



ISSN: 3006-7251 (Online)

MBSTU Journal of Science and Technology

DOI: <https://doi.org/10.69728/jst.v12.141>

Journal Homepage: <https://journal.mbstu.ac.bd>



Data Privacy in the Cloud: Trends, Risks, and Organizational Practices

Moskura Hoque^{1*}, Mostofa Kamal Nasir¹

¹ Department of Computer Science and Engineering, Mawlana Bhashani Science and Technology University, Santosh, Tangail-1902, Bangladesh

ARTICLE INFO

Article History

Received: 21 May, 2026

Revised: 03 September, 2026

Accepted: 27 September, 2026

Published: 04 October, 2026

Keywords

Cloud Computing, Data

Privacy, Encryption,

Governance, Risk

Management

ABSTRACT

Cloud computing is increasingly leveraged by Bangladeshi organizations, including utilities, financial institutions, and technology firms, for scalable data storage and analytic capabilities. However, migrating sensitive operational and personal data to cloud environments introduces serious privacy challenges. This study investigates the evolving trends, risks, and organizational practices related to data privacy in the cloud within the Bangladeshi context. We conducted a cross-sectional survey of 132 IT and security decision-makers such as CISOs, cloud architects, and compliance officers to assess perceived risks, governance maturity, and technical control adoption. Key findings reveal that misconfiguration, insider threat, and weak key management are viewed as the most significant risks, while regulatory compliance (e.g., under Bangladesh's new Personal Data Protection Ordinance) is also a major concern. On the governance front, 70% of organizations report having a formal data-governance framework, with over half using shared-responsibility matrices and including audit and breach-notification clauses in contracts. Technically, encryption (at-rest and in-transit) is widely used, but only a small fraction of firms has adopted advanced privacy-preserving technologies, such as homomorphic encryption or TEEs. Trust in cloud service providers is moderate (mean score $\sim 3.6/5$) and correlates strongly with governance maturity and external audits. Based on these insights and the regulatory landscape in Bangladesh, we organize organizational cloud privacy practices into a five-phase risk-management framework (Assessment, Design, Implementation, Monitoring, Review) to help organizations enhance their cloud privacy posture which is grounded theory in institutional and IT governance logic.

1. Introduction

The swift entry of cloud computing has revolutionized the manner in which sensitive data is stored, processed and managed by organizations. Cloud platforms come with numerous benefits, including scalability and cost savings, across various industries including banking, information and communication technology (ICT), and utilities, but they also raise longstanding issues about data privacy, governance and organizational trust. These are especially relevant in economies in transition, where institutional development and organizational competence is still in its infancy, and regulatory regimes are still maturing (Abed & Chavan, 2019). Existing work on cloud data privacy has been twofold so far. Another stream focuses on technical solutions, including anonymization and secure multi-party computation, as crucial tools to reduce the privacy concerns with cloud data storage and processing

(Silva *et al.*, 2021; Agrawal *et al.* (2012). The other stream is the regulatory compliance and governance, which emphasizes the need for new regulations that correspond to the practices of cloud computing (Sprague, 2010). Both viewpoints are important, but they are usually explored separately and there is little empirical research connecting technical controls, governance practices, and/or organizational trust, particularly in multi-sector, developing-country settings.

One of the key issues was that cloud platforms are multi-tenant, and multiple customers share a common set of physical resources, which made the failure of isolation and the presence of side-channel attacks more probable, and possibly confidential data being leaked out to an unintended recipient (Gholami & Laure, 2016). Moreover, cloud users can also lose control of data location and lifecycle management, bringing regulatory and

¹ Corresponding author: moskura123@gmail.com

governance issues. The smart grid systems pose specific privacy problems. Energy consumption data collected through smart meters has the potential to provide fine-grained data on energy usage by the household, and thereby, to profile individuals (Han *et al.*, 2025). Meanwhile, cloud computing also poses traditional and new security-privacy dilemmas. Common vulnerabilities are data loss or leakage, insecure interfaces, weak identity and access management, and misconfigurations (Soofi *et al.*, 2017). Moreover, adaptive attacks can be used to take advantage of weaknesses in the virtualization and control layers if strong isolation and monitoring are not put in place (Abdulsalam & Hedabou, 2021). Additionally, organizations must place trust in the internal controls of the cloud service provider, which is another key concern, and may not be able to see into their operations at all times (Chauhan & Shiaeles, 2023).

To overcome these challenges, regulatory and governance mechanisms are changing. Organizations are becoming more interested in operationalizing privacy in the cloud, and standards like ISO/IEC 27018, which offers a code of practice for protecting PII in public clouds (De Hert *et al.*, 2016), are becoming more popular. To harmonise GDPR compliance in CSPs, codes of conduct such as the EU Cloud Code of Conduct are trying to set transparency, accountability and norms of data handling (Calder, 2021). In terms of technology, privacy enhancing technologies (PETs) like homomorphic encryption, secure multi-party computation and differential privacy are actively researched and used to ensure privacy without compromising the utility. For instance, in the smart grid applications, some differential privacy techniques have been suggested to preserve the privacy of individual energy use information while enabling overall conclusions (Turan *et al.*, 2020). But there are a number of obstacles to be overcome. PETs can also cause computational overheads, making real-time analytics difficult. The survey respondents come from a cross section of industry, such as financial services, ICT companies and utilities.

In view of this, the study aims to fill in this gap by exploring the risks associated with cloud data privacy, cloud governance maturity, technical control and organizational trust while analyzing the survey data of the cloud adopting organizations in Bangladesh. This study does not call for new technological solutions or unknown risks, but rather provides empirical understanding of the interaction of existing risk factors and governance mechanisms, and how they relate to trust results at the organizational level. There are three contributions of this study specifically. First, it will give empirical evidence of the relative weight of perceived cloud privacy risks, governance practices, and technical controls on organizational trust in cloud service providers in an emerging regulatory landscape. Second, it embeds those features in an institutionally grounded organizational framework, accounting for the role of governance maturity as a key component connecting the risk management practices with trust. Third, the study builds on these findings to create a structured 5-phase

cloud privacy risk management framework as an analytical and practical lens as an alternative to a theoretical model.

1.1. Objective of the study

To examine the trends, risks, and organizational practices related to data privacy in cloud computing and assess how governance maturity and technical controls influence organizational trust in cloud service providers in Bangladesh.

1.2. Research Gap

Although cloud data privacy has been widely studied, existing research predominantly emphasizes either technical privacy-preserving mechanisms (e.g., encryption, differential privacy, homomorphic encryption) or regulatory and governance frameworks in isolation. Few empirical studies have simultaneously examined the interplay between perceived privacy risks, governance maturity, technical control adoption, and organizational trust within a single analytical framework. Furthermore, evidence from developing countries, particularly Bangladesh, remains limited despite the rapid adoption of cloud computing and the emergence of new data protection regulations. Most prior studies also focus on cloud adoption intention rather than post-adoption organizational privacy management practices. Consequently, there is insufficient empirical understanding of how governance mechanisms and technical controls jointly influence organizational trust and cloud privacy outcomes in real organizational settings. This study addresses these gaps by providing multi-sector empirical evidence from Bangladesh and proposing an organizationally grounded five-phase cloud privacy risk management framework.

1.3. Hypothesis

H1: *Higher organizational cloud governance maturity is positively associated with greater organizational trust in cloud service providers.*

2. Literature Review

2.1. Organizational Behavior, Trust, and Theory in Cloud Data Privacy

To understand how organizations view and respond to privacy threats in the cloud, organizational behavior and theory are crucial. In addition to technical solutions there are organizational factors of decision making, compliance pressures, and the process of trust formation that are revealed by research in real contexts that account for the development, adoption, and sustainability process of cloud privacy practices. For instance, studies on trustworthiness measurement models indicate that cloud trust can be manifested through compliance and feedback processes that assess the extent to which the CSPs comply with the governance and privacy expectations, which, in turn, affects the level of confidence of the users of cloud services (Akhtar *et al.*, 2024). The implementation of cloud technology also is discussed using the popular

behavioral and organizational models, the Technology Organization Environment (TOE) model and Theory of Planned Behavior (TPB). Theoretical models can be used to understand the relationship between attitudes regarding cloud privacy, perceived threat, and organizational readiness and intention to use cloud products/services (Gangwar *et al.*, 2015; Garrison *et al.*, 2018). The integration of TPB and TOE offers a comprehensive overview, highlighting that perceived ease of use and perceived trust are important factors, while perceived risk might not be a major barrier to adoption (Hanif *et al.*, 2025). However, there are some reports that there are still some aspects to cloud adoption that fall short of intention, such as organizational inertia and resistance to change, suggesting that despite the frameworks still some aspects of the cloud adoption remain problematic.

2.2. Regulatory and Organizational Context for Cloud Data Privacy

Organizations' attitudes toward and approaches to privacy risks in the cloud are deeply shaped by the pressure of regulation and governance arrangements. According to the institutional theory, it is possible to influence organizational governance, compliance behavior, and trust in third party service providers through the creation of formal rules, accountability, and legitimacy requirements. For instance, research in cloud adoption shows that external institutional pressures (coercive and normative) shape organizational attitudes and acceptance behavior toward cloud services with trust serving as a moderator between these pressures and attitudes (Gupta, 2025). In

the cloud computing world, organizational governance structures are seen as important for ensuring that information security policies are compatible with other policy goals. In cloud settings, systematic reviews point to the need to combine risk assessment, compliance, ongoing assessment and control to guarantee data protection and accountability in the context of information security governance (AlGhamdi *et al.*, 2020).

Moreover, the development of cloud governance frameworks emphasizes the need for beyond-technical safeguards, that is documented workflows and governance frameworks in compliance with regulatory requirements and compliance expectations of stakeholders (Rahmika *et al.*, 2025). Empirical studies on cloud trust also indicate that non-technical factors such as perceptions of security and privacy, and governance mechanisms influence organizational trust in cloud service providers. These studies support the concept of how trust builds up due to institutional and governance aspects, as well as perceived risk (Alsmadi *et al.*, 2022). The resulting body of scholarly workplaces regulatory regimes and organizational governance at the heart of cloud privacy practices and suggests an interpretative approach that focuses on organizational behavior and institutional compliance and the formation of trust rather than technology or cryptography.

Table 1 provides a comparative summary of selected studies and regulatory documents relevant to cloud data privacy, highlighting differences in scope, methodology, and contextual focus, and positioning the present study within this literature.

Table 1: Comparative Summary of Cloud Data Privacy Literature.

Study / Document	Primary Focus	Methodology / Approach	Context	Key Limitation
Akhtar <i>et al.</i> (2024)	Proposed a trustworthiness model for cloud service providers (CSPs) that combines compliance, user feedback, and auditor ratings to assess trust.	Qualitative development of a compliance + feedback trustworthiness model and experimental proof of concept implementation.	Cloud computing adoption and trust assessment for cloud based digital twins	Focuses on a specific scenario (digital twins); may not generalize to broader organizational contexts or different cloud services.
Garrison <i>et al.</i> (2018)	Identifies factors that motivate individuals to use cloud based services	Survey or empirical analysis of individual users	Cloud use adoption at the individual consumer level rather than organizational adoption.	Not specific to organizational or governance aspects; older focus on individual motivation may not align with organizational privacy/trust theory.
Gangwarr <i>et al.</i> (2015)	Investigates determinants of cloud adoption using TAM and TOE frameworks.	Empirical study using a TAM TOE integrated model (likely quantitative – surveys/SEM).	Organizational adoption decisions for cloud computing across industries.	Pre 2018 (outside your 8 year range), so less ideal for the latest organizational privacy contexts.

Hanif <i>et al.</i> (2025)	Explores factors influencing intention and actual usage of SaaS cloud applications among SMEs using integrated TAM and TOE models; highlights the role of trust	Structural Equation Modeling (SEM) on data from 204 Swedish SMEs to assess antecedents of adoption and usage.	Organizational SME cloud adoption context, focusing on SaaS applications.	Focused on SaaS usage and intention rather than cloud privacy governance directly; may not address privacy controls or compliance explicitly.
Gupta (2025)	Examines how institutional pressures, governance structures, and trust influence cloud adoption decisions	Empirical survey analysis using institutional theory and adoption models	Public sector e-government cloud services	Focuses on adoption intention rather than post-adoption governance effectiveness or privacy risk outcomes
AlGhamdi <i>et al.</i> (2020)	Identifies governance mechanisms, compliance drivers, and organizational challenges in information security	Systematic literature review of IS governance studies	Cross-sector organizational information systems	Does not empirically test relationships between governance mechanisms and trust or perceived privacy risk
Rahmika <i>et al.</i> (2025)	Proposes governance frameworks linking confidentiality, integrity, availability, and compliance in cloud environments	Conceptual framework development with illustrative cases	General organizational cloud computing environments	Conceptual in nature; lacks empirical validation using organizational survey data
Alsmadi <i>et al.</i> (2022)	Explores the role of trust and perceived risk in shaping cloud usage behavior	Quantitative survey with structural modeling	Organizational cloud service users	Focuses on behavioral intention rather than governance maturity or regulatory compliance mechanisms
	Cloud privacy risks, governance maturity, and trust	Survey-based empirical analysis with correlation and regression	Multi-sector (Bangladesh)	Context-specific findings; does not propose new cryptographic techniques

2.3. Critical Analysis and Synthesis

Existing studies on cloud data privacy have primarily focused on three areas: technical privacy solutions, governance and regulatory compliance, and cloud adoption and trust. While technical studies emphasize encryption and privacy-preserving technologies, governance research highlights compliance frameworks and organizational policies. Behavioral studies mainly examine trust as a driver of cloud adoption rather than post-adoption privacy management. Consequently, these research streams remain largely disconnected, providing limited empirical evidence on how perceived privacy risks, governance maturity, and technical privacy controls jointly influence organizational trust. Furthermore, most studies have been conducted in developed countries, leaving a significant gap in developing-country contexts such as Bangladesh. This study addresses these limitations by integrating these factors into a unified conceptual framework to explain organizational trust in cloud service providers and organizational data privacy practices.

2.4. Conceptual Framework

Based on Institutional Theory and IT Governance Theory,

this study proposes that organizational trust in cloud service providers is influenced by three key predictor variables: perceived privacy risks, governance maturity, and technical control adoption. Higher perceived privacy risks are expected to reduce organizational trust, whereas stronger governance practices and greater adoption of technical controls are expected to enhance trust. This framework provides the theoretical basis for examining the relationships between these variables in the context of cloud data privacy in Bangladesh.

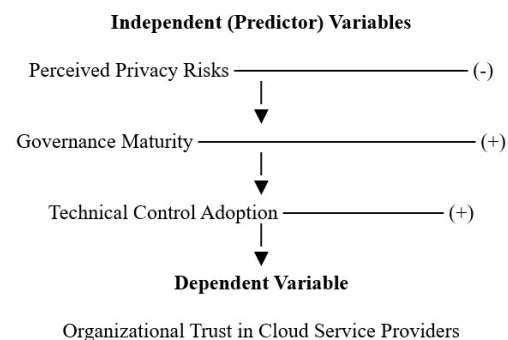


Figure 1: Conceptual Framework.

3. Methodology

3.1. Research Design

We adopted a cross sectional quantitative survey design to gain a holistic understanding of the data-privacy risk perception and management of the surveyed organizations in Bangladesh. This design is suitable for both descriptive and correlational analysis due to the snapshot of practices, perceptions and governance arrangements being taken at a specific moment in time across a variety of industries (e.g., banking, utilities, technology). A survey-based approach is preferred as it offers is scalable and allows the use of statistical analysis to examine relationships between variables, such as risk perception vs. adoption of technical control, as well as an insight into the maturity of governance frameworks. The survey questionnaire was adapted from previously published studies on cloud computing, IT governance, information security, and organizational trust (e.g., Gangwar *et al.*, 2015; Garrison *et al.*, 2018; Alsmadi *et al.*, 2022; Akhtar *et al.*, 2024; Gupta, 2025). Existing validated measurement items were adapted to the Bangladeshi organizational context and the objectives of this study. Content validity was established through expert review by specialists in cloud security, information systems, and research methodology before pilot testing. Face validity was strengthened through pilot testing with ten professionals, and internal consistency reliability was assessed using Cronbach's alpha. Since the primary objective of this study was exploratory and the sample size ($n = 132$) was relatively modest, exploratory and confirmatory factor analyses were beyond the scope of the present study. This limitation has been acknowledged in the revised manuscript, and future studies are recommended to conduct comprehensive construct validation using EFA/CFA and convergent validity assessment.

3.2. Sample & Recruitment

We specifically sought out a non-probability, purposive sample of senior IT and security decision makers in the organizations we surveyed in Bangladesh. We looked specifically at cloud roles that have decision-making authority or direct influence on cloud strategy: cloud architects, CISOs (Chief Information Security Officers), compliance officers, and IT managers. By focusing on this, respondents get visibility and accountability for cloud-privacy policies and practices. To ensure a wide reach of relevant organizations, recruitment efforts were made via several professional channels: LinkedIn, local forums for cloud computing, and industry associations. We received a total of 132 complete survey responses over a four-week period, a number that is adequate for descriptive statistics and regression analysis, but not so large as to impede in-depth analysis.

3.3. Survey Instrument

A structured, self-administered questionnaire was created with five main sections:

1. Organizational Profile – Size of the organization

(Number of employees), Sector (Banking, Utilities, ICT, etc.), Type of cloud deployment (Public, Private, Hybrid).

2. Risk Perceptions – participants rate, on a Likert scale, their level of concern with different cloud-privacy risks, including misconfiguration, insider threat, key management issues, noncompliance with cloud regulations, and multi-tenancy risks.

3. Governance Practices – questions focus on the presence and level of formality of governance arrangements, such as having a shared-responsibility matrix with the cloud provider, whether SLAs have certain clauses (audit rights, breach notification), and whether international standards (such as ISO 27001, ISO 27018) are being adopted.

4. Technical Controls – the instrument explores practical implementations: encryption (at-rest/in-transit), key management solutions (KMS/HSM), advanced PETs (homomorphic, MPC), trusted execution environments (TEEs), identity and access management (IAM), and use of policy-enforcement tools (CASBs).

5. Trust & Compliance – respondents rate their trust in their cloud service providers, describe how often they are subjected to third-party audits and list any provider certifications (such as ISO, SOC) or compliance activities pertaining to regulations.

To provide clarity, relevance and reliability, we tested the questionnaire with 10 security professionals in Bangladesh. Their input made improvements to the wording of the items, scale selections, and the flow of items, thus enhancing the instrument's face validity.

3.4. Pilot Testing and Instrument Refinement

The survey instrument was pre-tested with ten professionals of cloud and information-security in Bangladeshi organizations before the survey. The pilot test was not intended for statistical estimation purposes; it was used to test the clarity and relevance of the items on the survey, and the interpretability of these items. Following pilot participants' feedback, some refinements were made. First, the technical jargon, such as cloud-security jargon concerning access control and key management, was made understandable and/or provided with brief, explanatory descriptions. Secondly, the anchors of each scale were reformulated to ensure that they have the same meaning for all respondents. Third, the question sequence was restructured to enhance the logical flow, with a logical structure for the questions concerning risk perception, governance, and technical controls. The pilot process participants indicated that these changes in the tools were helpful to decrease the ambiguity and increase clarity, especially when answering questions related to governance and compliance. During the pilot phase, no substantive content was removed; a few clarifications were made, refinements made to the wording and ensuring consistency of responses. Consequently, the final instrument has better face validity and usability, which enhances the confidence in the instrument's responses

to the respondents' perceptions and their organizational practices.

3.5. Data Collection & Ethical Considerations

The questionnaire was sent out electronically using a survey software (such as Qualtrics or Google Forms) to ensure it was widely distributed and responses could be easily monitored. The data collection lasted four weeks and two reminder e-mails were sent to encourage respondents. All respondents received an informed-consent statement at the beginning of the survey, and participation was completely voluntary. We assured anonymity by not collecting personally identifying information and by aggregating responses. Responsive confidentiality was adhered to, and collected data were secured, following ethical best practice. For clearness and transparency, the survey questionnaire, survey report and a small sample of dataset has been added in Appendix A, B and C.

3.6. Data Analysis

We carried out a multi-step data analysis procedure:

To describe the distribution of the key variables (risk perception, control adoption, governance maturity, trust), we calculated mean values, frequencies, and standard deviations. This allows a clear understanding of the common practices and perceptions of organizations.

To determine if there are sensible correlations between the level of association of organization perceived risk and the level of association of the implementation of governance or technical controls, we used Pearson correlation coefficients. This helps to highlight trends like: are companies that are more worried about misconfigurations more likely to invest in encryption and governance?

We used multiple linear regression (MLR) to gain insight into the factors influencing Cloud service providers (CSPs) trust. Trust (a self-report Likert measure) was the dependent variable. Independent variables included:

- Governance maturity (a composite score based on the presence of the governance framework, shared-responsibility matrix, SLA clauses)
- Establishment of technical controls (an index of encryption, IAM, PETs, etc.).
- Audit frequency – frequency of external audits conducted on the CSP by an organization.

In doing this we evaluate the extent to which this variance is accounted for by these factors.

3.7. Rationale and Validity

The cross-sectional survey method was chosen to address our research objectives of describing practices, understanding perceptions and examining the relationships between institutional characteristics and trust. This design is known in social science methodology as an appropriate design for exploratory/explanatory study.

The purposive sampling technique is used to ensure that the respondents are knowledgeable decision makers, although this may be at the expense of generalizability.

But as we are interested in organizational practices, and not general population behavior, the tradeoff is not a big disadvantage. Bias was minimized through pilot testing, clarifying the survey, and standard statistical methods.

For the purpose of improving internal validity, we grouped the survey together in several domains that align directly with our research questions, namely governance, risk and controls. We sought to maintain reliability by consistently using Likert scales and will calculate the internal consistency (Cronbach's alpha) for multi-item constructs.

3.8. Sampling, Measurement, and Interpretation Considerations

The sample consisted of organizations that were selected as a purposive, non-probability sampling from professional networks that use clouds. Therefore, the findings and interpretations in this study are restricted to the surveyed organizations and cannot be generalized to the entire organizations in Bangladesh and policy level inferences are excluded. This sampling methodology may have created selection bias, with those cloud organizations that are more mature and have better governance awareness and compliance preparedness more likely to be sampled, leading to an apparent high level of governance maturity and control adoption.

Self-reported data was used to assess all key constructs (perceived risks, governance mechanisms, technical controls, and organizational trust) in a single collection, which may have led to common method variance and conceptual overlap between the constructs. Association, not causality found in the regression analysis could be due to a shared measurement context or conceptual proximity, not because of strong causal effects.

3.9. Limitations

Our methodology allows for rich insight, but the results are associational and there are some limitations:

- **Sampling Bias:** As for sampling method, we have applied non-probability (purposive) sampling and thus our sample may overrepresent more mature and cloud-savvy companies, and our results might not be generalizable across all Bangladeshi companies.
- **Self-report bias:** responses reflect self-reported practices, rather than actual practices, and participants may "over" report adoption of good practices.
- **Cross-Sectional Nature:** The design reflects perceptions and practices at one point in time and does not fully reflect on how perceptions and practices have changed over time, or on how perceptions and practices have caused changes.

4. Results

4.1. Reliability and Internal Consistency

The analysis emphasizes analytically informative and unexpected patterns, not a thorough description of expected practices. Cronbach's alpha was computed to determine the internal consistency of multi-item

constructs in the survey. All constructs have acceptable to good reliability, as indicated in Table 2, which is above the frequently used criterion of 0.70. Alpha values were not indicating redundancy across any construct,

suggesting a good level of internal consistency and breadth of the construct. The results suggest that all of the items in each construct are measuring the same underlying constructs.

Table 2: Internal Consistency of Survey Constructs.

Construct	Number of Items	Cronbach's Alpha (α)	Interpretation
Perceived Privacy Risk	5	0.81	Good
Governance Maturity	6	0.78	Acceptable
Technical Control Adoption	7	0.74	Acceptable
Trust in Cloud Service Providers	4	0.83	Good

4.2. Overall Findings: Risk Perception, Governance, and Technical Controls

Table 3 provides a summary of respondents' perceptions of the major potential risks associated with cloud privacy, as well as the presence of governance controls, technical controls, and trust-related controls within the organizations surveyed. The table below summarizes the average scores and percentages for risk perception and governance and technical safeguards adoption, giving an overview of how organizations are dealing with cloud privacy concerns. All these are descriptive of organization practices and attitudes towards the cloud data protection.

The findings show that organizations have a high level of concern about privacy risks related to cloud services, with misconfiguration, insider threats and key management risks being the most salient risks. The use of more sophisticated

technologies that can enhance privacy and confidential computing is limited, although baseline technical safeguards like encryption and key management services are well adopted. Governance practices are moderately mature: most organizations have formal governance structures and contractual protections with cloud providers, but compliance with international standards and werewolf practices of continuous auditing varies. For instance, trust in cloud service providers is moderate, meaning that mass adoption of technical controls does not necessarily lead to high levels of trust in the organization. Together, the results suggest that there is a mismatch between the security implementation at the surface level and the governance and assurance processes used at a deeper level, and that the organizational governance—more than technology—is the key to securing the cloud.

Table 3: Summary of Risk Perceptions, Governance Practices, and Technical Controls.

Dimension	Indicator	Value
Risk Perception (Mean, 1–5)	Misconfiguration Risk	4.2
	Insider Threat Risk	4.0
	Key Management Risk	3.9
	Regulatory / Compliance Risk	3.8
	Multi-Tenancy Risk	3.6
Governance Practices (% Adoption)	Formal Cloud Data Governance Framework	70%
	Shared Responsibility Matrix with CSP	55%
	Audit Rights in CSP Contracts	65%
	Breach Notification Clauses	60%
	ISO-Based Governance (27001/27018)	40–45%
Technical Controls & Trust	Encryption (At Rest / In Transit)	85% / 78%
	Dedicated Key Management Services	60%
	Advanced PETs (HE, MPC)	15%
	Trusted Execution Environments	10%
	Zero-Trust Architectures	30%
	External Audits Conducted	58%
	Trust in CSPs (Mean, 1–5)	3.6

4.3. Model Fit Summary

The overall regression model demonstrates strong explanatory power. As shown in the model summary (Table 4), the model explains 61% of the variance in organizational trust in cloud service providers ($R^2 = 0.61$; Adjusted $R^2 = 0.58$), indicating a substantial model fit for

applied organizational research. The moderate explained variance R^2 suggests that perceived privacy risks, governance mechanisms, and assurance practices jointly play a critical role in shaping trust in cloud environments within the Bangladeshi context.

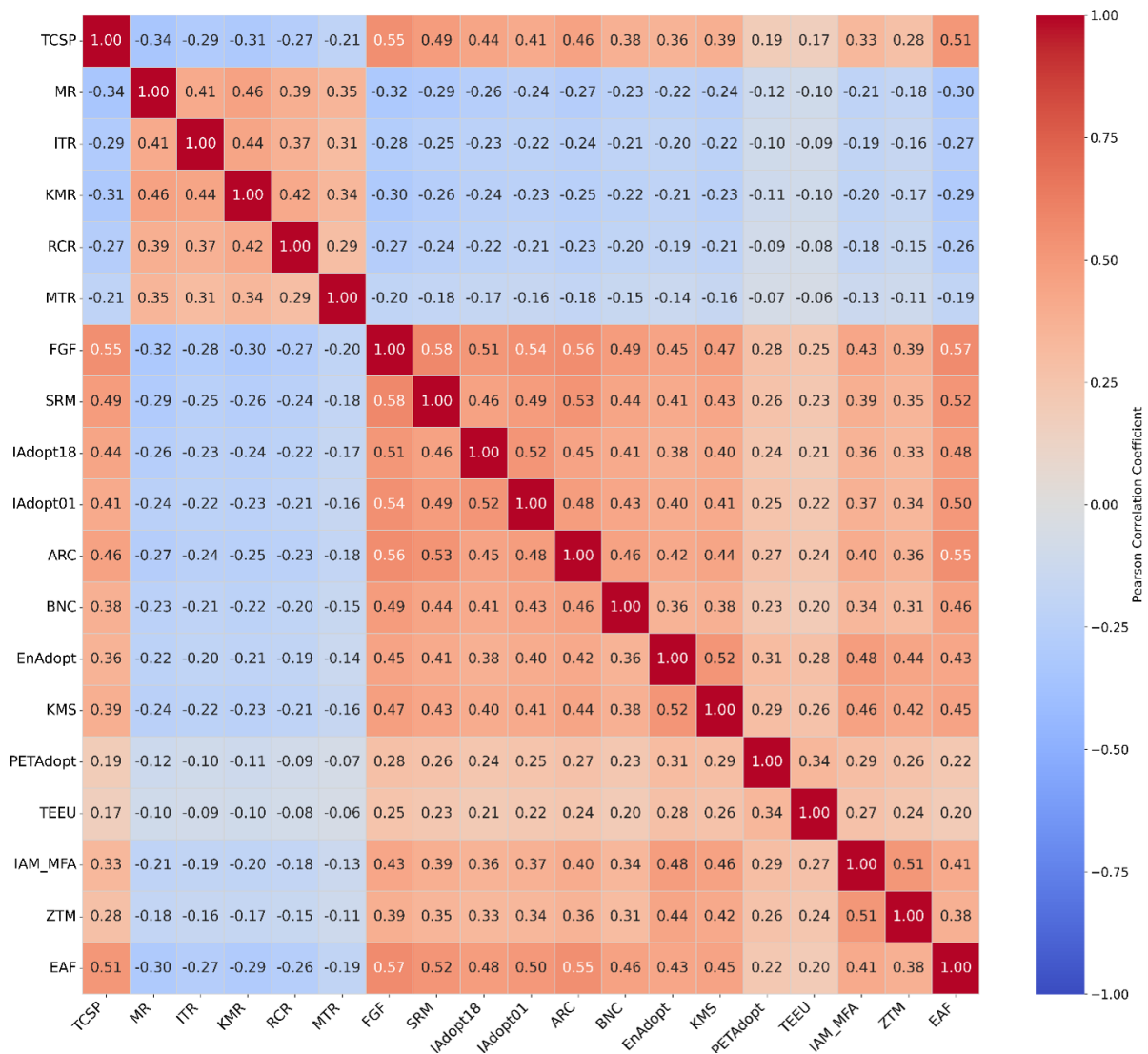
Table 4: Model fit summary.

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.781	0.610	0.580	0.49

4.4. Correlation Analysis

A bivariate correlation heatmap is provided in Figure 2 to show all the bivariate relationships among the variables measured. There are a number of obvious trends. The perceived vulnerabilities regarding privacy risks exhibit moderate to strong negative correlation with trust; that is, the higher perceived vulnerability the lower the confidence in cloud service providers particularly in misconfiguration risk, insider threat risk and key management risk. Third, governance-related variables such as the presence of a formal data-governance framework, shared responsibility matrices,

and audit-rights clauses are highly positively correlated with trust, highlighting how institutional and contractual arrangements can contribute to trust. Third, technical controls including encryption, identity and access management and key-management systems exhibit positive correlations, although comparatively less strong, indicating that technical safeguards are important, but not solely sufficient to account for the extent of trust. The adoption and maturity of the advanced privacy-enhancing technologies (e.g., homomorphic encryption, TEEs) are relatively low, demonstrated by relatively weaker correlations.

**Figure 2:** Correlation Heatmap.

4.5. Regression Analysis Summary

All measured variables were analyzed by correlation, but the regression model uses a subset of predictors which is theoretically motivated and statistically parsimonious.

This was done to prevent overfitting and multicollinearity, because of the small sample size ($n = 132$) and to provide sufficient statistical power. The selected variables are those that showed their salience in previous studies

and in the correlation analysis: perceived privacy risks, governance maturity and contractual accountability, and core technical assurance mechanisms. Conceptually similar variables and variables with low explanatory power were not included in the final model.

The results of the regression model (Table 5) show that governance and assurance mechanisms are the most significant factors influencing the trust in cloud service providers. A formal data-governance framework and regular external audits have the greatest positive

impact, underscoring the importance of accountability, oversight, and compliance signaling. Perceived privacy risks, however, particularly misconfiguration risk and key-management weaknesses, have significant negative impacts on trust, thus confirming that trust erosion is mainly due to fears of operational and control failures. Technical safeguards, including identity and access management and encryption also have positive impacts (albeit smaller), indicating that technology is not a primary, but secondary trust driver.

Table 5: Multiple Linear Regression Results.

Predictor	B	SE	β	t	p	95% CI (Lower, Upper)	VIF
(Constant)	1.12	0.34	—	3.29	0.001	[0.45, 1.79]	—
Misconfiguration Risk	−0.23	0.07	−0.21	−3.50	<0.001	[−0.37, −0.09]	2.10
Insider Threat Risk	−0.18	0.07	−0.15	−2.48	0.015	[−0.32, −0.04]	1.96
Key Management Risk	−0.20	0.07	−0.18	−2.71	0.008	[−0.35, −0.05]	2.28
Regulatory Compliance Risk	−0.14	0.06	−0.12	−2.32	0.022	[−0.26, −0.02]	1.87
Formal Governance Framework	0.41	0.08	0.34	4.86	<0.001	[0.25, 0.57]	2.94
Shared-Responsibility Matrix	0.26	0.08	0.19	3.17	0.002	[0.10, 0.42]	2.62
Audit Frequency	0.38	0.08	0.29	4.83	<0.001	[0.22, 0.54]	2.41
ISO/IEC 27018 Adoption	0.22	0.07	0.16	3.05	0.003	[0.08, 0.36]	2.18
Encryption Adoption	0.19	0.07	0.14	2.69	0.008	[0.05, 0.33]	2.07
IAM + MFA	0.17	0.07	0.13	2.48	0.015	[0.03, 0.31]	1.99

4.6. Subgroup Analysis by Industry, Organization Size, and Cloud Deployment Model

To explore whether cloud-privacy perceptions and practices vary across organizational contexts, we

conducted descriptive subgroup analyses based on industry sector, organization size, and cloud deployment model in table 8.

Table 6: Subgroup Comparison of Key Variables.

Subgroup	Regulatory Risk (Mean)	Governance Framework (%)	External Audit (%)	Trust in CSPs (Mean)
Industry Sector				
Banking / Financial	4.1	82%	75%	3.4
ICT / Technology	3.6	65%	48%	3.8
Utilities	3.9	70%	60%	3.5
Organization Size				
Small (<100 employees)	3.5	52%	40%	3.7
Medium (100–500)	3.8	68%	55%	3.6
Large (>500)	4.0	85%	78%	3.4
Cloud Deployment Model				
Public Cloud	3.6	60%	45%	3.8
Private Cloud	3.9	75%	65%	3.5
Hybrid Cloud	4.0	82%	72%	3.4

The results of the subgroups are meaningful. Financial institutions have the highest regulatory-risk perception and the highest level of governance adoption, indicating that they are likely to have more stringent compliance requirements. ICT companies have higher trust in cloud service providers, which may be because of their familiarity

with the technology and maturity of cloud. But it is not just about the size of the organisation; larger companies are more likely to have a formal governance structure and to conduct audits more frequently, although this does not necessarily translate to greater levels of trust as there may be an increased burden on compliance and risk awareness.

Thirdly, the intensity of governance is influenced by cloud deployment model. Hybrid and private cloud users say that they have more robust governance and audit controls, in line with greater awareness of importance of data localization and control. The analysis is descriptive as the study is exploratory and the size of the subgroups is not equal, so formal hypothesis testing is not conducted.

4.7. Associational Interpretation and Model Robustness

The association between the relationships reported here should be interpreted, not as causal, but rather associational. As the study is a cross-sectional and correlational study, regression results do not allow for causal inference with respect to the impact of governance maturity, audit practices and technical controls on organizational trust. Additionally, constructs are conceptually linked and can even overlap in part, such as in the case of governance mechanisms, audit practices and the construct of trust, which can lead to observed associations being amplified by the use of perceptual survey items.

To test the robustness of the results, alternative model specifications were explored by estimating regressions with smaller subsets of factors and dropping factors with high cross-correlations with the factors in the main specification. The direction and meaning of the main associations especially the positive association between governance maturity and organizational trust, were similar for these specifications, yet effect magnitudes differed. These findings do not appear to be confounded with a single model configuration but should be taken with a grain of salt as representative of models and patterns, not causal mechanisms.

5. Discussion

The findings are complex, showing a picture of how the organisation in Bangladesh deals with the tension between ambition and constraint, regulatory demand and capability, when it comes to cloud data privacy.

The regulatory pressures have led to a strong response in the high levels of governance and good practice in contracts. Bangladesh Bank (2023) has made it mandatory to classify data, perform regular audits, and establish responsibility matrices in the Cloud Guidelines. It seems that organizations tend to take these into account. This reflects the fact that regulation is not a mere formality, but a factor that affects cloud governance.

The PDPO, 2025, gives an added impetus. The introduction of notions about data subject rights, consent and security (including security around encryption) are driving organizations to formalize data governance (Jagonews24, 2025; The Daily Star, 2025).

The PDPO makes a point of holding organizations accountable for data breaches and sets forth robust security measures, so there is a definite incentive to do so - both legal and technical.

The empirical results are summarized in a five-phase cloud privacy risk management framework as shown in

Figure 3. This framework is not intended to be a theory, but rather an analytic and interpretive tool that describes the ways in which organizations surveyed have organized their approaches to privacy risk management in terms of governance, technical controls, and oversight activities. Its circular layout is indicative of the dynamic nature of cloud environments and regulatory frameworks like the Personal Data Protection Ordinance (PDPO).

The Assessment phase corresponds to the high-risk perception levels that were observed in the survey regarding misconfiguration, insider threats and key management vulnerabilities. The results of this regression analysis also suggest the presence of formal governance mechanisms, policies, and contractual safeguards factors which emerged as the strongest associates of organizational trust, and which are established in the Design phase. Encryption, identity and access management, and key management systems are just some of the technical controls that are employed to implement these decisions and were mentioned by most of the respondents in the Implementation phase.

Continuous Monitoring focuses on the on-going oversight, auditability and compliance assurance and this area shows some discrepancies in the level of maturity across the organizations. The Review phase focuses on the regular reviews of risks, controls and governance, accounting for new risks, regulatory changes and controls.

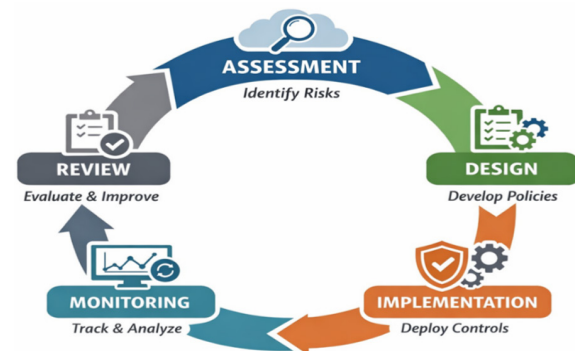


Figure 3: Five-phase Cloud Privacy Risk Management Framework.

The framework is conceptually embedded in institutional theory and IT governance literature that underline the institutionalization of governance structures and risk management routines when companies are facing regulatory pressure and normative standards, and industry expectations. In this light, controls and governance measures aimed at privacy are not just technical safeguards but are also institutional cues that affect inter-organizational trust. Assessment, design, implementation, monitoring and review are the same stages as those used in well-known governance cycles but are adapted here to describe the pattern of empirical observations of cloud privacy practices.

5.1. Governance Maturity as a Primary Driver of Trust

The empirical findings show that the strongest association

with the organizational trust in cloud service providers is governance maturity. Of technical controls, formal data-governance frameworks, shared-responsibility matrices and regular external audits are more strongly associated with trust than are the individual technical controls. This finding supports the idea that trust for cloud environments does not have to be of a technical nature, but it is an institutional/managerial construct. This is particularly a remarkable discovery in the context of Bangladesh. Accountability, auditability and contractual clarity is clearly emphasized in the Bangladesh Bank Guidelines on Cloud Computing and the Ordinance on Personal Data Protection (PDPO). Governance-first strategies are reinforced by organizations that fit these requirements, which seem to have a better chance of building trust relationships with cloud providers. These interpretations are only applicable to the surveyed organizations and should be taken as a representation of association and not a cause-and-effect relationship.

5.2. Risk Perception and Trust Erosion

The analysis also shows that there is a negative correlation between the perceived privacy risks and trust: the less trust, the less perceived privacy risk. Other risks such as misconfiguration risk, insider threat risk and key management weaknesses also show strong negative correlation with trust, indicating that organizations are still very vulnerable to failure and control gaps in the cloud environment. The results indicated that trust is not only established via the assurance mechanisms but also can be easily destroyed by the sense of unresolved vulnerabilities. This trend underscores the need for constant monitoring of risk, but does not allow for the determination of causality, due to its cross-sectional nature.

5.3. Technology Adoption Gaps and Practical Constraints

The study shows that many of those basic technical controls, including encryption, identity-and-access management, are becoming common practice, but there is less adoption of advanced privacy-enhancing technologies (PETs) and confidential computing solutions. The relatively low association with trust might be because they are in their early stage of development and/or because of the limitations of the organizations to which the survey was sent. There are probably some obstacles in terms of cost, lack of skills, and ROI. This implies that there is a gap between advanced technologies and governance and compliance mechanisms that immediately provide tangible assurance benefits.

5.4. Practical and Theoretical Implications

The findings have important practical and theoretical implications. Practically, they suggest that organizations should prioritize governance maturity by establishing formal cloud governance frameworks, clearly defining shared responsibilities with cloud service providers,

conducting regular external audits, and strengthening compliance with standards such as ISO/IEC 27018. While foundational technical controls, including encryption and identity and access management, remain essential, governance mechanisms appear to play a more influential role in building organizational trust. Policymakers may also use these findings to support the effective implementation of the Personal Data Protection Ordinance (PDPO) through stronger regulatory guidance and capacity-building initiatives. Theoretically, the study extends institutional theory and IT governance literature by demonstrating that organizational trust in cloud service providers is shaped not only by technical safeguards but also by governance structures and institutional accountability. Furthermore, the proposed Five-Phase Cloud Privacy Risk Management Framework provides an empirically informed conceptual model that can guide future research on cloud privacy governance, particularly in developing-country contexts.

6. Limitations and Future Research

This study's findings and the proposed five-phase cloud privacy risk management framework are subject to several limitations. First, the framework is a descriptive, empirically informed construct rather than a formally validated theoretical model. It synthesizes observed associations based on existing governance cycles and should not be viewed as a prescriptive standard.

Second, the use of a cross-sectional survey with purposive, non-probability sampling limits statistical generalizability. Since respondents were drawn from professional networks of existing cloud users in Bangladesh, the results reflect specific organizational experiences rather than the broader market. This recruitment strategy introduces potential selection bias, as cloud-mature firms with higher governance awareness were more likely to participate.

Third, the reliance on self-reported, single-respondent data introduces the risk of common method variance. Measures for perceived risk, governance, and trust may suffer from perceptual overlap, as objective metrics were not utilized. Consequently, the analysis identifies associational rather than causal relationships; the high explained variance in the trust model likely reflects conceptual proximity among constructs rather than definitive causality.

Future research should address these gaps by employing probabilistic sampling and longitudinal or multi-source data to mitigate bias. Additionally, sector-specific analyses and robustness checks using alternative model specifications would help further validate and refine the framework across diverse global and industrial contexts.

7. Conclusion

In sum, the organizations surveyed in Bangladesh are increasingly aware of and responsive to cloud data privacy risks. Their adoption of governance frameworks and encryption is strong, driven in part by regulatory mandates but advanced privacy technologies like PETs

and TEEs lag behind due to cost, complexity, and capacity gaps. Trust in cloud service providers is built not just through technology, but through governance, audits, and external assurance.

The Personal Data Protection Ordinance, 2025 and Bangladesh Bank's Cloud Guidelines are powerful levers for change: organizations that align with these regulations, invest in structured governance, and systematically enhance technical controls will likely both reduce risk and gain stakeholder trust.

Future work should focus on pilot implementations of advanced privacy technologies, trust-as-a-service models, and capacity-building initiatives to close the gap between regulatory ambition and practical adoption.

References

- Abdulsalam, Y. S., & Hedabou, M. (2021). Security and privacy in cloud computing: technical review. *Future Internet*, 14(1), 11. <https://doi.org/10.3390/fi14010011>
- Abed, Y., & Chavan, M. (2019). The challenges of institutional distance: Data privacy issues in cloud computing. *Science, Technology and Society*, 24(1), 161-181. <https://doi.org/10.1177/0971721818806088>
- Agrawal, D., El Abbadi, A., & Wang, S. (2012). Secure and privacy-preserving data services in the cloud: A data centric view. *Proceedings of the VLDB Endowment*, 5(12), 2028-2029. <https://doi.org/10.14778/2367502.2367569>
- Akhtar, S.I., Rauf, A., Abbas, H. *et al.* Compliance and feedback based model to measure cloud trustworthiness for hosting digital twins. *J Cloud Comp.*, 13, 132 (2024). <https://doi.org/10.1186/s13677-024-00690-0>
- AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & security*, 99, 102030. <https://doi.org/10.1016/j.cose.2020.102030>
- Alsmadi, D., Halawani, M., Prybutok, V., & Al-Smadi, R. (2022). Intention, trust and risks as core determinants of cloud computing usage behavior. *Journal of Systems and Information Technology*, 24(3), 178-201. <https://doi.org/10.1108/JSIT-09-2020-0180>
- Bangladesh Bank. (2023). *Guidelines on Cloud Computing*. BRPD Circular No. 05, 16 March 2023. Available: <https://share.google/kn74AZ3RqYswXWQM> [Accessed: Dec. 18, 2025].
- Calder, A. (2021). *The EU data protection code of conduct for cloud service providers: a guide to compliance*.
- Chauhan, M., & Shiaeles, S. (2023). An analysis of cloud security frameworks, problems and proposed solutions. *Network*, 3(3), 422-450. <https://doi.org/10.3390/network3030018>
- De Hert, P., Papakonstantinou, V., & Kamara, I. (2016). The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection. *Computer Law & Security Review*, 32(1), 16-30. <https://doi.org/10.1016/j.clsr.2015.12.005>
- Gangwar, H., Date, H., & Ramaswamy, R. (2015). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. *Journal of enterprise information management*, 28(1), 107-130. <https://doi.org/10.1108/JEIM-08-2013-0065>
- Garrison, G., Rebman Jr, C. M., & Kim, S. H. (2018). An identification of factors motivating individuals' use of cloud-based services. *Journal of Computer Information Systems*, 58(1), 19-29. <https://doi.org/10.1080/08874417.2016.1180653>
- Gholami, A., & Laure, E. (2016). *Security and privacy of sensitive data in cloud computing: a survey of recent developments*. <https://doi.org/10.48550/arXiv.1601.01498>
- Gupta K. P. (2025). Technology Adoption: Evidence from an E-Government Cloud Service. *Foresight and STI Governance*, 19(1), 93-103. <https://doi.org/10.17323/fstg.2025.24832>
- Han, Y., Wang, Y., Wu, L., Feng, H., Wu, X., & Li, R. (2025). Survey of privacy-preserving data aggregation schemes in smart grid. *Journal of King Saud University Computer and Information Sciences*, 37(9), 263. <https://doi.org/10.1007/s44443-025-00179-z>
- Hanif, M. S., Khurshid, A., Kulibaba, D., & Sajid, A. (2025). Adoption and Actual Usage of SaaS-Based Cloud Applications Among the Swedish SMEs—A TAM-TOE Integrated Perspective. *Human Behavior and Emerging Technologies*, 2025(1), 2730400. <https://doi.org/10.1155/hbe2/2730400>
- Jagonews24. (2025, October 9). Cabinet nods Personal Data Protection Ordinance 2025. *Jagonews24*. Available: <https://www.jagonews24.com/en/national/news/86241>. [Accessed: Dec. 18, 2025].
- Rahmika, A. R., Muhammad Akbar, Deni Luvi Jayanto, & Joshua Reska Bu'tu. (2025). Cloud Governance Frameworks: CIA-Based Security and Compliance. *Journal of Embedded Systems, Security and Intelligent Systems*, 6(3), 379-389.
- Silva, P., Monteiro, E., & Simoes, P. (2021). Privacy in the cloud: A survey of existing solutions and research challenges. *IEEE access*, 9, 10473-10497. <https://doi.org/10.1109/ACCESS.2021.3049599>
- Soofi, A. A., Khan, M. I., & Amin, F. E. (2017). A review on data security in cloud computing. *International Journal of Computer Applications*, 96(2), 95-96. DOI:10.5120/16338-5625
- Sprague, Robert, Cloud Privacy: Normative Standards Needed to Foster Innovation (June 1, 2010). Department of Commerce Internet Policy Task Force, Information Privacy and Innovation in the Internet Economy, Docket No. 100402174-0175-01, Available at SSRN: <http://dx.doi.org/10.2139/ssrn.1585376>
- The Daily Star. (2025, October 9). Shielding personal data: Govt brings big tech under local courts' purview. *The Daily Star*. Available: <https://www.thedailystar.net/news/bangladesh/news/shielding-personal-data-govt-brings-big-tech-under-m-4006206>. [Accessed:

Dec. 18, 2025].
Turan, F., Roy, S. S., & Verbaauwhede, I. (2020). HEAWS:
An accelerator for homomorphic encryption on the

Amazon AWS FPGA. *IEEE Transactions on Computers*,
69(8), 1185-1196. <https://doi.org/10.1109/TC.2020.2988765>