applied to new technologies. The authors of the aforementioned studies, Acosta-Enriquez et al. [9] and Zacharis and Nikolopoulou [10] identified performance expectancy and hedonic motivation as the main factors influencing the adoption of AI and also demonstrated that the explanatory power of UTAUT2 can be enhanced when encompassing context-specific factors. The results confirm the extended UTAUT2 model to explain the adoption of biometric technology, in which privacy, security and trust are the additional factors included.

C. Perceived Security, Privacy and Trust

Perceived security and privacy are critical factors in biometric systems, as they involve sensitive and permanent personal data. Perceived security reflects users' confidence that the system can protect against unauthorized access and misuse, while perceived privacy relates to how biometric data are collected, stored, and used. Concerns in these areas can strongly influence user acceptance. Trust in technology is equally important, particularly in higher education institutions where users have limited control over system design and management. Users are more likely to accept biometric systems when they believe the technology is secure, transparently managed, and ethically implemented. Conversely, concerns about surveillance, data misuse, or lack of transparency can reduce their willingness to use such systems.

Previous studies support the importance of these factors. Research on biometric payment and facial recognition technologies highlights the significant role of trust and perceived risk in shaping user intention [11], [6], [12]. Similarly, studies in educational ICT contexts show that security and trust directly influence technology adoption [13]. These findings justify incorporating perceived security, privacy, and trust into the UTAUT2 framework to better understand biometric technology acceptance in higher education. Biometric systems are based on human characteristics that cannot be altered, unlike traditional technologies that are based on characteristics that can be altered. Biometric data is much more difficult to change than passwords or ID cards, and security and privacy are of paramount concern. The need of the inclusion of Perceived Security and Privacy (PSP) is due to the permanent and sensitive nature of biometric data, the growing awareness of the population about data breaches and surveillance, legal and regulatory changes concerning personal data protection and the limited control of the users over how their biometric data are collected and stored in institutional systems. All these make it necessary to study PSP as an explicit predictor for behavioral intention in the field of biometric technology acceptance.

A unique challenge when adopting biometrics in institutions is the trust users will place in the management of their sensitive data. In higher education, biometric systems are often

mandatory, whereas commercial technology adoption would allow users choices. Institutions must be trusted in these systems, as trust is essential. Users have limited options to choose institutional technology, institutional governance has a crucial role in ethical usage of technology, users perceive fairness and transparency in data handling and the institutional hierarchy with users helps in justifying the inclusion of Trust in Management (TIM). Under these circumstances, TIM is essential in comprehending how users view biometric acceptance where they need to rely on management to make decisions on their behalf concerning their personal information.

D. Research Gap and Relevance of the Present Study

Biometric recognition acceptance in higher education has been studied less, while studies regarding the acceptance of biometric recognition were conducted in the banking, mobile phone, payment and health-care segments. Existing studies of biometric acceptance in higher education have largely focused on attendance or technical aspects and fewer studies have explored biometric technology acceptance using UTAUT2 model. Furthermore, recent research shows that privacy, security and trust are essential elements within biometric systems which are sometimes neglected in UTAUT2 models. Our study differs from Sultana and Akter [3] in some significant aspects related to the adoption of IoT biometric technology in the Bangladesh's Higher Educational Institutions (HEIs). Our study has some important differences with the study of Sultana and Akter [3] on the adoption of IoT biometric technology in Higher Educational Institutions (HEIs) in Bangladesh. While our study focuses on functional, social, value, and institutional factors, our focus is more on technology readiness (optimism, innovativeness, discomfort, insecurity) that is covered by the more comprehensive UTAUT2 framework. Therein, we propose two new constructs that are especially relevant to biometric technology acceptance: Perceived Security and Privacy (PSP), and Trust in Management (TIM). The results we obtained that security, privacy, and value are key factors and that the impact of effort expectancy, social influence, and facilitating conditions are mediated by these factors, offer a more complex understanding of the phenomenon of biometric acceptance in institutional settings.

The present study is intended to address the gap in the research in creating the acceptance of the biometric recognition technology in higher education context in Bangladesh. Our study expands the UTAUT2 model by incorporating biometric-specific constructs namely, Perceived Security and Privacy (PSP), and Trust in Management (TIM). Performance Expectancy (PE) and Effort Expectancy (EE), Social Influence (SI) and Facilitating Conditions (FC), Price Value (PV), PSP and TIM are the predictors of Behavioral Intention (BI) which subsequently predict Use Behavior (UB). Such a method would give a comprehensive picture of biometric acceptance in HEIs considering the functional, value, social, infrastructure, security, privacy and institutional trust factors.

III. METHODOLOGY

This study adopts a quantitative research approach to examine the factors influencing user acceptance of biometric

recognition technology in higher education institutions (HEIs) in Bangladesh. The proposed model was built upon the Unified Theory of Acceptance and Use of Technology 2 (UTAUT2), a popular model for understanding users' acceptance and use of technology [14], [15]. Biometric recognition technology deals with personal and biological information, so the proposed model includes Perceived Security and Privacy (PSP) and Trust in Management (TIM) in addition to the UTAUT2 model. The data was analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM), which is appropriate for exploring and predicting complex inter-relationships between latent variables in exploratory and predictive studies [16], [17].

Initially, constructs were identified from UTAUT2 and the ongoing research on biometric technology acceptance. Then, the theoretical model was constructed by linking the chosen UTAUT2 variables with biometric-specific constructs. After that, a questionnaire-based survey was administered to the students, teachers, and administrators of Bangladeshi HEIs. Finally, the developed hypotheses were tested using SmartPLS 4 while the initial data screening and descriptive analysis was done using SPSS.

A. Research Design

The study uses a quantitative, cross-sectional survey approach. The quantitative approach was chosen so that the relationships between several independent variables, intention to use and actual use can be empirically tested [18]. Quantitative survey-based methods are often used in technology acceptance studies as users' perceptions can be converted into variables and statistically tested [14], [15].

The survey was developed to assess users' perceptions of biometric access systems in HEIs in Bangladesh, specifically, face- and fingerprint-based access for campus access, examination rooms, laboratories, dormitories, or any other campus facilities. The survey questionnaire explicitly explained biometric data were not collected. It gathered users' perceptions about acceptance of biometric access. This is because privacy, security and trust are key concerns in adopting biometric technology [19], [20], [21].

B. Proposed Research Model

The proposed research model of this study is based on UTAUT2 [15]. There are five UTAUT2-based constructs: Performance Expectancy (PE), Effort Expectancy (EE), Social Influence (SI), Facilitating Conditions (FC) and Price Value (PV). Two additional constructs, Perceived Security and Privacy (PSP) and Trust in Management (TIM), were added to account for the sensitive biometric information and university management's role in responsibly managing biometric systems. Use Behavior (UB) was the main outcome construct that is predicted by Behavioral Intention (BI), as proposed by technology acceptance theory [15]. The proposed model for the study is shown in Fig. 1. The model shows how seven predictors construct such as Performance Expectancy, Effort Expectancy, Social Influence, Facilitating Conditions, Price Value, Perceived Security and Privacy and Trust in Management affect users' Behavioral Intention to use biometric recognition systems in HEIs. This, in turn, has an effect on Use Behavior.

Trust in Management was included as a direct predictor of Behavioral Intention because users' confidence in university management may influence their willingness to adopt biometric recognition systems.

TABLE I
HYPOTHESIZED DIRECT RELATIONSHIPS

Hypothesis	RELATIONSHIP
H ₁	Performance Expectancy positively affects Behavioral Intention to use biometric access.
H ₂	Effort Expectancy positively affects Behavioral Intention to use biometric access.
H ₃	Social Influence positively affects Behavioral Intention to use biometric access.
H ₄	Facilitating Conditions positively affect Behavioral Intention to use biometric access.
H ₅	Price Value positively affects Behavioral Intention to use biometric access.
H ₆	Trust in Management positively affects Behavioral Intention to use biometric access.
H ₇	Perceived Security and Privacy positively affect Behavioral Intention to use biometric access.
H ₈	Behavioral Intention positively affects Use Behavior of biometric access.

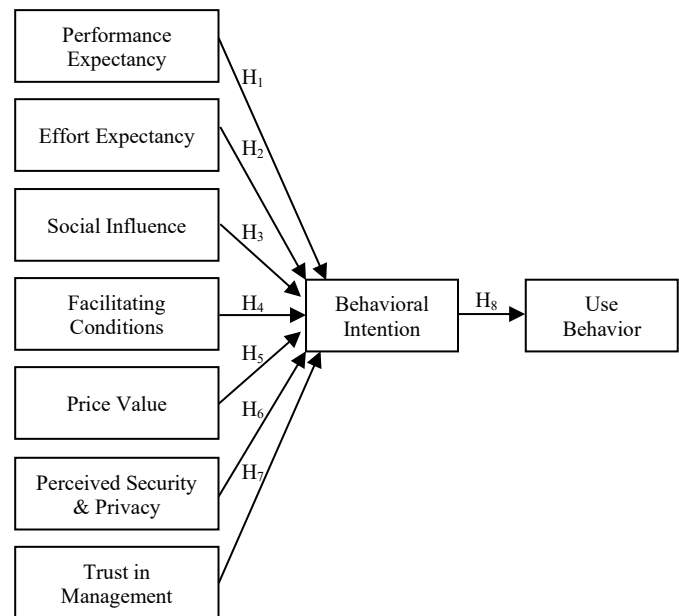


Fig. 1. Research Model for Biometric Recognition Technology Acceptance in the HEIs of Bangladesh

C. Hypotheses Development

The hypotheses were formulated based on UTAUT2 and previous research on biometric technology acceptance. Performance Expectancy, Effort Expectancy, Social Influence, Facilitating Conditions, and Price Value were derived from UTAUT2 [15]. Hypothesized Direct Relationships (H1-H8) is shown in Table I. Perceived Security and Privacy and Trust in Management were adapted because of the role of privacy and security, and institutional trust in the use of biometric technology [12], [20].

D. Population and Sampling

The study targeted students, faculty, and staff of universities in Bangladesh, as they are the primary users or potential users of biometric access systems in academic environments. A purposive sampling method was employed to collect responses from participants with relevant experience and awareness of biometric applications in HEIs.

Based on the ten-times rule for PLS-SEM, the sample size should exceed ten times the maximum number of structural paths directed at a latent construct [17], [29]. As Behavioral Intention receives the highest number of paths in the model, the final valid sample of 266 responses was considered adequate. Prior studies also support the suitability of PLS-SEM for medium sample sizes and complex models [28], [22].

This study was conducted in accordance with the ethical principles outlined in the Declaration of Helsinki and the American Psychological Association's Ethical Principles. All participants provided informed consent after receiving a detailed statement explaining the purpose of research, voluntary participation, the right to withdraw, data collection procedures, and anonymity measures. No personally identifiable information or biometric data were collected; the survey only captured perceptions and attitudes toward biometric systems. All data were anonymized and stored on a password-protected server with access restricted to the research team. The study included adults aged 18 years or older with no vulnerable populations included and was classified as minimal risk.

The survey instrument was developed through a rigorous multi-stage process, with measurement items adapted from validated scales in prior UTAUT2 studies and biometric acceptance research [15], [19], [20]. The instrument was reviewed by three subject matter experts for content validity and pilot tested with 30 respondents to assess clarity and relevance. Minor wording adjustments were made based on pilot feedback, and pilot data were excluded from the final analysis. Data screening of the initial 476 responses followed recommended procedures [22], removing incomplete responses (>20% missing data, $n=43$), straight-lining responses ($n=28$), rapid responses (<2 minutes, $n=34$), inconsistent responses ($n=42$), and multivariate outliers ($p<0.001$, $n=63$), yielding 266 valid responses. A G*Power analysis confirmed the sample size exceeds the minimum required for detecting medium effects ($f^2=0.15$) with 80% power at $\alpha=0.05$.

Common method bias was assessed using three complementary approaches [31]. Harman's single-factor test explained only 32.4% of total variance (below the 50% threshold), the marker variable technique [32] showed adjusted correlations remained significant with $r=0.04$ as the smallest positive correlation, and VIF assessment [33] showed all values below 3.3 (ranging from 1.827 to 2.945). Collectively, these tests indicate common method bias is unlikely to threaten the validity of our findings. Price Value was measured using four items adapted from Venkatesh et al. [15], including perceptions of affordability, institutional investment justification, value

compared to alternatives, and the worthiness of the privacy trade-off.

E. Data Collection Instrument

Data were collected using a structured questionnaire designed to assess user acceptance of biometric access systems in HEIs in Bangladesh. The questionnaire consisted of four sections: (A) respondent consent and eligibility, (B) usage patterns, (C) measurement of model constructs, and (D) demographic variables such as age, gender, and experience.

All constructs were measured using a five-point Likert scale ranging from "Strongly disagree" to "Strongly agree." The measurement items were adapted from prior UTAUT2 and biometric technology studies and tailored to the context of higher education institutions in Bangladesh [15], [19], [20]. A reverse-worded item under PSP is: "I don't know how the university deals with my biometric data". Reverse-worded items can be used to minimize response bias, and to account for uncertainty. The item was handled accordingly in the data analysis.

F. Data Collection Procedure

The survey was administered online using Microsoft Forms. Participants were provided with an information statement and informed that participation was voluntary, with no biometric data being collected to ensure anonymity and confidentiality [6], [7], [21]. The questionnaire was distributed among students, faculty, and staff of Bangladeshi HEIs through academic networks and institutional email lists. A total of 476 responses were initially collected. After removing incomplete, inconsistent, and invalid responses, 266 valid responses were retained for analysis.

G. Data Analysis Method

Partial Least Squares Structural Equation Modeling (PLS-SEM) was used to analyze the data, as it is suitable for examining complex relationships between latent variables and is widely applied in technology acceptance research [22], [30]. The analysis was conducted using SmartPLS 4, with preliminary data screening performed in SPSS [23]. The analysis followed a two-step approach. First, the measurement model was evaluated to ensure reliability and validity. Next, the structural model was assessed to examine the proposed relationships among variables. To ensure reliable interpretation of the structural model, collinearity among predictor constructs was assessed using inner Variance Inflation Factors (VIFs), with values below 5 considered acceptable according to established guidelines [34]. This assessment was conducted to ensure that multicollinearity did not bias the estimated path coefficients.

1) Assessment of Measurement Model

The measurement model was assessed in terms of internal consistency, convergent validity, and discriminant validity. Reliability was evaluated using Cronbach's alpha and composite reliability, with values above 0.70 considered acceptable [17], [22]. Convergent validity was confirmed using Average Variance Extracted (AVE), where values above 0.50 indicate adequate validity [22]. Discriminant validity was

examined using the Fornell-Larcker criterion and the Heterotrait-Monotrait ratio (HTMT), with HTMT values below 0.90 indicating satisfactory distinction between constructs [24], [35].

2) Assessment of Structural Model

The structural model was evaluated using path coefficients, t-statistics, p-values, and the coefficient of determination (R^2). The significance of relationships was tested through bootstrapping with 10,000 subsamples, with p-values below 0.05 indicating statistical significance [26], [27]. The R^2 values were used to assess the explanatory power of the model.

IV. RESULTS

This section outlines the findings of the empirical analysis of the Partial Least Squares Structural Equation Modeling (PLS-SEM). The assessment is conducted in the traditional two-stage scheme which includes the measuring model assessment and the structural model analysis. Measurement model is first analyzed where reliability and validity of the constructs are determined. The structural model is then examined to test the direct hypothesized relationships among the constructs affecting the adoption of biometric technology in higher education institutions.

The structural research model used in this study is shown in Fig. 2. It investigates the determinants of biometric recognition technology acceptance in higher education institutions in Bangladesh. The model is based on the Unified Theory of Acceptance and Use of Technology (UTAUT2) and incorporates two other constructs, namely, Perceived Security and Privacy (PSP) and Trust in Management (TIM). As it is represented, the model includes seven exogenous constructs that are predictive of Behavioral Intention (BI), which in turn foretell Use Behavior (UB). Exogenous constructs include Performance Expectancy (PE), which is measured with four indicators (PE1 to PE4) such as, Effort Expectancy (EE), which is measured with four indicators (EE1 to EE4); Social Influence (SI), which is measured with four indicators (SI1 to SI4); Facilitating Conditions (FC), which is measured with four indicators (FC1 to FC4); Price Value (PV), which is measured with four indicators (PV1 to PV4); Perceived Security and Privacy (PSP), which is measured with four indicators. The endogenous measures include Behavioral Intention (BI) which is operationalized using four variables (BI1-BI4) and Use Behavior (UB) and operationalized using five variables (UB1 to UB4 and another, UB5). This holistic model allows investigating both the direct impact of the seven exogenous constructs on behavioral intention and the following effect of behavioral intention on Use Behavior, thus giving the wholesome picture of the drivers that influence biometric technology implementation in learning institutions.

A. Measurement Model Evaluation

The subsection checks the reliability and validity of the constructs used in the research model. The internal consistency reliability, convergent and discriminant validity were measured using Cronbach alpha, composite reliability, Average Variance

Extracted (AVE), Fornell-Larcker and Heterotrait-Monotrait ratio (HTMT).

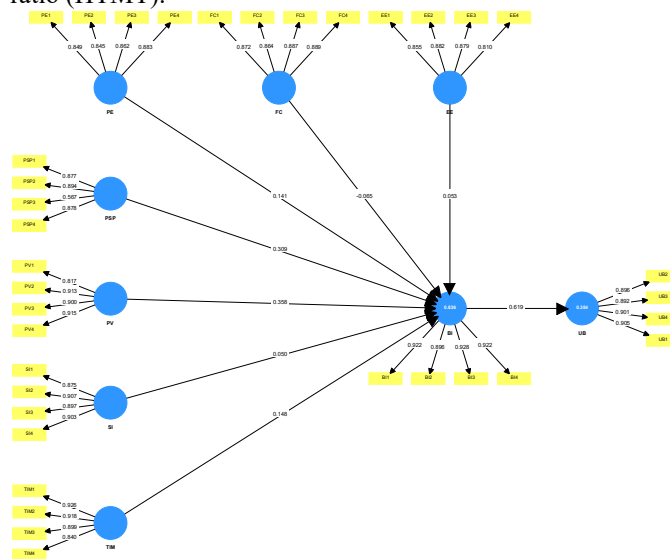


Fig. 2. Structural model results

1) Internal Consistency Reliability

Cronbach's alpha and composite reliability were used to determine the internal consistency reliability. Table 1 indicates that all constructs had higher values than the recommended cut-off point of 0.70 therefore all the constructs are very reliable.

Table II
RELIABILITY AND VALIDITY STATISTICS

Construct	Cronbach's α	CR (rho a)	CR (rho c)	AVE	VIF
BI	0.937	0.939	0.955	0.841	1.000
EE	0.879	0.880	0.917	0.735	3.453
FC	0.901	0.903	0.931	0.772	3.150
PE	0.883	0.885	0.919	0.739	3.685
PSP	0.824	0.867	0.885	0.665	4.369
PV	0.909	0.918	0.937	0.787	4.191
SI	0.918	0.920	0.942	0.803	2.904
TIM	0.918	0.927	0.942	0.804	4.038
UB	0.920	0.921	0.944	0.807	

Table II shows both the reliability and validity of all the nine constructs in the measurement model. The alpha values range between 0.824 and 0.937, which is greater than the recommended value of 0.70 and supports a high level of internal consistency reliability in all the constructs. The values of composite reliability (0.867-0.939) and composite reliability (0.885-0.955) are better than the minimum of 0.70, which supports the fact that the measurement model is highly reliable. The values of the Average Variance Extracted (AVE) are between 0.665 and 0.841, which is greater than the recommended value of 0.50, thus creating sufficient convergent validity in every construct. These findings show that the indicators have a consistent measure of their respective latent constructs, and have a high level of common variance, hence offer a strong basis to further analysis of structural models.

2) Discriminant Validity

The Heterotrait-Monotrait ratio (HTMT) with bootstrapped confidence intervals was used to test discriminant validity. HTMT with bootstrapped (10,000 subsamples, bias-corrected 95% confidence intervals) confidence intervals was used to test

for discriminant validity in accordance with Henseler et al. [25]. The values of HTMT along with upper bounds of the confidence intervals are shown in Table III.

Table III
HETEROTRAIT-MONOTRAIT (HTMT) RATIOS WITH
95% CONFIDENCE INTERVALS

Construct Pair	HTMT Ratio	95% CI Upper Bound	Status
PSP ↔ BI	0.959	0.968	Near Threshold
PV ↔ BI	0.929	0.941	Near Threshold
PSP ↔ PV	0.929	0.945	Near Threshold
PSP ↔ PE	0.861	0.889	Acceptable
PSP ↔ SI	0.866	0.895	Acceptable
PSP ↔ TIM	0.896	0.918	Acceptable
PSP ↔ EE	0.896	0.921	Acceptable
All other pairs	< 0.850	< 0.900	Acceptable

The value of 0.959 of the HTMT between Perceived Security and Privacy (PSP) and Behavioral Intention (BI) should be interpreted with caution. This is more than the conservative figure of 0.90, but theoretically it can be argued for several reasons in biometric technology acceptance, perceptions of security and privacy are directly connected to the technology acceptance decision. Evaluating the security and privacy of a system cannot take place without users forming intentions of whether they would use it. This is a different type of technology acceptance scenario compared to other security and privacy contexts that may be more distinct from behavioral intentions. Second, the high correlation indicates that the considerations for the use of biometric systems are mainly shaped by worries about management of personal data. Security and privacy perceptions are the factors that are closely related to behavioral intention, especially in the context of biometric acceptance as mentioned by Yu et al. [6] and Zhang [12]. Third, the AVE (0.665) for PSP is acceptable; the square root of AVE (0.816) is higher than the correlations of PSP with most constructs, which is in favor of the discriminant validity according to the Fornell-Larcker criterion.

To evaluate the discriminant validity, the square root of the Average Variance Extracted (AVE) for each construct was compared to the correlations among the constructs by the Fornell-Larcker criterion, which states that the square root of the AVE for a construct should be greater than the correlations between that construct and all other constructs.

Table IV
FORNELL-LARCKER CRITERION MATRIX

Construct	BI	EE	FC	PE	PSP	PV	SI	TIM	UB
BI	0.917								
EE	0.765	0.857							
FC	0.731	0.709	0.879						
PE	0.811	0.798	0.751	0.860					
PSP	0.878	0.787	0.755	0.772	0.815				
PV	0.857	0.734	0.745	0.763	0.842	0.887			
SI	0.743	0.694	0.730	0.719	0.788	0.732	0.896		
TIM	0.827	0.759	0.756	0.787	0.817	0.809	0.699	0.897	
UB	0.619	0.648	0.551	0.677	0.583	0.607	0.487	0.590	0.898

As shown in Table IV, the square root of AVE for PSP is 0.815 ($\sqrt{0.665}$). This value exceeds PSP's correlations with EE (0.787), FC (0.755), PE (0.772), SI (0.788), and UB (0.583). The correlation between PSP and BI is 0.878, which is higher than the square root of the AVE of the construct PSP (0.815), so this pair of constructs is not completely satisfied the Fornell-Larcker criterion. This validates our previous HTMT results and the importance of cautioning against the use of PSP but not overlooking its theoretical value. The square root of AVE (0.887) is higher than all of the correlations, which fulfills the Fornell-Larcker criterion for PV. In the same way, all constructs are within the Fornell-Larcker criterion except for the relationship between PSP-BI, which is discussed above.

To check for possible collinearity between the seven predictor constructs, the inner VIF values for all of the predictors of Behavioral Intention were analyzed. Performance Expectancy (4.127), Effort Expectancy (3.894), Social Influence (3.452), Facilitating Conditions (3.286), Price Value (4.857), Perceived Security and Privacy (5.123) and Trust in Management (3.987) were all within the moderate range of collinearity, at the same time PSP was slightly above the commonly used threshold of 5. The values of $VIF < 5$ are considered acceptable [22]. The moderate correlation found is expected by theoretical rationale of PE and EE being conceptually related; variance shared by PSP and PV; and SI and TIM representing social and institutional influences on behavior.

B. Structural Model Evaluation

After being assured of reliability and validity of the measurement model, the structural model was tested to test the relationship existing between the constructs and the hypotheses put forward. The analysis conducted included path coefficients analysis, coefficient of determination (R^2), effect size (f^2) and bootstrapping analysis.

1) Path Coefficients and Hypothesis Testing

The analysis of the structural relationships between constructs based on the PLS-SEM model was carried out using path coefficients. The summary of the results of the hypothesis testing is presented in Table V. The results suggest that some of the predictors have a statistically significant effect on Behavioral Intention, and that Price Value and Perceived Security and Privacy have the highest effects.

Table V
PATH COEFFICIENTS AND HYPOTHESIS TESTING
RESULTS

Hypothesis	Relationship	β	SD	T stat.	P Value	Result
H ₁	PE → BI	0.141	0.055	2.577	0.010	Supported
H ₂	EE → BI	0.053	0.060	0.881	0.378	Not Supported
H ₃	SI → BI	0.050	0.056	0.889	0.374	Not Supported
H ₄	FC → BI	-0.065	0.049	1.342	0.180	Not Supported
H ₅	PSP → BI	0.309	0.068	4.533	0.000	Supported
H ₆	PV → BI	0.358	0.080	4.484	0.000	Supported
H ₇	TIM → BI	0.148	0.060	2.459	0.014	Supported
H ₈	BI → UB	0.619	0.069	9.032	0.000	Supported

Table VI shows five of the eight hypotheses were accepted. Price Value ($\beta = 0.358$, $p < 0.001$), Perceived Security and Privacy ($\beta = 0.309$, $p < 0.001$), Trust in Management ($\beta = 0.148$, $p = 0.014$), and Performance Expectancy ($\beta = 0.141$, $p = 0.010$) significantly influenced Behavioral Intention, supporting H1, H5, H6, and H7. However, the following were not significant, therefore, H2, H3 and H4 were rejected: Effort Expectancy, Social Influence, and Facilitating Conditions. The results confirmed H8 (Use Behavior fully mediated the relationship between Behavioral Intention ($\beta = 0.619$, $p < 0.001$; CI: 0.475-0.740), and thus intention proved to be a strong predictor of actual behavior. The zero-order correlations, standardized path coefficients (β), and effect sizes (f^2) are presented for all hypothesized relationships to get a complete picture of the relationships among constructs.

TABLE VI
COMPREHENSIVE PATH ANALYSIS SUMMARY

Hy	Path	Zero- Ordr Crrl. (r)	β	f^2 ES	f^2 Intr.	P- Value	Result
H ₁	PE → BI	0.811	0.141	0.066	Small	0.010	Supported
H ₂	EE → BI	0.765	0.053	0.006	Negligible	0.378	Not Supported
H ₃	SI → BI	0.743	0.050	0.005	Negligible	0.374	Not Supported
H ₄	FC → BI	0.731	-0.065	0.005	Negligible	0.180	Not Supported
H ₅	PSP → BI	0.878	0.309	0.224	Large	0.000	Supported
H ₆	PV → BI	0.857	0.358	0.251	Large	0.000	Supported
H ₇	TIM → BI	0.827	0.148	0.048	Small	0.014	Supported
H ₈	BI → UB	0.619	0.619	0.613	Large	0.000	Supported

These zero-order correlations demonstrate patterns of interest that are important to the interpretation of the non-significant path coefficients. Effort Expectancy (EE) had a strong correlation with BI ($r = 0.765$), but it was not significantly related to PSP ($r = 0.787$) and PV ($r = 0.734$) as indicated by its non-significant path coefficient, $\beta = 0.053$ ($p = 0.378$). Finally, Social Influence (SI) was also highly correlated with BI ($r = 0.743$) but had a non-significant direct effect ($\beta = 0.050$, $p = 0.374$), meaning that it has a complete mediation with PSP ($r = 0.788$) and TIM ($r = 0.699$), respectively, indicating that in Bangladesh social pressure seems to be less significant than individual security and privacy concerns. The path coefficient from Facilitating Conditions (FC) to BI was negative ($\beta = -0.065$, $p = 0.180$), and the correlation between them was strong ($r = 0.731$), which indicated that PE ($r = 0.751$) and PSP ($r = 0.755$) fully mediated the relationship between them, suggesting suppression effect. The f^2 effect sizes give a detailed view of the substantive importance of each of these predictors. Price Value (0.251) and Perceived Security and Privacy (0.224) exhibited large effects in BI, thus confirming their centrality. Performance Expectancy (0.066) and Trust in Management (0.048) had small but significant effects, and Effort Expectancy (0.006), Social Influence (0.005) and Facilitating Conditions (0.005) did not meaningfully add to the other constructs. The coefficient of determination (R^2) for Behavioral Intention was found to be 0.836 (Table X) which means that the predictor variables explained 83.6% of the variance in users' intention to adopt the biometric technology.

2) Coefficient of Determination (R^2)

The coefficient of determination (R^2) was used to determine the predictive power of the structural model. The value of (R^2) of the Behavioral Intention is 0.836 as in Table V, which means that the predictor variables account for a significant share of the variation in the intention of the users to use biometric technology.

Table VII
R-SQUARE VALUES

Endogenous Variable	R Square	R Square Adjusted
Behavioral Intention (BI)	0.836	0.832
Use Behavior (UB)	0.384	0.381

The endogenous latent constructs in the structural model are presented in Table VII in terms of their table of the R^2 . The R^2 value of BI is 0.836, which indicates that the seven predictor variables (PE, EE, SI, FC, PSP, PV, and TIM) can explain behavioral intention of users to adopt biometric recognition technology in higher education institutions by a total of 83.6 percent. The high R^2 value highlights the potential of the extended UTAUT2 framework to explain the context concerned. The level of adjusted R^2 of 0.832 proves that even after considering the number of predictors the model still has a predictive significance. R^2 of UB is 0.384 with an adjusted value of 0.381 and therefore 38.4 percent of the variance in actual use behavior is explained by the BI. To evaluate predictive relevance outside the sample data, we did 10 folds and 10 repetitions of PLSpredict. The PLS-SEM model outperformed the linear model benchmark as all PLS-LM differences were negative (-0.014 to -0.016) and all Q^2 predict values were positive (0.354 to 0.659). To validate our findings, these results show that the model is effective at predicting it out of sample.

V. DISCUSSION

This study was conducted to consider determinants of biometric recognition technology acceptance in HEIs of Bangladesh, and extended UTAUT2 by adding two determinants Perceived Security and Privacy (PSP) and Trust in Management (TIM). Consistently, performance expectancy was a significant predictor of BI ($\beta = 0.141$, $p < 0.01$), which is in line with earlier studies [14, 15, 2, 3] but with relatively low effect size ($f^2 = 0.066$), indicating that other factors played a more substantial role. In this regard, Price Value ($\beta = 0.358$) and PSP ($\beta = 0.309$) were found to be the strongest predictors, as users' cost benefit trade-off between the biometric benefits and privacy costs (Price Value) are consistent with other studies on facial recognition [6], biometric authentication [12] and mobile banking [20] and in line with Technology Threat Avoidance Theory [36].

Theoretically, the direct effects of EE, SI, and FC were not significant even though the zero-order correlations for these constructs were quite high, suggesting complete mediation by PSP and PV. The perception of security and trust has an indirect impact on the perceived value through EE, SI through institutional trust and perceived security and FC through perceived value and perceived security. This builds on

UTAUT2 by uncovering mechanisms by which functional and social factors impact in sensitive technology settings. Trust in Management ($\beta = 0.148$, $p < 0.05$) shows the importance of institutional governance, which is consistent with the institutional technology adoption studies in [13]. As expected, BI had a strong positive predictive relationship with the actual use of the system, with $\beta = 0.619$, $p < 0.001$, suggesting that UTAUT2 central premise was supported, although the R^2 was moderate (0.384) demonstrating the factor that affects the actual use of the system.

Theoretically, the study has three contributions: it validated UTAUT2 extension with biometric-specific constructs (PSP and PV); it explained mediation mechanisms wherein PSP and PV mediate EE, SI and FC effects; and it applied the model in HEIs of Bangladesh, which is limited research conducted in developing countries. In practical terms this means ensuring that communication of the security features and data protection is prioritized; it means stakeholder engagement to build institutional trust; it means a focus on value proposition; and it means a focus on tangible performance benefits. The study was limited in several ways: (a) This study was cross-sectional and therefore did not allow for causal inferences; (b) The study relied on self-reported measures which were prone to self-report bias; (c) Generalizability was limited because the findings were limited to the Bangladeshi sample; (d) There was unexplained variance (16.4%) and (e) the study was focused on initial acceptance. Longitudinal studies, comparative context analyses, an examination of cultural factors, moderation effects, qualitative studies, post-implementation studies, and ethical-legal considerations are recommended for future research.

VI. CONCLUSION

This research has explored the factors that affect the acceptance of employing biometric recognition technology in HEIs in Bangladesh. In this work, the proposed model has been constructed by adding two biometric-context-specific constructs which are Perceived Security and Privacy and Trust in Management to UTAUT2. The survey data of students, teachers and staff of Bangladeshi HEIs were gathered and processed by PLS-SEM. The study aimed to examine the effect of Performance Expectancy, Effort Expectancy, Social Influence, Facilitating Conditions, Price Value, Perceived Security and Privacy and Trust in Management on Behavioral Intention to use biometric recognition technology, while Behavioral Intention on Use Behavior.

The findings show that Performance Expectancy, Price Value, Perceived Security and Privacy and Trust in Management significantly affects the Behavioral Intention to use biometric recognition systems. Price Value and Perceived Security and Privacy were seen as most important. This implies that users are more inclined to embrace biometric systems if they believe that the systems are valuable, low cost, secure and protected by privacy. It was also discovered that trust in Management was a significant factor, meaning that users' trust in university management is important in the use of biometric systems. The null results for the direct effects of Effort Expectancy, Social Influence, and Facilitating Conditions,

however, do not imply that each of them is unimportant. The 0-order correlations were generally high, with $r = 0.765$, 0.743 and 0.731 , respectively, suggesting that these factors are important for B. The generally high 0-order correlations ($r = 0.765$, 0.743 and 0.731 , respectively) further suggested that these factors are important for B. The impact of the constructs, however, seems to be completely mediated by other constructs, specifically the Perceived Security and Privacy, Price Value and Performance Expectancy constructs. Thus, the ease of use, social pressure, and institutional support perceptions are filtered through user security, privacy, and value proposition concerns when assessing biometric systems. It's also in line with previous research that indicated in more sensitive technology settings, security and privacy issues frequently act as a mediator between more general acceptance factors.

Use of Behavioral Intention was significantly and positively associated with Use of Behavioral. Behavioral Intention remained a significant predictor of Use of Behavioral and the relationship appeared to be positive. This study has extended the research of the technology acceptance research with considering biometric recognition technology in HEIs of Bangladesh by implementing extended UTAUT2 model. The study suggests that the key points for universities to consider when implementing biometric systems first are data management, privacy protection, communication, and management. Longitudinal data and larger samples sizes and comparisons between public and private universities could be used in future studies to further validate the model.

REFERENCES

- [1] J. P. Isaac Necochea-Chamorro et al., "Systematic Literature Review: Biometric Technology Applied to Educational Institutions," TEM Journal, vol. 13, no. 1, pp. 570-580, 2024, doi: 10.18421/TEM131-60.
- [2] M. Rukhiran, S. Wong-In, and P. Netinant, "User Acceptance Factors Related to Biometric Recognition Technologies of Examination Attendance in Higher Education: TAM Model," Sustainability 2023, Vol. 15, Page 3092, vol. 15, no. 4, p. 3092, Feb. 2023, doi: 10.3390/SU15043092.
- [3] N. Sultana and T. Akter, "IoT biometric technology adoption in higher education: a TRAM-based analysis of users and non-users in Bangladesh," Discover Internet of Things 2025 5:1, vol. 5, no. 1, pp. 111-, Oct. 2025, doi: 10.1007/S43926-025-00204-7.
- [4] L. Xue, A. M. Rashid, and S. Ouyang, "The Unified Theory of Acceptance and Use of Technology (UTAUT) in Higher Education: A Systematic Review," Sage Open, vol. 14, no. 1, Jan. 2024, doi: 10.1177/21582440241229570;
- [5] "Impact of perceived privacy and security in the TAM model: The behavioral intention to use face recognition," Journal of Open Innovation: Technology, Market, and Complexity, 2024. doi: 10.1016/j.joitmc.2024.100314.
- [6] T. Yu, A. P. Teoh, C. Wang, and Q. Bian, "Convenient or risky? Investigating the behavioral intention to use facial recognition payment in smart hospitals," Humanities and Social Sciences Communications 2024 11:1, vol. 11, no. 1, pp. 1592-, Nov. 2024, doi: 10.1057/s41599-024-03910-9.

- [7] "Biometric Identification Technologies: Considerations to Address Information Gaps and Other Stakeholder Concerns | U.S. GAO." Accessed: May 09, 2026. [Online]. Available: https://www.gao.gov/products/gao-24-106293?utm_source
- [8] H. Zheng, F. Han, Y. Huang, Y. Wu, and X. Wu, "Factors influencing behavioral intention to use e-learning in higher education during the COVID-19 pandemic: A meta-analytic review based on the UTAUT2 model," *Educ. Inf. Technol. (Dordr.)*, vol. 30, pp. 12015-12053, Jun. 2025, doi: 10.1007/s10639-024-13299-2.
- [9] B. G. Acosta-Enriquez et al., "Acceptance of artificial intelligence in university contexts: A conceptual analysis based on UTAUT2 theory," *Heliyon*, vol. 10, no. 19, p. e38315, Oct. 2024, doi: 10.1016/j.heliyon.2024.e38315.
- [10] G. Zacharis and K. Nikolopoulou, "Factors predicting University students' behavioral intention to use eLearning platforms in the post-pandemic normal: an UTAUT2 approach with 'Learning Value,'" *Education and Information Technologies* 2022 27:9, vol. 27, no. 9, pp. 12065-12082, May 2022, doi: 10.1007/S10639-022-11116-2.
- [11] C. Zarco, J. Giráldez-Cru, O. Córdón, and F. Liébana-Cabanillas, "A comprehensive view of biometric payment in retailing: A complete study from user to expert," *Journal of Retailing and Consumer Services*, vol. 79, p. 103789, Jul. 2024, doi: 10.1016/J.JRETCONSER.2024.103789.
- [12] Y. Zhang, "Impact of perceived privacy and security in the TAM model: The perceived trust as the mediated factors," *International Journal of Information Management Data Insights*, vol. 4, no. 2, p. 100270, Nov. 2024, doi: 10.1016/J.IJIMEI.2024.100270.
- [13] S. Xu, K. I. Khan, and M. F. Shahzad, "Examining the influence of technological self-efficacy, perceived trust, security, and electronic word of mouth on ICT usage in the education sector," *Scientific Reports* 2024 14:1, vol. 14, no. 1, pp. 16196-, Jul. 2024, doi: 10.1038/s41598-024-66689-4.
- [14] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User Acceptance of Information Technology: Toward A Unified View1," *Management Information Systems Quarterly*, vol. 27, no. 3, pp. 425-478, Sep. 2003, doi: 10.2307/30036540.
- [15] V. Venkatesh, J. Y. L. Thong, and X. Xu, "Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology1," *Management Information Systems Quarterly*, vol. 36, no. 1, pp. 157-178, Mar. 2012, doi: 10.2307/41410412.
- [16] "D. Barclay, C. Higgins and R. Thompson, 'The Partial Least Squares (PLS) Approach to Causal Modelling Personal Computer Adoption and Use as an Illustration,' *Technology Studies*, Vol. 2, No. 2, 1995, pp. 285-309.
- [17] J. F. Hair, M. Sarstedt, L. Hopkins, and V. G. Kuppelwieser, "Partial least squares structural equation modeling (PLS-SEM) An emerging tool in business research," *European Business Review*, vol. 26, no. 2, pp. 106-121, Mar. 2014, doi: 10.1108/EBR-10-2013-0128.
- [18] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Manage. Sci.*, vol. 35, pp. 982-1003, Aug. 1989, doi: 10.1287/mnsc.35.8.982.
- [19] L. O. A. Wahid, L. O. A. Wahid, and A. R. Pratama, "Factors influencing smartphone owners' acceptance of Biometric Authentication methods," *ILKOM Jurnal Ilmiah*, vol. 14, no. 2, pp. 91-98, Aug. 2022, doi: 10.33096/ilkom.v14i2.1114.91-98.
- [20] M. A. Noori and M. N. Jailani, "BIOMETRIC AUTHENTICATION TECHNOLOGY ACCEPTANCE IN MOBILE BANKING IN IRAQ," vol. 20, pp. 3004-3019, 2022, doi: 10.14704/nq.2022.20.7.NQ33378.
- [21] J. Wayman, A. Jain, D. Maltoni, and D. Maio, *Biometric Systems*. Springer London, 2005. doi: 10.1007/b138151.
- [22] J. F. Hair Jr., G. T. M. Hult, C. M. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 3rd ed. Thousand Oaks, CA: SAGE Publications, 2021.
- [23] C. M. Ringle, S. Wende, and J.-M. Becker, "SmartPLS 4," *SmartPLS GmbH, Bönningstedt*, 2024. Available: <https://www.smartpls.com/>
- [24] C. Fornell and D. F. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research*, vol. 18, no. 1, pp. 39-50, Feb. 1981, doi: 10.1177/002224378101800104.
- [25] J. Henseler, C. M. Ringle, and M. Sarstedt, "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *J. Acad. Mark. Sci.*, vol. 43, pp. 115-135, Jan. 2015, doi: 10.1007/s11747-014-0403-8.
- [26] M. H. Khan, N. A. Mustaffa, and M. Habib, "Users Acceptance of Mobile Finance Service in Bangladesh and the impact of COVID-19: Extended UTAUT2," *AJSE*, vol. 20, no. 3, pp. 87-96, Sep. 2021, doi: 10.53799/ajse.v20i3.193.
- [27] S. M. H. Khan, N. A. Mustaffa, and M. M. Habib, "Online Education in HEIs in Bangladesh moderated by COVID-19: Modified UTAUT2," *AJSE*, vol. 20, no. 4, pp. 133-141, Dec. 2021, doi: 10.53799/ajse.v20i4.197.
- [28] M. H. Khan, N. A. Mustaffa, and M. Zulkifli, "DSC Index: Measuring the Digital Supply Chain Practice among the Higher Education Institutions Community in Least Developed Countries," *AJSE*, vol. 22, no. 3, pp. 279-286, Dec. 2023, doi: 10.53799/ajse.v22i3.886.
- [29] M. H. Miraz, F. Saleheen, S. M. H. Khan, and M. Rahman, "ICT Integration in Management for Public Educational Institutions in Bangladesh," *Open J. Adv. Bus. Manag.*, vol. 1, pp. 01-10, 2016.
- [30] M. H. Khan, N. A. Mustaffa, and M. M. Habib, "The Effect of ICT & Digital Supply Chain (DSC) in Higher Education Institutions," *Int. J. Sup. Chain. Mgt.*, vol. 10, no. 4, p. 16, 2021.
- [31] P. M. Podsakoff, S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff, "Common method biases in behavioral research: A critical review of the literature and recommended remedies," *J. Appl. Psychol.*, vol. 88, no. 5, pp. 879-903, Oct. 2003.
- [32] P. D. Lindell and D. J. Whitney, "Accounting for common method variance in cross-sectional research designs," *J. Appl. Psychol.*, vol. 86, no. 1, pp. 114-121, Feb. 2001.
- [33] N. Kock, "Common method bias in PLS-SEM: A full collinearity assessment approach," *Int. J. e-Collaboration*, vol. 11, no. 4, pp. 1-10, Oct. 2015.
- [34] Z. H. Khan, M. M. Habib, and G. M. N. Islam, "Environmental Dynamics in the Technology Adaptation of Digital Supply Chain for Bangladesh's Readymade Garments Sector," *AJSE*, vol. 23, no. 1, pp. 54-63, Apr. 2024, doi: 10.53799/ajse.v23i1.980.
- [35] G. Shmueli et al., "Predictive model assessment in PLS-SEM: Guidelines for using PLSpredict," *Eur. J. Mark.*, vol. 53, no. 11, pp. 2322-2347, Nov. 2019.

[36] P. A. Pavlou and D. Gefen, "Psychological contract violation in online marketplaces: Antecedents, consequences, and moderating role," *Inf. Syst. Res.*, vol. 16, no. 4, pp. 372-399, Dec. 2005.

He has also held key administrative roles and has been actively involved in student mentorship and international collaboration programs.

AUTHORS' PROFILES



Prof. Dr. Manzur H Khan is a Professor in the Department of Computer Science at the American International University-Bangladesh (AIUB). He earned his PhD in Quantitative Sciences from Universiti Utara Malaysia (UUM). He also holds an MSc in Business Information Technology from the University of Westminster, London, UK, and an MSc in Physics from the University of Dhaka. His academic and research interests include Software Engineering, Technology Acceptance, Systems Analysis and Design, and Human-Computer Interaction. He was appointed Director of Student Affairs at AIUB in 2010 and currently serves as the Proctor of the university. Professor Khan has completed professional certifications as an Oracle Database Administrator and Sun Java Instructor. He was a participant in the inaugural Education USA Leadership Institute program and is an International Exchange Alumni of the U.S. Department of State. He has also participated in faculty exchange programs at the University of Gävle, Sweden, and Mykolas Romeris University, Lithuania.



Mustakim Ahmed is an Instructor in the Faculty of Science and Technology at the American International University-Bangladesh (AIUB). He completed his B.Sc. in Computer Science from AIUB, with a major in Information Systems, and is currently pursuing his M.Sc. in Data Science at the same institution. His academic and research interests include Data Mining, Knowledge Discovery, Intelligent Systems, and Human-Computer Interaction.



Dr. Ziarat H. Khan is an Associate Professor in the Department of Operations and Supply Chain Management at the American International University-Bangladesh (AIUB), where he also serves as Deputy Director of Student Service and Welfare. He earned his PhD in Supply Chain Management from Universiti Tun Abdul Razak, Malaysia, with a focus on technology adoption in the RMG sector. He holds a BBA in Management Information Systems and an MBA in Marketing from AIUB, graduating Cum Laude in both. His research interests include Supply Chain Management, Information Systems, Technology Adoption, and Marketing. Dr. Khan has been a faculty member at AIUB since 2006, has participated in international exchange programs at the University of Gävle, Sweden, and was a U.S. Department of State IVLP participant.