Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 5, 2026

IMPACT OF BLOCKCHAIN TECHNOLOGY ON DATA PRIVACY AND TRUST IN CLOUD COMPUTING

Zeeshan Ali
RESEARCH SCHOLAR
EMAIL: *Marizeeshan962@Gmail.Com*

DOI:- https://doi.org/10.5281/zenodo.20528753

Keywords
Blockchain technology, Cloud computing, Data privacy, Trust, PLS-SEM.

Article History
Received: 06 May, 2026
Accepted: 27 May, 2026
Published: 30 May, 2026

Corresponding Author: *

Zeeshan Ali

Abstract

This research aims to explore how blockchain technology affects data privacy and trust in Cloud Computing. While the cloud offers organizations and users the promise of flexible, scalable, and cost-effective digital services, cloud users and organizations still have concerns about control of their data, unauthorized access, privacy violations, and trust in cloud service providers. This study aims to examine the potential of blockchain technology to enhance perceived data privacy and trust in the cloud-based context. The research design used in this study was quantitative. A structured questionnaire was used to collect primary data from 265 respondents. Data privacy and data trust were conceptualized as dependent variables, and blockchain technology as an independent variable. The analysis of the collected data was carried out using the method of Partial Least Squares Structural Equation Modeling (PLS-SEM), which allowed us to assess the measurement model and the structural relationships between the models. The study suggests that the impact of blockchain technology on data privacy and trust in cloud computing is positive and significant. With the decentralization, transparency, immutability, traceability, and cryptographic verification that are expected to be hallmarks of the blockchain, issues of privacy are likely to diminish, and users will have increased confidence in cloud-based systems. This study adds to the literature of cloud computing and blockchain, as it empirically investigates an important, but simple model of blockchain technology with regard to data privacy and trust. The study offers insights from primary data and real-world implications for cloud service providers, IT managers, and other organizations looking to enhance the privacy protection and trust of their cloud-based services and solutions via blockchain technology.

1. Introduction

Cloud computing is one of the most significant digital infrastructure elements used by modern organizations, enabling users to store, process, and access data via internet-based platforms in addition to relying on local hardware and internal servers (Sunyaev, 2024). It is scalable, flexible, cost-effective, remotely accessible, and accelerates digital transformation (Walsh et al., 2026). Cloud systems have become essential for organizations in various sectors, such as banking, education, healthcare, retail, logistics, and public administration, to handle sensitive data and provide digital services (Yandamuri, 2026). In the context of the broader digital economy, new technologies like artificial intelligence, digitalization, cloud computing, and blockchain are playing a crucial role in driving change, efficiency, and innovation within organizations (Bohio et al., 2025; Naeem et al., 2025; Shahab et al., 2025). These benefits come with significant challenges, however, in terms of data privacy and trust in cloud computing. Direct control of information is limited when the information is stored on cloud platforms, and the responsibility for security shifts to the cloud service providers. This situation only adds to the question of who can access the data, how the data is stored, if there is a possibility for unauthorized changes, and if the service provider can be fully trusted.

Cloud computing is a highly debated technology for business due to the sensitive nature of information that users and organizations wish to place in the cloud, such as personal, financial, operational, and strategic information. Potential privacy threats can include unauthorized access, weak authentication, insider misuse, inadequate access control, data leakage, cyberattacks, lack of transparency, and accountability structures. According to Ali et al. (2026), the security threats in cloud computing encompass a wide array of potential vulnerabilities, making comprehensive information security risk assessment essential for managing vulnerabilities to ensure the protection of data and safeguard the integrity of cloud-based operations. In the same vein, Asheshemi and Adawaren (2026) highlighted insider threats and data breaches as key challenges in financial cloud systems, particularly when dealing

with sensitive customer and organizational data. These concerns are more significant if cloud users do not have complete visibility into the internal security measures of cloud service providers. The effectiveness of privacy protection mechanisms is therefore important for influencing users' willingness to trust the use of cloud-based technologies.

The other significant challenge in this context is trust, as users of the cloud rely on third parties with regard to data storage, data processing, service continuity, and protection of the cloud system. With centralized, complex, and less transparent cloud environments, it becomes challenging to trust. Transparency, reliability, technological capabilities, and responsible data governance are closely related to trust in digital transformation contexts (Walsh et al., 2026). It is also shown that in studies on digital technologies, the confidence of users increases when the organizations use advanced digital systems in a responsible and transparent manner (Naeem et al., 2023; Shaikh et al., 2025). With cloud computing, users may be reluctant to fully comply with cloud services if they think their data may be misused, altered, accessed without permission, or inadequately protected. So, not only is trust a technical challenge, but a managerial and relational challenge as well. To achieve the confidence of users, cloud service providers need to show reliability, accountability, transparency, and security.

Blockchain technology is now a potential remedy to privacy and trust issues in cloud computing. The blockchain is a distributed ledger technology that maintains records on decentralized nodes and employs cryptographic methods to verify, validate, and secure transactions. It offers decentralization, immutability, transparency, traceability, auditability, and cryptographic security. The qualities make blockchain applicable to cloud computing, and contribute to decreasing reliance on a single central authority, tracking data activities and users, enhancing access control, and increasing trust in data integrity. Asheshemi and Adawaren (2026) proposed using blockchain-based ZTF to reduce the likelihood of data breaches and insider threats in cloud financial systems. This means that blockchain can lend greater security governance in which data

privacy and trust matter greatly.

Blockchain's ability to combine with cloud computing can help enhance privacy data by delivering tamper-resistant records, decentralized verification, clear access logs, and more robust identity and access management. In contrast to a single entity with control of the cloud, blockchain can enable distributed validation and provide an audit trail of data transactions. This can assist users in determining if data has been accessed, changed, or shared. Moreover, blockchain-based access control processes can also allow for automated access control and the minimization of data manipulation by third parties. Recent studies indicate that scaling cloud systems for intelligent systems also needs to improve the security, governance, and decision-support approaches applied to safeguard data and optimize the operations of the industry (Yandamuri, 2026). As such, blockchain can enhance the technical and psychological mechanisms underlying the data's privacy in cloud environments.

By offering transparency, verifiability, and accountability, blockchain technology can enhance trust in cloud computing by making the activities of the cloud more transparent and verifiable. Traditional clouds are often lacking in transparency regarding what happens to users' data when it is uploaded to the clouds. Blockchain technology can help alleviate this uncertainty by securely and traceably documenting access to and transactions with the cloud. This improves users' ability to verify data-handling practices and reduces the need to rely entirely on cloud service providers' claims. Research on digital transformation indicates that in order to create reliable technology-enabled systems, it is crucial that everything is connected, transparent, and scalable (Walsh et al., 2026). Likewise, research on digitalization and Industry 4.0 indicates that the use of new technology can help organizations achieve better outcomes when it is coupled with strong governance and operational processes (Bohio et al., 2025; Naeem et al., 2025).

Previous works have explored the technical implications of blockchain in cloud security, privacy, access control, and trust management, but there has been little empirical work that looks at, from a primary data perspective, how blockchain impacts users' perceptions of data privacy

and trust in cloud computing. There are a number of existing studies that are conceptual, technical, review, or architecture-oriented. Therefore, there is a need for quantitative evidence showing whether blockchain technology has a meaningful impact on data privacy and trust for users and professionals. The previous research on digital transformation, artificial intelligence, fintech, and technology-based organizational systems further suggests empirical exploration of new technologies in a specific organizational and social setting (Anser et al., 2025; Naeem et al., 2023; Shaikh et al., 2025). The current study aims to solve this problem by conducting research using primary data obtained from 265 respondents and Partial Least Squares Structural Equation Modeling.

Thus, the aim of this study is to explore the effect of blockchain technology on data privacy and trust in cloud computing. Blockchain technology as the independent variable and Data privacy and trust as the dependent variable. This study is an addition to the literature because it offers empirical support for the perception of privacy and trust in cloud environments with the use of blockchain. It also has practical applications for cloud service providers, IT managers, technologists, and organizations looking to enhance user trust in cloud-based systems by implementing blockchain solutions.

2. Literature review and hypotheses development

2.1 Blockchain technology

Blockchain technology is a decentralized and distributed ledger system, where digital transactions and records are distributed across multiple network nodes instead of being managed by a single central entity. Consensus mechanisms are used to validate each transaction, and the validated transactions are added to blocks, which are connected to each other through cryptographic hashes. This design makes it harder to modify, alter, or delete blockchain records without verification, as the network checks them. The key characteristics of blockchain are decentralization, transparency, immutability, traceability, auditability, cryptographic security, and peer-to-peer verification. The properties of blockchain make it appropriate to enhance security, privacy, and trust in digital environments

where data is shared between a number of users, organizations, and service providers.

Cloud computing has made blockchain technology more and more a tool to combat the shortcomings of centralized cloud systems. Typically, cloud computing relies on an external service provider to store, process, control access to, and manage data. This approach is flexible and scalable, but it also raises issues of data ownership, unauthorized access, lack of transparency, and reliance on cloud service providers (Sunyaev, 2024). A decentralized verification layer can alleviate these concerns by using blockchain to audit the activities related to data, making them transparent and tamper-proof. Blockchain is also proving to be relevant in the context of secure governance in financial cloud systems, with the introduction of zero-trust based on blockchain proposed as a solution to decrease insider threats and data breaches (Asheshemi & Adawaren, 2026). Thus, blockchain is not just a technical solution but also a governance tool that can enhance data control, transparency, and reliability in cloud computing environments.

2.2 Data privacy in cloud computing

Data privacy is the protection of personal information, organizational information, and sensitive information from unauthorized access, misuse, disclosure, manipulation, and unauthorized sharing. With cloud computing, data privacy becomes a significant point of concern since the user accesses data from a remote server, which is managed by a third-party cloud services provider. This puts data ownership apart from data control. While users might have ownership of the data, cloud providers typically control the infrastructure on which the data is stored and processed. This means that users often don't know what is happening with their data, who has access to it, if it is moved to other locations, or how it is secured from internal and external threats.

Cloud computing privacy threats are data leakage, weak authentication, insider threats, lack of transparency in data processing, insecure application programming interfaces, and unauthorized access. According to Ali et al. (2026), information security risk assessment in cloud computing is essential since cloud computing is composed of multiple vulnerabilities that can impact the

confidentiality, integrity, and availability of information. Additionally, Asheshemi and Adawaren (2026) noted that insider threats and data breaches can have a profound impact on privacy in financial cloud systems. In industries where data privacy is paramount, like healthcare, finance, education, government, and e-commerce, these concerns are particularly relevant. If users feel that cloud platforms are not sufficiently secure to protect their data, they might either decrease the amount of cloud use or not share data through cloud-based systems that store sensitive data.

Technical measures are not the only ones that ensure data privacy in the cloud: transparency and accountability measures also play a key role. When users can confirm access, monitor data movement, and know how their data is safeguarded, they are more likely to feel that their data is private. When it comes to traditional cloud systems, they are a challenge in this regard, as they are mostly provider-controlled and centralized. One of the potential solutions for this limitation provided by blockchain is the ability to generate secure, transparent, and tamper-proof data transactions. By using decentralized verification, cryptographic protection, and an immutable audit trail, blockchain can enhance users' trust that cloud data cannot be tampered with without detection.

2.3 Trust in cloud computing

Trust in cloud computing is the confidence placed in cloud service providers, cloud platforms, and data management processes in the cloud. Trust translates to an expectation that cloud services will be both reliable and secure, will provide service integrity, and will behave responsibly and transparently in the protection of user data. Cloud environments rely on trust, as users rely on external providers for data storage, processing, backup and recovery, and security. However, users are unable to directly manage infrastructure and have to depend on the competence, honesty, reliability, and accountability of the provider.

Trust has been a much-talked-about issue in cloud adoption and the ongoing usage of cloud. Cloud computing can facilitate the process of digital transformation by providing flexible, scalable, and connected systems that allow users to benefit from cloud technology; however, it relies on user

trust in cloud-based platforms (Sunyaev, 2024; Walsh et al., 2026). In the wider field of digital transformation studies, technological trust is linked to the reliability of the infrastructure, to responsible digital practices, and to governance structures (Bohio et al., 2025; Naeem et al., 2025). Likewise, research on AI and digital systems reveals that trust in AI technology is linked to user confidence in system reliability, transparency, and responsible use (Anser et al., 2025; Naeem et al., 2023). Thus, both technical security and accountability, as can be seen, are necessary for trust to be built in cloud computing.

By allowing blockchain technology to help verify data-related activities, cloud computing could be enhanced to build trust amongst users, rather than relying on the claims of the provider. Blockchain-based systems can be used to log transactions, access events, interactions with services, and even data sharing activities in a transparent and immutable ledger. This increases accountability and minimizes uncertainty. If cloud activities can be confirmed by users on blockchain, then trust is not dependent on promises made by cloud providers but has been reinforced by technology. Thus, the blockchain technology can transform the cloud trust model from provider-centric to technology-driven verification.

2.4 Blockchain technology and data privacy

Blockchain technology holds the potential to positively impact data privacy in cloud computing through data control, transparency, access verification, and data tamper resistance. Traditional cloud systems have been plagued with privacy issues due to the inability to fully control data storage, access, modification, and sharing that cloud users have. Blockchain can solve this by providing a decentralized and unalterable data-related transactional record. Upon verification and inclusion on the blockchain, it is hard to change without the consensus of the network. This allows for the protection of data in the cloud from unauthorized changes and increases confidence in data integrity.

The privacy-enhancing function of blockchain is also associated with cryptographic techniques. Blockchain relies on a variety of cryptographic tools, including consensus mechanisms, digital

signatures, and public-private key systems, to verify transactions and safeguard data. These mechanisms can help to ensure secure access control and identity verification in cloud settings. For instance, access permissions can be set using smart contracts on the blockchain, and privacy rules can be automatically enforced. This minimizes reliance on manual authorization and minimizes the risk of unauthorized sharing of data. Asheshemi and Adawaren (2026) demonstrated that the implementation of the zero trust paradigm in cloud systems with the help of blockchain technology can help to reduce insider threats and data breaches. In the same way, Ali et al. (2026) have pointed out that data confidentiality, unauthorized access, and cyber risks are all closely associated with data privacy and should be included in the assessment of the security risks in cloud computing.

Cloud computing has the ability to use blockchain to enhance privacy due to its auditability. Auditability enables organizations and users to know who accessed data, when it was accessed, and if it was altered. Having said this, it is crucial to not only make sure that data cannot be accessed by others without authorization, but also to establish accountability when data is accessed or processed. Cloud-based intelligent systems are also scalable, thus need to support decision making and digital optimization, along with securing the information (Yandamuri, 2026). So, blockchain technology can improve the perception of users that the data in the cloud is secure, managed, and less susceptible to unauthorized manipulation.

From the above discussion, it is clear that the use of blockchain technology in cloud computing is likely to increase the privacy of data by offering decentralization, cryptographic security, immutability, traceability of access, and the application of smart contracts for granting permissions. It is therefore hypothesized that:

H1. Blockchain technology has a significant impact on data privacy in cloud computing.

2.5 Blockchain technology and trust

Blockchain technology has the potential to enhance transparency, accountability, reliability, and verifiability, thereby positively impacting trust in cloud computing. Trusted interactions in a cloud computing environment are reduced due

to the lack of visibility of users over the provider's controlled systems. They might not be aware if their data has been accessed without their permission, if service providers secure it properly, or if the data stored stays unchanged. Blockchain technology can eliminate the uncertainty by offering a decentralized and transparent ledger on which cloud-related activities can be recorded and verified.

Users' confidence in the system is enhanced when they are able to confirm the actions of the system rather than relying on institutional assurances. Blockchain enables this verification, as transactions are visible and hard to manipulate. Transparency, connectivity, and reliable infrastructure are important characteristics of digital systems in the context of digital transformation to gain user confidence (Walsh et al., 2026). Research into digitalization and Industry 4.0 also indicates that operational and governance systems that support digitalization technologies can boost organizational trust and performance (Bohio et al., 2025; Naeem et al., 2025). Thus, blockchain can be used as a technology-based trust-building process in cloud computing.

The blockchain also promotes trust by eliminating the need for a single central authority. With traditional cloud computing, a high level of dependency is placed on service providers to handle data, access control, and security guarantees. This results in a trust imbalance as providers cannot be fully verified by users. Blockchain helps this imbalance by decentralizing the validation process. Furthermore, blockchain can help to build trust via smart contracts that automatically follow pre-established rules and minimize human participation in cloud transactions. Smart contracts can be used to create service conditions, access control, and data sharing agreements. If cloud users are confident that rules are being enforced automatically and transparently, they might be willing to trust the system. If they think rules are being enforced without their own involvement and in an understandable way, they may be more willing to trust the system. Therefore, blockchain can enhance trust beyond the technical security aspects by also bolstering perceptions of fairness, transparency, and accountability.

From the above discussion, it is evident that the technology of blockchain can be expected to increase transparency, decentralization, auditability, traceability, and verification of cloud computing, thereby bringing trust to cloud computing. Based on the above, the following is hypothesized:

H2. Blockchain technology has a significant impact on trust in cloud computing.

2.6 Conceptual framework

The conceptual framework of this study is presented in Figure I below.

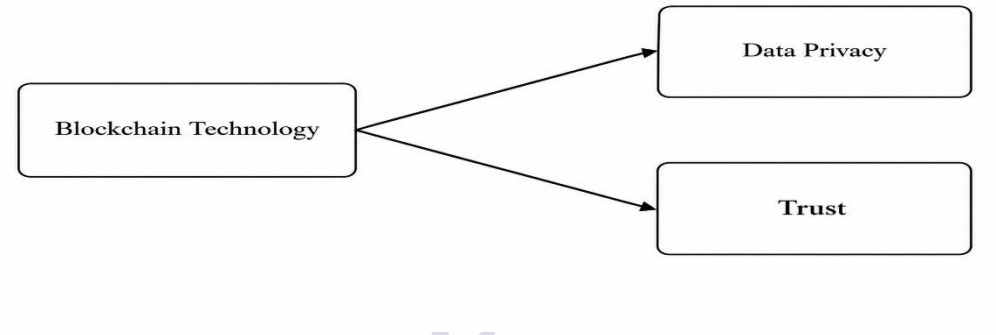

Figure I

3. Methodology

3.1 Research design

The design of this research is quantitative, which was used to study the effects of blockchain technology on data privacy and trust in cloud computing. A quantitative approach was deemed appropriate as the purpose of the study was to test hypothesized relationships among clearly defined latent constructs. The study design was a cross-sectional survey design, with data being gathered from the respondents at a single point in time. Information systems and technology adoption research is characterized by the use of cross-sectional survey designs, as they enable researchers to gain an understanding of users' perceptions, attitudes, and behavioral evaluations of emerging technology in real organizational and digital settings.

The study was of an explanatory type, to explain the impact of blockchain technology on two key outcomes in cloud computing: data privacy and trust. The data privacy and trust were the dependent variables, and the blockchain technology was the independent variable. The use of a structured questionnaire enabled the researcher to collect standardized responses from a relatively large number of

respondents. This approach was also appropriate for statistical testing using the Partial Least Squares Structural Equation Modeling (PLS-SEM), which can be used to test complex relationships between latent constructs and measure and test both measurement and structural models (Hair et al., 2021).

3.2 Population and sample

This study aimed to target the population of people who have knowledge, awareness, or experience of cloud computing, digital platforms, data storage systems, blockchain technology, or IT-based services. Professionals, students, IT users, cloud service users, and those in technology-related or digitally enabled environments were among the respondents. The study was based on perceptions of blockchain technology and data privacy, as well as trust in cloud computing, so basic knowledge of digital technologies was deemed a suitable condition for respondents.

A sample of 265 respondents was used to collect primary data. The sample size was found to be satisfactory for PLS-SEM analysis as the PLS-SEM can be applied for relatively small to medium-sized samples and is suitable for prediction-oriented research (Hair et al., 2021). Furthermore, the model of the study consisted of one independent variable and two dependent variables, so the sample size was adequate to estimate the model relationships. The study applied a non-probability purposive sampling technique because the respondents who were selected were relevant to the context of the study and could provide meaningful responses concerning the use of blockchain technology and cloud computing. The use of purposive sampling in technology and management research is frequently used when the research requires individuals who possess special knowledge or experience in a topic.

3.3 Data collection procedure

A structured questionnaire was used to collect data. The questionnaire was aimed at capturing the perceptions of blockchain technology, data privacy, and trust in cloud computing among the respondents. Before data collection, the study's purpose was explained to the respondents. The respondents were asked if they wanted to participate in the study, and their responses would be used only for academic research. Respondents' confidentiality and

anonymity were respected during the research process.

The questionnaire was sent to people who knew about cloud-based services, online data storage, digital platforms, or blockchain-related concepts. Participants were asked to give their honest answers, based on their understanding and experiences. The responses were screened to eliminate those that were not complete or appropriate, leaving 265 valid responses for final analysis. Responses that were incomplete, inconsistent, or unusable were not included in the data set to ensure the quality and reliability of the analysis.

3.4 Measurement of constructs

The study was conducted to measure three main constructs: blockchain technology, data privacy, and trust. The independent variable measured was the blockchain technology, and the dependent variables measured were data privacy and trust. All constructs were assessed with a set of multiple items based on previous studies on the constructs of blockchain, cloud computing, data security, privacy, and trust. The use of pre-established measurement items enhances the content validity of the questionnaire, and the measures of the constructs are in accordance with the academic literature.

A collection of items, representing the essence of blockchain properties, decentralization, translucidities', immutability, traceability, cryptographic security, and secure data verifications, was used to assess blockchain technology. The dimensions represent the fundamental technological characteristics of blockchain that can be relevant to environments that use cloud computing. Data privacy is measured by questions about perceived protection of personal or organizational data, prevention of unauthorized access, control over data sharing, secure handling of data, and trust in data privacy mechanisms. Trust was assessed by questions about trust in the reliability of cloud services, security, transparency, accountability, and that cloud systems with blockchain would provide protection for the interests of users.

Every item of the questionnaire was assessed on a 5-point Likert scale, from 1 = strongly disagree to 5 = strongly agree. The study investigated the perception and attitude of the respondents to the privacy and trust of cloud computing enabled by

blockchain, so a Likert scale was used. Multiple-item scales also helped to capture the construct's latent nature and helped to enhance the reliability of measurement.

3.5 Questionnaire design

The questionnaire consisted of two main sections. The first section included demographic information about the respondents, such as gender, age, education, experience, and professional or academic background. These demographic items were included to describe the sample characteristics and provide a clearer understanding of the respondents who participated in the study.

The second section included measurement items related to the three research constructs. The items were developed and adapted based on the literature on blockchain technology, cloud computing, data privacy, and trust. Blockchain technology items focused on the perceived ability of blockchain to provide decentralized, transparent, immutable, and secure data management. Data privacy items focused on the perceived protection, control, and confidentiality of data in cloud computing. Trust items focused on respondents' confidence in the reliability, transparency, and accountability of blockchain-supported cloud systems.

The questionnaire was reviewed to ensure clarity, relevance, and simplicity of language. The wording of the items was kept understandable so that respondents with different levels of technical knowledge could answer accurately. This helped reduce ambiguity and response bias.

3.6 Data analysis technique

The collected data were analyzed using Partial Least Squares Structural Equation Modeling. PLS-SEM was selected because it is suitable for prediction-oriented research and for testing relationships among latent constructs measured through multiple indicators. PLS-SEM is also appropriate when the research model is relatively new or when the objective is to maximize the explained variance of the dependent variables (Hair et al., 2021). Since this study examined how blockchain technology predicts data privacy and trust in cloud computing, PLS-SEM was considered suitable for the analysis.

The data analysis followed a two-stage approach. First, the measurement model was assessed to examine the reliability and validity of the constructs. Second, the

structural model was assessed to test the hypothesized relationships among blockchain technology, data privacy, and trust. This two-stage approach is recommended in PLS-SEM because researchers must first establish that the measurement model is reliable and valid before interpreting structural relationships (Hair et al., 2021; Henseler et al., 2015).

3.7 Measurement model assessment

The measurement model was evaluated through indicator reliability, internal consistency reliability, convergent validity, and discriminant validity. Indicator reliability was assessed through outer loadings. Items with factor loadings of 0.70 or above were considered acceptable because they indicate that the item explains a sufficient amount of variance in the underlying construct. However, items with slightly lower loadings may be retained if their removal does not improve composite reliability or average variance extracted (Hair et al., 2021).

Internal consistency reliability was assessed using Cronbach's alpha and composite reliability. Cronbach's alpha values above 0.70 indicate acceptable reliability, while composite reliability values between 0.70 and 0.95 are generally considered satisfactory. Composite reliability was also examined because it is considered more suitable for PLS-SEM than Cronbach's alpha, as it does not assume equal indicator loadings.

Convergent validity was assessed through average variance extracted. AVE values of 0.50 or above indicate that a construct explains at least 50 percent of the variance in its indicators. Therefore, AVE was used to confirm whether the measurement items adequately represented their respective constructs. Discriminant validity was assessed using the Fornell-Larcker criterion and the Heterotrait-Monotrait ratio. The Fornell-Larcker criterion requires that the square root of AVE for each construct should be greater than its correlations with other constructs. The HTMT ratio was also used because it is considered a more rigorous method for assessing discriminant validity in PLS-SEM. HTMT values below 0.85 or 0.90 indicate acceptable discriminant validity, depending on the conceptual similarity of the constructs (Henseler et al., 2015).

3.8 Structural model assessment

After confirming the reliability and validity

of the measurement model, the structural model was assessed to test the proposed hypotheses. The structural model examined the direct effects of blockchain technology on data privacy and trust. The path coefficients were used to determine the direction and strength of the relationships. The significance of the path coefficients was assessed through the bootstrapping procedure.

Bootstrapping was applied to generate t-statistics and p-values for hypothesis testing. A relationship was considered statistically significant if the p-value was below 0.05. The coefficient of determination, denoted by R-squared, was used to assess the model's explanatory power. R-squared values indicate the extent to which blockchain technology explains the variance in data privacy and trust. In addition, effect size was assessed through F-squared values to determine the relative contribution of blockchain technology to each dependent variable. Predictive relevance may also be evaluated using Q-square values to assess the model's predictive capability.

The structural model included two hypotheses. H1 proposed that blockchain technology has a significant positive impact on data privacy in cloud computing. H2 proposed that blockchain technology has a significant positive impact on trust in cloud computing. The acceptance or rejection of these hypotheses was based on the direction, strength, and statistical significance of the path coefficients.

3.9 Common method bias

Since the study collected data from the same respondents through a single questionnaire, common method bias was considered a potential concern. To reduce this issue, several procedural measures were adopted. The questionnaire was designed with clear, simple wording; respondents were assured of anonymity; and there were no right or wrong answers. These steps helped reduce evaluation apprehension and encouraged respondents to provide honest responses.

Statistical assessment of common method bias may be conducted through Harman's single-factor test or full collinearity assessment. Harman's single-factor test examines whether a single factor accounts for the majority of the variance in the dataset. If the first factor explains less than 50 percent of the total variance, common

method bias is not considered a serious issue. In addition, full collinearity variance inflation factor values below 3.3 indicate that common method bias is unlikely to distort the results (Kock, 2015). Therefore, both procedural and statistical remedies were considered to ensure the robustness of the findings.

4. Results and analysis

4.1 Respondents' demographic profile

The demographic profile of the respondents is presented in Table 1. A total of 265 valid responses were used for the final analysis. The demographic results show that the sample included respondents of different genders, ages, education levels, and professional backgrounds. This diversity helped obtain a broader understanding of respondents' perceptions of blockchain technology, data privacy, and trust in cloud computing.

Table 1. Demographic results

Demographic variable	Category	Frequency	Percentage
Gender	Male	157	59.20%
	Female	108	40.80%
Age	18–25 years	72	27.20%
	26–35 years	109	41.10%
	36–45 years	58	21.90%
	Above 45 years	26	9.80%
Education	Bachelor's degree	83	31.30%
	Master's degree	127	47.90%
	MS/MPhil	39	14.70%
	PhD/Other	16	6.10%
Experience with cloud services	Less than 1 year	47	17.70%
	1–3 years	96	36.20%
	4–6 years	78	29.40%
	More than 6 years	44	16.60%
Professional	IT/Software	91	34.30%

background	Business/Management	64	24.20%
	Education/Research	58	21.90%
	Other sectors	52	19.60%

The demographic results indicate that male respondents accounted for 59.2 percent of the sample, while female respondents accounted for 40.8 percent. Most respondents were between 26 and 35 years of age, representing 41.1 percent of the total sample. In terms of education, the largest group had a master's degree, representing 47.9 percent of the respondents. The majority of respondents also had at least 1 year of experience with cloud services, suggesting they were reasonably familiar with the research context. The professional background of respondents also shows sufficient diversity, with the largest proportion coming from IT and software-related fields.

4.2 Descriptive statistics

Descriptive statistics were calculated to examine the general response pattern of the study constructs. Table 2 presents the mean and standard deviation values for blockchain technology, data privacy, and trust.

Table 2. Descriptive statistics

Construct	N	Minimum	Maximum	Mean	Standard deviation
Blockchain Technology	265	1	5	3.91	0.694
Data Privacy	265	1	5	3.84	0.721
Trust	265	1	5	3.79	0.748

The descriptive results show that blockchain technology had a mean of 3.91, indicating that respondents generally agreed that it provides useful features for cloud computing. Data privacy had a mean value of 3.84, suggesting that respondents perceived blockchain-supported cloud systems as helpful for improving privacy protection. Trust had a mean value of 3.79, indicating that respondents also showed a positive perception of blockchain technology in strengthening trust in cloud computing. The standard deviation values were below 1.00, which suggests that

responses were relatively consistent across respondents.

4.3 Assessment of measurement model

The measurement model was assessed through factor loadings, Cronbach's alpha, composite reliability, and average variance extracted. The purpose of the measurement model assessment was to confirm the reliability and validity of the constructs before testing the structural relationships. According to Hair et al. (2021), outer loadings should preferably be above 0.70, Cronbach's alpha and composite reliability should exceed 0.70, and AVE should be above 0.50.

4.3.1 Factor loadings

The factor loadings of all measurement items are presented in Table 3.

Table 3. Factor loadings

Construct	Item	Factor loading
Blockchain Technology	BT1	0.812
	BT2	0.846
	BT3	0.821
	BT4	0.858
	BT5	0.834
Data Privacy	DP1	0.801
	DP2	0.837
	DP3	0.849
	DP4	0.826
	DP5	0.815
Trust	TR1	0.818
	TR2	0.852
	TR3	0.841
	TR4	0.809
	TR5	0.833

The factor loading values ranged from 0.801 to 0.858. All values were above the recommended threshold of 0.70. This indicates that each item had a strong

association with its respective construct. Therefore, no item was removed from the model. The results confirm the acceptable reliability of the indicators for blockchain technology, data privacy, and trust.

4.3.2 Reliability and convergent validity

Reliability and convergent validity results are presented in Table 4.

Table 4. Reliability and convergent validity

Construct	Cronbach's alpha	rho_A	Composite reliability	AVE
Blockchain Technology	0.891	0.895	0.92	0.697
Data Privacy	0.883	0.887	0.914	0.681
Trust	0.889	0.892	0.918	0.691

The reliability results show that Cronbach's alpha values ranged from 0.883 to 0.891, exceeding the minimum threshold of 0.70. Composite reliability values ranged from 0.914 to 0.920, also exceeding the recommended value of 0.70. These findings indicate strong internal consistency reliability. The AVE values ranged from 0.681 to 0.697, exceeding the 0.50 threshold. This confirms convergent validity, meaning that the items adequately explain their respective constructs.

4.3.3 Discriminant validity: Fornell-Larcker criterion

The Fornell-Larcker criterion was used to assess discriminant validity. The results are shown in Table 5. The diagonal values represent the square root of AVE.

Table 5. Fornell-Larcker criterion

Construct	Blockchain Technology	Data Privacy	Trust
Blockchain Technology	0.835		
Data Privacy	0.641	0.825	
Trust	0.672	0.614	0.831

The Fornell-Larcker results show that the square root of the AVE for each construct exceeds its correlations with other constructs. The square root of AVE for blockchain technology was 0.835, for data privacy 0.825, and for trust 0.831. Since each diagonal value is higher than the corresponding inter-construct correlations,

discriminant validity is established.

4.4 Assessment of multicollinearity

Before testing the structural model, multicollinearity was assessed using variance inflation factor values. The results are shown in Table 6.

Table 6. Collinearity statistics

Predictor	Dependent variable	VIF
Blockchain Technology	Data Privacy	1
Blockchain Technology	Trust	1

The VIF values were 1.000 for both structural paths. Since the values are below the recommended threshold of 3.3 and 5.0, multicollinearity was not a concern in the structural model. This means the predictor variable did not pose estimation problems for the model.

4.5 Common method bias

Since data were collected from the same respondents through a single questionnaire, common method bias was assessed. Harman's single-factor test was used to examine whether one factor explained the majority of the variance. The results are presented in Table 7.

Table 7. Harman's single-factor test

Test	Value
Total variance explained by the first factor	36.84%
Recommended maximum threshold	50.00%
Common method bias issue	Not serious

The first factor explained 36.84 percent of the total variance, which is below the recommended threshold of 50 percent. Therefore, common method bias was not considered a serious issue in this study. This suggests that a single common factor did not mainly influence the results.

4.6 Structural model assessment

After confirming the reliability and validity of the measurement model, the structural model was assessed. The structural model was evaluated through R-square, adjusted R-square, Q-square, f-square, and path coefficients.

4.6.1 Coefficient of determination

The coefficient of determination explains the amount of variance in the dependent variable explained by the independent variable. The results are shown in Table 8.

Table 8. R-square and adjusted R-square

Dependent variable	R-square	Adjusted R-square
Data Privacy	0.411	0.409
Trust	0.452	0.45

The R-squared value for data privacy was 0.411, indicating that blockchain technology explained 41.1 percent of the variance in data privacy. The R-squared value for trust was 0.452, indicating that blockchain technology explained 45.2 percent of the variance in trust. These values indicate moderate explanatory power. The results suggest that blockchain technology is an important predictor of both data privacy and trust in cloud computing.

4.6.2 Predictive relevance

Predictive relevance was assessed through Q-square values. The results are presented in Table 9.

Table 9. Predictive relevance

Dependent variable	Q-square
Data Privacy	0.276
Trust	0.311

The Q-square values for data privacy and trust were 0.276 and 0.311, respectively. Since both values are greater than zero, the model has predictive relevance. This indicates that blockchain technology has useful predictive capability in explaining data privacy and trust in cloud computing.

4.6.3 Effect size

The effect size was assessed using F-squared values. The results are presented in Table 10.

Table 10. Effect size

Relationship	f-square	Effect size
Blockchain Technology → Data Privacy	0.698	Large
Blockchain Technology → Trust	0.825	Large

The f-square value for the effect of blockchain technology on data privacy was

0.698, indicating a large effect size. The f-square value for the effect of blockchain technology on trust was 0.825, also indicating a large effect size. These results show that blockchain technology has a strong practical contribution to explaining both dependent variables.

4.7 Hypothesis Testing

The hypotheses were tested using bootstrapping in PLS-SEM. The results are presented in Table 11.

Table 11. Hypotheses testing

Hypothesis	Path	Beta	Standard error	t-value	p-value	Decision
H1	Blockchain Technology → Data Privacy	0.641	0.047	13.638	0.000	Supported
H2	Blockchain Technology → Trust	0.672	0.044	15.273	0.000	Supported

The findings indicate that blockchain technology positively and significantly influences data privacy in cloud computing, featuring a beta of 0.641, a t-value of 13.638, and a p-value of 0.000. Given that the p-value is less than 0.05, H1 is validated. This discovery suggests that more robust views of blockchain technology correlate with greater perceptions of data privacy in cloud computing. The findings indicate that blockchain attributes like decentralization, immutability, traceability, and cryptographic security contribute to users' perception of enhanced protection for their cloud-stored data.

The findings indicate that blockchain technology exerts a beneficial and substantial effect on trust in cloud computing, presenting a beta of 0.672, a t-value of 15.273, and a p-value of 0.000. Because the p-value is lower than 0.05, H2 is validated. This discovery shows that blockchain technology enhances users' confidence in cloud computing. The finding indicates that blockchain enhances trust by boosting transparency, accountability, auditability, and verifiability within cloud-based systems.

4.8 Discussion

This study aimed to investigate the effects

of blockchain technology on data privacy and trust within cloud computing. The research utilized blockchain technology as the independent variable, while data privacy and trust served as dependent variables. Data were gathered from 265 participants and examined using Partial Least Squares Structural Equation Modeling. The results endorsed both suggested hypotheses. The findings indicated that blockchain technology positively influences data privacy in cloud computing. The results also verified that blockchain technology positively and significantly influences trust in cloud computing.

The initial hypothesis suggested that blockchain technology greatly enhances data privacy in cloud computing. The outcome backed this theory. This discovery suggests that blockchain characteristics like decentralization, immutability, cryptographic security, traceability, transparency, and auditability can enhance users' views on privacy protection within cloud settings. In conventional cloud computing, users frequently rely significantly on centralized cloud service providers for data storage, access regulation, and security oversight. This reliance brings worries regarding unauthorized access, data abuse, lack of transparency, and reduced user control. Blockchain can address these issues by offering tamper-proof records, decentralized validation, and clear access logs. Consequently, the result indicates that blockchain technology can serve as a privacy-boosting tool in cloud computing.

The second hypothesis suggested that blockchain technology greatly enhances trust in cloud computing. The outcome further validated this hypothesis. This discovery suggests that users are more inclined to have confidence in cloud computing systems when blockchain mechanisms improve transparency, accountability, and verifiability. Trust represents a significant concern in cloud computing since users lack physical control over the infrastructure housing and processing their data. Blockchain can enhance trust by rendering cloud transactions traceable and hard to alter. When users feel that blockchain can validate cloud-related activities, their trust in the cloud system grows. This outcome reinforces the idea that blockchain enhances not only technical security but

also fosters psychological confidence and trust in digital spaces.

The results show that blockchain technology plays a significant role in enhancing data privacy and trust in cloud computing. The findings align with earlier studies indicating that blockchain can facilitate secure, transparent, decentralized, and reliable data management in cloud systems. The research further establishes that trust and privacy are strongly associated with the technological features of blockchain. When users see blockchain as secure, transparent, and resistant to tampering, they are more inclined to trust that their data is safeguarded and that cloud systems are dependable.

5. Conclusion

This research explored the effect of blockchain technology on data privacy and trust in cloud computing. The study utilized a quantitative approach, gathering primary data from 265 participants. The analysis of the data was conducted using PLS-SEM. The findings verified that blockchain technology positively affects data privacy substantially. The results also validated that blockchain technology greatly enhances trust. As a result, both hypotheses of the research were confirmed. The research finds that blockchain technology can function as a potent tool for enhancing privacy and trust within cloud computing settings. Its distributed framework minimizes dependence on a singular central authority, while its permanent and clear records improve accountability and validation. The blockchain's cryptographic attributes facilitate secure data management and access regulation. These characteristics together make cloud users more assured that their data is safeguarded from unauthorized access, inappropriate use, and alteration.

The results also indicate that blockchain-based cloud computing can offer enhanced security to both users and organizations. In contemporary digital settings, cloud services are frequently utilized for storing, sharing, and handling sensitive data. Nonetheless, risks to privacy and a shortage of trust continue to be significant obstacles to adopting and consistently using cloud services. Cloud service providers can enhance transparency, accountability, and user trust by incorporating blockchain technology. Consequently, blockchain

technology is seen as an important resource for creating cloud computing systems that are more secure, focused on privacy, and dependable.

6. Theoretical implications

This research provides multiple theoretical contributions to the existing literature regarding blockchain technology, data privacy, trust, and cloud computing. The study enhances understanding by empirically examining the direct effects of blockchain technology on data privacy and trust within the realm of cloud computing. Numerous prior studies have examined blockchain and cloud computing from a technical or conceptual viewpoint. Nevertheless, few studies have explored users' views using primary data. Utilizing survey information from 265 participants, this research offers empirical proof that blockchain technology is positively linked to both trust and privacy results.

Secondly, the research broadens the body of work on cloud computing by demonstrating that privacy and trust rely not only on conventional security measures but can also be enhanced through decentralized technologies. Research in cloud computing has frequently concentrated on encryption, quality of service, reliability of providers, and compliance strategies. This research adds to that conversation by demonstrating that features of blockchain, like immutability, decentralization, transparency, and auditability, can also clarify views on privacy and trust. Consequently, the research offers a wider perspective on how new technologies can enhance user trust in cloud settings.

Third, the research adds to blockchain literature by framing blockchain as a technology that both enhances security and builds trust. The results indicate that blockchain ought not to be seen merely as a system for storing data or recording transactions. Rather, it may also be seen as a governance tool that enhances accountability, verification, and transparency in cloud computing. This broadens the theoretical function of blockchain from just a technical instrument to a digital infrastructure that facilitates trust.

Fourth, the research adds methodologically by utilizing PLS-SEM to evaluate a straightforward and targeted model. Utilizing PLS-SEM allowed the research to

evaluate measurement reliability and validity, in addition to the structural connections between blockchain technology, data privacy, and trust.

7. Practical implications

The results of this research hold significant practical relevance for cloud service providers, IT administrators, technology creators, policymakers, and organizations utilizing cloud computing services. Initially, cloud service providers ought to think about incorporating blockchain technologies into cloud frameworks to enhance data privacy. Blockchain can facilitate the creation of secure access logs, tamper-resistant records, decentralized identity control, and transparent systems for data sharing. These attributes may alleviate users' privacy worries and enhance trust in cloud data security.

Organizations that utilize cloud computing ought to contemplate integrating blockchain into their overall data governance and cybersecurity plans. Numerous organizations keep confidential customer, financial, operational, and employee information on cloud services. By implementing blockchain-based verification and audit systems, organizations can enhance their control over data access and reinforce accountability. This is especially beneficial for industries like banking, healthcare, education, government, e-commerce, and supply chain management, where trust and data privacy are essential.

Third, IT managers need to prioritize user trust while implementing blockchain-powered cloud systems. The results indicate that blockchain technology enhances trust by boosting transparency and verifiability. Consequently, organizations must not only adopt blockchain on a technical scale but also convey its advantages to users. Transparent communication regarding how blockchain secures data, logs access, deters tampering, and fosters transparency can enhance user trust.

Fourth, cloud service providers can utilize blockchain technology to achieve a competitive edge. In a market where users are growing more worried about privacy violations, cyber threats, and data abuse, blockchain-based privacy and trust capabilities can distinguish cloud service providers from their rivals. Providers delivering transparent, verifiable, and

blockchain-based cloud services could appeal to clients who prioritize data security and integrity.

8. Limitations

While this research presents valuable insights, it also has certain constraints. Initially, the research employed a cross-sectional study design. Data were gathered at one specific moment, restricting the ability to track shifts in perceptions over time. Users' perceptions regarding blockchain technology, data privacy, and trust could evolve as they accumulate more experience with blockchain-based cloud systems. Consequently, the results should be viewed as a reflection of respondents' views at the moment of data gathering.

Secondly, the research utilized primary data collected from 265 participants. Even though the sample size was adequate for PLS-SEM, a larger sample could enhance the generalizability of the results. The respondents could also vary in their degree of technical understanding regarding blockchain and cloud computing. Certain respondents might possess significant technical knowledge, whereas others may only have a basic understanding. This distinction could affect their views on blockchain technology, privacy, and trust.

Third, the research employed a straightforward model featuring one independent variable and two dependent variables. This model effectively facilitated a straightforward analysis of the immediate influence of blockchain technology on privacy and trust in data. Nonetheless, privacy and trust in cloud computing can also be affected by various factors, such as perceived security measures, adherence to regulations, quality of service, reputation of the provider, user experience, awareness of cybersecurity, and perceived risks. These factors were excluded from the present model.

Fourth, the research depended on data from self-reported questionnaires. Data that individuals report about themselves can be influenced by response bias, social desirability bias, or common method bias. Even though procedural and statistical measures can mitigate these problems, they cannot be completely eradicated. Subsequent research might employ mixed methods, interviews, experiments, or system-level data to enhance the credibility of results.

Fifth, the research emphasized user

perceptions instead of the real technical execution of blockchain in cloud systems. Consequently, the findings illustrate how participants view blockchain's function in enhancing privacy.

9. Future research directions

Future researchers may further develop this study in various ways. Initially, upcoming studies could utilize longitudinal research methods to explore how views on blockchain technology, data privacy, and trust evolve over time. With the rise of blockchain-powered cloud systems, users' understanding and trust might grow. A longitudinal study would allow researchers to ascertain if blockchain consistently affects privacy and trust over the long haul.

Secondly, upcoming studies could incorporate more variables to create a more thorough model. As mediators or moderators, factors like perceived security, perceived risk, transparency, regulatory adherence, service quality, provider reputation, and user experience could be included. These factors can clarify how and under which circumstances blockchain technology enhances data privacy and trust in cloud computing.

Third, upcoming studies could analyze various sectors, including banking, healthcare, education, government, and e-commerce. Given that different sectors manage various kinds of data, the impact of blockchain on enhancing privacy and trust could differ among industries. For instance, blockchain could hold greater significance in healthcare and banking due to the sensitive nature of the data handled in these industries.

Fourth, upcoming research could analyze users from various countries or areas. Countries vary in terms of data privacy laws, technological frameworks, blockchain knowledge, and levels of cloud adoption. Comparative research across countries can offer a better understanding of how cultural, legal, and technological variations affect the connection between blockchain technology, privacy, and trust.

Fifth, upcoming studies could utilize mixed-methods strategies. Quantitative data can examine the connections between variables, whereas qualitative interviews can clarify why users have trust or distrust in blockchain-based cloud computing. This would offer a deeper understanding of users' expectations, worries, and experiences.

Ultimately, future technical studies can create and evaluate blockchain-based cloud computing systems within authentic organizational environments. These studies can assess real system performance, transaction speed, scalability, expenses, privacy safeguards, and security results. This would facilitate the link between perception-oriented studies and technical execution.

Reference

Sunyaev, A. (2024). Cloud computing. In *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies* (pp. 165-209). Cham: Springer Nature Switzerland.

Walsh, G., Connolly, N., Otlyvanska, G., Derzhuk, O., Donnellan, B., & Dooley, J. (2026). Enhancing network access and scaling capacities through neutral host networks: the role of connectivity in supporting digital transformation. In *Research Handbook on Digital Transformation and Responsibility* (pp. 136-152). Edward Elgar Publishing.

Yandamuri, U. S. (2026). Scalable Cloud-Based Intelligent Decision Systems Leveraging AI and Big Data for Industry-Specific Optimization. *Minnesota Journal of Business Law and Entrepreneurship*, (1), 584-601.

Ali, T., Al-Khalidi, M., & Al-Zaidi, R. (2026). Information security risk assessment methods in cloud computing: Comprehensive review. *Journal of Computer Information Systems*, *66*(1), 123-150.

Asheshemi, N. O., & Adawaren, M. (2026). Mitigating Insider Threats and Data Breaches in Nigerian Financial Cloud Systems Using a Blockchain-Based Zero Trust Framework. *Scientific Journal of Engineering, and Technology*, *3*(1), 28-43.

Anser, M. K., Naeem, M., Ali, S., Ali, S., & Javid, R. (2025). The relationship between artificial intelligence and environmental performance: the mediating role of external environmental factors. *Humanities and Social Sciences Communications*, *12*(1), 1-7.

Anser, M. K., Naeem, M., Ali, S., Huizhen, W., & Farooq, S. (2024). From knowledge to profit: business reputation as a mediator in the impact of green intellectual capital on business performance. *Journal of Intellectual Capital*, *25*(5-6), 1133-1153.

Bohio, K. K., Shaikh, F., Amin, M. S., & Naeem, M. (2025). From Green Policies to

Performance: How Digitalization and Innovation Transform Organizational Outcomes in industry 4.0 of Pakistan. *Journal of Business and Management Research*, *4*(4), 800-816.

Khan, N., Naeem, M., & Siraj, M. (2024). Evaluating Green Supply Chain Performance Using Multi-Criteria Decision-Making (MCDM) Models. *RADS Journal of Business Management*, *6*(2), 113-123.

Mujtaba, M., Naeem, M., & Khan, K. (2025). From Leadership to Performance: Exploring the Pathway through Psychological Empowerment and Job Satisfaction in Developing Economies. *Journal of Management & Social Science*, *2*(5), 166-183.

Naeem, M., Memon, S., Salman, M., Mehboob, A., Fatima, A., & Rehman, A. (2025). Transformational Leadership and Operational Efficiency in Industry 4.0: The Mediating Role of Digitalization through the Lens of Dynamic Capabilities Theory. *Asian Journal of Economics, Finance and Management*, *7*(1), 240-251.

Naeem, M., Siraj, M., & Farooq, S. (2023). Teacher and Administrator Perceptions of Using Artificial Intelligence in Education. *Journal of Education & Social Sciences*, *11*(2), 71-88.

Shahab, S., Khan, K., & Naeem, M. (2025). The Power of Generative AI in Shaping Green and Responsible Supply Chains: Rethinking and Advancing Sustainable Solutions for Social Change. *Journal of Business and Management Research*, *4*(4), 800-817.

Shaikh, F., Sial, A., Khan, K., & Naeem, M. (2025). FinTech-Enabled HR Payroll Automation and Its Effect on Employee Satisfaction and Brand Image. *Advance Journal of Econometrics and Finance*, *3*(4), 74-83.

Sial, A., Khan, M. K., & Naeem, M. M. (2025). Green Finance, Business Reputation and Sustainability Performance: Evidence from Pakistan. *Bulletin of Management Review*, *2*(3).

Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. *Blockchain: research and applications*, *3*(2), 100067.

Hair Jr, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). An introduction to structural equation modeling. In *Partial least squares structural equation modeling (PLS-SEM)*

using R: a workbook (pp. 1-29). Cham: Springer International Publishing.

Li, W., Wu, J., Cao, J., Chen, N., Zhang, Q., & Buyya, R. (2021). Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. *Journal of Cloud Computing*, *10*(1), 35.

Lynn, T., Mooney, J. G., van der Werff, L., & Fox, G. (2021). *Data Privacy and Trust in Cloud Computing: Building trust in the cloud through assurance and accountability* (p. 149). Springer Nature.

Rahmani, M. K. I., Shuaib, M., Alam, S., Siddiqui, S. T., Ahmad, S., Bhatia, S., & Mashat, A. (2022). [Retracted] Blockchain-Based Trust Management Framework for Cloud Computing-Based Internet of Medical Things (IoMT): A Systematic Review. *Computational Intelligence and Neuroscience*, *2022*(1), 9766844.