International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250-3552

Secure Multi-Tenant AI Architecture Enhances Enterprise AI Adoption Through Tenant Trust Using PLS-SEM in India's Salesforce Cloud Industry

Harika Gajjela

Independent Researcher, India

Mahathi Kari

Independent Researcher, India

Abstract

The emerging difficulty facing organizations is to acquire multi-tenant AI deployment, without losing the confidence in Salesforce cloud platforms. The idea that a secure multi-tenant architecture-oriented AI will enhance the acceptance of enterprise AI in the cloud-based Salesforce business setting in India was investigated in this paper, as it builds trust amongst tenants. The research was anchored on Trust Theory that classified the elements of perceived security assurance and its way of increasing the acceptance of the organizational technology and platform confidence. PLS-SEM was used to test the proposed relationships and 412 Indian-based IT managers, Cloud Administrators, Sales Force Professionals obtained the data, with the help of structured questionnaires. The findings have indicated that secure multi-tenant AI architecture positively affects the trust of tenants and was instrumental in influencing the adoption of AI throughout an enterprise, Salesforce-centered institutions. Also, the indirect influence of secure multi-tenant AI architecture to the adoption of enterprise AI based on tenant trust was high in its turn since all of the structural relationships were found statistically significant at $p < 0.01$. The study provides current knowledge which fills in the gap between AI security architecture and enterprise uptake through trust, thereby contributing to socio-technical cloud governance studies as well as setting a strategic path of deploying AI in Salesforce without issues over security.

Keywords

Secure Multi-Tenant AI Architecture, Enterprise AI Adoption, Tenant Trust, PLS-SEM, Salesforce Cloud Industry, India, AI Security Governance

1. Introduction

High speed adoption of artificial intelligence (AI) in cloud-based enterprise ecosystems has revolutionized how companies are dealing with customer relations, operational intelligence, and electronic decisions. Multi-tenant cloud systems, notably Salesforce, have made it possible to deploy AI on a large scale, along with cost optimizations on infrastructure and flexibility within organizations. Nevertheless, the increasing reliance on common AI-enabled settings has also raised the alarm on tenant isolation issues, data leakage, algorithmic transparency, and cloud security controls. These statistics are supported by the fact the average cost of a data breach per organization is USD 4.24 million in 2021 according to the IBM Security Report, with cloud vulnerabilities and unauthorized access becoming the significant risks to enterprises. The current findings show that even with the efficiency of AI-powered cloud environments and their capabilities to enhance operational efficiency and digital responsiveness, organizations are still confronted with significant uncertainty about data security and platform safeguarding (Dwivedi et al., 2021; Vial, 2021). This is an indicator that technological scalability may not guarantee the permanent enterprises adoption unless firms develop trust and security with cloud infrastructures. In the enterprise software sector, Salesforce cloud solutions have been instrumental to AI-based customer relationship management, workflow automation, and predictive analytics. The combination of AI-type recommendation systems (or the integration of automation tools and intelligent customer engagement mechanisms) has increased the pace with which organizations depend on multi-tenant cloud infrastructures (Benbya et al., 2021; Huang and Rust, 2021). Though these developments have occurred, businesses still face issues of data privacy, access controls,

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250-3552

accountability of algorithms, and security protection at the tenant level. The hypothetical reason is that when the AI environment is multi-tenant, there is a complexity of governance due to the presence of multiple organizations that share computational resources and intelligent services within the identical ecosystem. Moreover, managerial distrust towards AI-based enterprise platforms has grown due to cybersecurity breaches related to cloud-native platforms (Kshetri, 2021; Tawalbeh et al., 2020). As such, secure multi-tenant AI architecture has emerged as a strategic requirement in addition to technical infrastructure requirement.

India presents an exceptionally topical environment to analyze secure AI-based Salesforce ecosystems since over the past decade, the country has made exceptional progress in its cloud computing and enterprise digital transformation. The growing use of AI-based enterprise applications in banking, healthcare, retail, and information technology industries has led to the near-monolithic growth of the enterprise cloud business in India. Moreover, India is one of the biggest international locations of Salesforce implementation, cloud technology consultancy, and enterprise technology services. Nonetheless, in spite of increased rates of digital adoption, Indian organizations still experience significant cybersecurity issues related to AI integration, compliance with governance, and protective data of tenants (Gupta et al., 2022; Sarker et al., 2021). This means that the Indian Salesforce cloud sector offers a suitable and strategically relevant backdrop to research the effect of secure multi-tenant architecture of AI in terms of its role in determining the uptake of AI in the enterprise using trust-based systems.

Despite a rise in investment in AI-powered cloud ecosystem within the organizations, numerous enterprise AI projects remain elicitation resistant, poorly defined in governance, and lacking organizational trust. Current cloud security models have mainly focused on technical safeguards like encryption, authentication, and intrusion detection, with relatively little focus placed on organizational trust implications with regard to secure AI structures (Taleb et al., 2021; AlHogail, 2021). As a result, organizations can embrace highly developed AI infrastructures and yet there seems to be a sense of high uncertainty as per accountability, reliability, and integrity of the platform. This unsolved tension is an urgent issue in the Salesforce cloud ecosystems since the decisions to adopt the enterprise at their level are not only based on the technical features but also on the image of trust and the guarantee of governance. Thus, research is already a significant, yet not sufficiently studied factor that needs more attention to understand how secure multi-tenant AI architecture creates trust among tenants.

The adoption approach of cloud computing, governance of cybersecurity, enterprise AI systems, and the policies of digital transformation are some of the issues that have been discussed in the context of literature extensively. A number of studies have investigated the correlation between the capabilities of cloud security and the outcomes of organizational performance (AlHogail, 2021; Khan et al., 2022). The other scientists explored AI-based enterprise systems and their impact on the operational agility, customer intelligence and digital innovation (Dwivedi et al., 2021; Benbya et al., 2021). Also, the research of multi-tenant cloud models focused on the optimization of infrastructures, virtualization in enterprise eco-systems, and scalability (Taleb et al., 2021; Tawalbeh et al., 2020). Nevertheless, the majority of literature available today is too technology-affected and is oriented to the infrastructural performance specifics, but not types of socio-technical trust formations. Conversely, the literature on information systems is increasingly focused on the idea that organizational trust is core in technology acceptance and sustained digital viability in the long term (Gefen et al., 2003; Vial, 2021).

Regardless of an increasing academic interest in AI governance and enterprise cloud systems, major theoretical and practical shortcomings have yet to be addressed. The use of direct relations between cloud security mechanisms and organizational outcomes has been a major aspect in past research yet it has not explored the role of tenant trust as a mediating factor between secure multi-tenant AI architecture and enterprise AI adoption. Moreover, most original studies were based on imaginary debates, technical benchmarking, or simulation studies and provided little empirical

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250-3552

validation based on such sophisticated latent-variable models as PLS-SEM (Benbya et al., 2021; Gupta et al., 2022). The other contextual constraints are the relatively limited number of studies investigating context-specific trust-based AI uptake in the Salesforce cloud sector of India despite its growing digital community. This disconnect also implies that one may need a more customized socio-technical structure that can explain the impact of secure AI architecture on enterprise adoption behavior in terms of trust formation.

To address these limitations, the current study aims to fulfill a number of objectives that are inter-related. To begin with, the paper will investigate the connection between secure multi-tenant AI architecture and enterprise AI adoption in the Salesforce cloud industry in India. Second, it examines the role played by tenant trust in mediating the relationship between secure multi-tenant AI architecture and enterprise adoption of AI. Third, the article assesses the relevance of Trust Theory in the context of explaining AI-based multi-tenant cloud ecosystem organizational confidence. Lastly, the research uses PLS-SEM to estimate the conceptual model suggested and determine intricate relationships between the constructs.

To tackle these objectives, the research questions of the study are as follows. RQ1: Does secure multi-tenant AI architecture have a significant impact on enterprise adoption of AI on Salesforce cloud platforms? RQ2: Is there a mediation between secure multi-tenant AI architecture and enterprise AI adoption? RQ3: How does Trust Theory justify the organizational trust in safe AI-enabled cloud environments? These questions draw a logical analytical framework that can be used to consider both direct and indirect relations within the proposed framework.

This research has an added value in expanding the field of AI governance, cloud security of enterprises, and socio-technical trust building in multi-tenant ecosystems. Theoretically, the research carries forward Trust Theory by making the concept of the tenant trust as a mediating variable between the secure AI architecture and the adoption of AI in an enterprise. The research has been conducted methodologically to enhance the empirical rigor by integrating the use of PLS-SEM in a complex latent-variable framework. The contextually, the research presents novel information on Salesforce cloud industry in India, which is still less explored though the numbers of enterprises using AI are surging positively. They also provide give advice to managers, cloud architects, and policymakers in enterprises who want to enhance trust-driven AI governance measures in cloud-native architectures.

The rest of this paper will be structured in the following way. The second part will summarize the available literature and come up with the theoretical framework and hypotheses. The third section explains the methodology of research such as sampling procedures, measuring development and the PLS-SEM analysis procedures. The fourth part discusses the results of a hypothesis test and empirical evidence. The fifth part comments on theoretical and managerial implications as far as the previous literature is concerned. Lastly, the conclusion will provide some limitations, practical recommendations and future research directions.

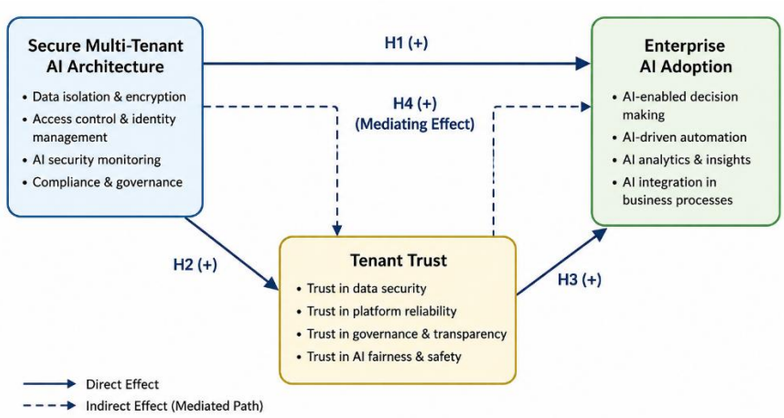

Figure 1. Conceptual Framework of Secure Multi-Tenant AI Architecture and Enterprise AI Adoption

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250-3552

2. Literature Review and Hypotheses Development

Secure multi-tenant AI architecture can be understood as a cloud-based intelligent infrastructure semantics, which allow several organizational tenants to utilize computational resources and obtain robust data isolation, data governance, and AI-operational integrity. Multi-tenant-based architecture has gained relevance in enterprise ecosystems like Salesforce since organizations need scalable AI implementation without sacrificing the security, privacy or assurance of governance. The adoption of enterprise AI on the contrary illustrates the acceptance of enterprise willingness to involve AI-enabled systems in the strategic and operational tasks in deciding. Tenant trust reflects the extent of perceptions of enterprise users towards the service provider that it is secure, reliable, transparent, and capable of safeguarding organizational interests when used in common cloud settings. The current research is based on the Trust Theory, which states that trust is a key mechanism that helps to minimize uncertainty and perceived risk in adoption settings of technologies (Gefen et al., 2003; McKnight et al., 2011).

The Trust Theory is especially applicable as AI-enabled multi-tenant ecosystems are associated with high complexity, information asymmetry, and uncertainty in governance and thus, organizational trust becomes a precondition to an enterprise adoption determination decision. The latest studies on the digital transformation further increase the role of trust that the organization is increasingly ready to accept in the domain of AI-powered cloud services since enterprises consider not only technical efficiency but also governance credibility, and assurance of the security (Vial, 2021; Dwivedi et al., 2021). Although the Technology Acceptance Model (TAM) and the Diffusion of Innovation Theory have been applied to explain user adoption based on perceptions of usefulness and the nature of innovation, there is less explanation of the models on security-compelled trust formation in shared AI ecosystems (Davis, 1989; Rogers, 2003). Consequently, the Trust Theory is a much stronger explanation since it directly reflects the way in which perceived security assurance and governance confidence predetermine enterprise adoption behavior in the uncertain situation of technological uncertainty. However, the theory can be limited in very controlled places where compliance requirements and not perceptions in terms of trust rules the organizational decision.

The existing literature suggests that safe cloud architecture has a beneficial impact on the implementation of technologies by enterprises since institutions are more comfortable with the system minimizing the risk of exposure to operations and maximizing the assurance of their control (Benbya et al., 2021; Gupta et al., 2022). Tenant isolation, encryption schemes, identity access control, and zero-trust systems are architectural security features related to multi-tenant AI environments and enhance the organizational trust levels by lessening the perceived risks related to unauthorized access and data leakage (Khan et al., 2022; Tawalbeh et al., 2020). It implies that a business faster embraces AI-based Salesforce cloud offerings in the context of security structures that are reliable and accountable. Moreover, according to the digital transformation research, organizations are becoming more and more inclined to see secure AI infrastructure as a strategic competence that allows them to run long-term innovation and operational resiliency (Vial, 2021; Rjoub et al., 2023). Other researchers state, however, that advanced security systems can add complexity and implementation price to the system, thus reducing the adoption of the enterprise in some types of organizations (Kshetri, 2021; AlHogail, 2021). Conversely, some researchers even state a positive correlation between the investments in security and the state of technological maturity and readiness in the organization, as well as the increasing acceptance of the enterprise (Sarker et al., 2021; Dwivedi et al., 2023). Therefore, the current literature is inconclusive on whether secure multi-tenant AI architecture is a consistent, positive factor in securing enterprise AI adoption in cloud-native ecosystems. Using the Trust Theory, secure architecture minimizes uncertainty and maximizes institutional trustworthiness perceptions, leading to higher adoption decision of AI at the enterprise level. Therefore, it is assumed that:

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250-3552

H1: Secure multi-tenant AI architecture has a favorable impact on the adoption of enterprise AI in the Salesforce cloud industry in India.

The Trust Theory also indicates that security assurance is an antecedent of organizational trust since organizations ensure confidence when their computer systems are reliable, transparent, and safeguarded by governance (Gefen et al., 2003; McKnight et al., 2011). According to past researchers, through secure technological support, the establishment of trust has a positive effect by alleviating worries about cyber threats, data misuse, and managing operational instability (Alshamrani et al., 2022; Taleb et al., 2021). Several tools in AI-enabled Salesforce ecosystems, including multi-tenant security controls, e.g., AI-driven anomaly detection, role-based access control, and encryption protocols, are likely to enhance tenant trust since organizations will feel that the ecosystem is responsible and robust. Furthermore, recent AI regulation texts highlight the fact that trust grows more based on how data are viewed to be responsibly handled and how intelligent systems are transparent and are not just based on technical efficiency (Huang and Rust, 2021; Dwivedi et al., 2021). Nonetheless, there are also conflicting results. Other researchers believe that even the presence of robust security frameworks does not ensure that organizations will trust AI-based systems since algorithmic opacities and automated decision-making algorithms lead to uncertainty in the case of accountability and fairness (Benbya et al., 2021; Kshetri, 2021). Other researchers, in turn, provide that these concerns may be addressed by more sophisticated mechanisms of governance, increasing the level of transparency and perceived reliability (Gupta et al., 2022; Sarker et al., 2021). In this way, the current body of work is disjointed as the research has not examined the degree to which secure multi-tenant AI architecture enhances tenant confidence towards enterprise cloud ecosystems. The Trust Theory offers an excellent explanation since perceived vulnerability is decreased directly when security assurance is given, which makes the organizations build stronger confidence in common AI infrastructures.

H2: Secure multi-tenant AI architecture has a positive impact on tenant trust in Salesforce cloud industry in India.

The issue of tenant trust has also become a decisive factor in the adoption of AI in enterprises as organizations are slowly gauging the quality of intelligent systems on the provisions of reliability, transparency, and assurance of governance in place of operational efficiency only (Gefen et al., 2003; Vial, 2021). According to past research, trust has a positive impact on organizational readiness to use cloud-native, decreasing uncertainty around data protection, service continuity, and algorithmic decision-making (Rjoub et al., 2023; AlHogail, 2021). In Salesforce cloud ecosystems, the trust between tenants can boost enterprise AI adoption as organizations tend to engage AI systems, more when they believe the platform to be safe, responsible, and has the ability to secure strategic information protection. Moreover, the organizational relationships based on trust promotes long-term commitment and decreases the degree of opposition to AI-enabled innovation efforts (Dwivedi et al., 2023; Benbya et al., 2021). Nevertheless, a body of opposing evidence argues that trust, on its own, might be ineffective in triggering enterprise adoption since the cost factor, organizational culture, and technological preparedness might also influence the decision to adopt (Khan et al., 2022; Gupta et al., 2022). Conversely, some studies suggest that trust has been the leading predictor in the presence of not only the complexity of technology but also uncertainty of cybersecurity since organizations are not interested in short-term operational effectiveness but in reducing the amount of risk (Sarker et al., 2021; Taleb et al., 2021). Therefore, current literature is still theoretically behind in terms of pinpointing the exact effect of tenant trust on the uptake of enterprise AI platforms in AI-enabled multi-tenant cloud systems. The connection between these two is explained through the Trust Theory which suggests that the organizational trust minimizes the perceived uncertainty and enhances confidence in technology-based decision environments. Thus, it is hypothesized that:

H3: Tenant trust has a positive impact on enterprise AI adoption in Salesforce cloud industry in India.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250-3552

The mediation of the tenant trust is the key theoretical approach in the offered framework since the secure multi-tenant AI architecture might not directly change the uptake of enterprise AI unless the organizations consider the environment to be trustful and governance-is oriented. According to Trust Theory, technology protection has the indirect effect of determining the behavior outcomes through the formation of confidence, perceived less vulnerability, and institutional assurance (Gefen et al., 2003; McKnight et al., 2011). This suggests that trustworthy AI architecture develops a safe governance system, which, in turn, can contribute to the increase in enterprise enthusiasm on AI-filled systems. Past research efforts in the field of cloud computing and digital transformation show that trust is often a channel of transmission between the technological potential and organizational acceptance behavior (Vial, 2021; Dwivedi et al., 2021). Also, the enterprise-based cybersecurity studies reveal that the organizations tend to perceive security investments as the tokens of reliabilities and commitment to governance throughout the long term (Alshamrani et al., 2022; Huang and Rust, 2021). Nonetheless, the available literature only looks at direct correlations between cloud security and adoption performance and ignores more socio-technical processes of how organizational confidence fosters. The most level-headed explanation is that existing technology-based models fail to offer a substantial perspective in the psychology and governance-based nature of AI uptake in a mutual cloud ecosystem. Accordingly, tenant trust is capable of being a theoretically significant mediating variable in the sense that it elucidates the connection that will exist between secure architecture and organizational adoption behavior in uncertain and risky conditions. So, it is assumed that:

H4: The mediating variable between secure multi- tenant AI architecture and enterprise AI adoption in the Salesforce cloud industry in India is the tenant trust.

Despite the fact that earlier studies have already done relevant contributions to cloud computing, AI governance, and enterprise-level digital transformation books, there are still gaps in concepts and methodologies that require filling. Current research mainly focuses on technical performance, scalability, or infrastructural optimization with a relatively minimal distinction to trust-driven organizational adoption processes in AI-enabled multi-tenant ecosystems (Benbya et al., 2021; Khan et al., 2022). In addition to this, lots of the earlier studies are based on either conceptual discussions or simulation-based studies instead of empirically testing the relationships among the latent variables by using sophisticated methods like PLS-SEM. Contextual constraints can also be observed as few studies focus on trust-based enterprise AI adoption in the Salesforce cloud sector of India that is strategically significant in global digital transformation. Hence, this study mitigates these shortcomings by incorporating the Trust Theory with the safeguarding multi-tenant artificial intelligence architecture and enterprise adoption of AI under the mediating influence of tenant trust, non-randomly providing a multifaceted socio-technical facial expression of toix AI adoption action in cloud-native business environments.

3. Research Methodology

The paper used a quantitative cross-sectional research design to find out the relationship between secure multi-tenant AI architecture, trust between tenants and enterprise adoption of AI in the Salesforce cloud industry in India. Quantitative approach was deemed suitable, since the research was meant to empirically test theoretically derived relationships between latent constructs by the use of statistical modelling techniques. Also, the cross-sectional design provided an opportunity to collect data on a significant number of respondents at a certain time, which simplifies the measurement of organizational attitudes to AI-enhanced cloud security and enterprise adoption behavior. Past research into information systems and cloud computing has used cross-sectional quantitative designs to study technology adoption and outcomes of organizational trust (Hair et al., 2021; Benbya et al., 2021). Since the proposed framework comprises mediation and predictive relationships, it was deemed that Partial Least Squares Structural Equation Modeling (PLS-SEM) is methodologically appropriate since it is predictive in orientation, complex models can be

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250-3552

analyzed without ignoring latent variables, and the technique allows studying the influence of multiple independent variables on a dependent one (Hair et al., 2022; Sarstedt et al., 2020).

The research was carried out in the Salesforce cloud sector in India. The selected audience comprised of IT managers, Salesforce administrators, cloud architects, cybersecurity professionals, AI consultants, and enterprise technology experts operating in companies that have Salesforce-based cloud systems. Only valid responses were collected to make final analysis based on 412 responses. The chosen sample size was found to be sufficient since PLS-SEM needs to have enough observations to guarantee statistical power and reliable estimation of the factors. The minimal integration of the sample size as mandated by the 10-times- regulation and recent methodology guidelines is generally larger than ten times the largest quantity of structural paths that can be directed at a construct (Hair et al., 2021). As the proposed model has moderate structural complexity and mediation relationships, a sample of 412 was sufficient to substantially address minimum methodological requirements, contributing to greater predictive precision of the model and robustness.

The research used purposive sampling and convenient sampling methods since the necessary condition was that the respondents be practicing knowledge of Salesforce cloud mechanisms, AI-powered enterprise software or cloud security governance. It was appropriate to use this sampling method since it is usual to find specialized enterprise technology professionals in cloud ecosystems to be limited and either context-specific. The respondents were referenced via professional networking sites, Sales Force community groups, enterprise technology forums, LinkedIn professional connections and organization contacts in Indian IT and cloud computing industry. Past studies of enterprise technology adoption have also been based on purposive when exploring more specialized technological settings (Dwivedi et al., 2021; Gupta et al., 2022). Hence, the chosen sampling provided the possibility to gather relevant and experience-related responses that are specific to the objectives of the study.

Structured questionnaire, which is destined to be distributed by the means of online survey, was used to gather data. The questionnaire was originally created with the help of the already tested measurement scale and then adjusted to the setting of secure multi-tenant AI architecture in Salesforce clouds. Before the mass distribution, the instrument has been assessed by two academic specialists in the field of cloud computing and information systems research and three practitioners in the sphere of Salesforce AI governance. To ensure clarity, reliability and contextual suitability of the measurement items, a pilot study was done with 35 respondents. Insignificant changes in word usage were made with the help of expert and pilot responses. The last questionnaire link was shared electronically with the help of emails in form of invitations, professional communities, as well as organizational networks. Four hundred and eighty-seven responses were received in total and seventy-five incomplete or inconsistent responses were then eliminated in data screening leaving 412 usable responses and an effective response rate of 84.6 percent. Before final analysis was conducted, missing values, outliers and inconsistency of responses were analyzed to test the quality and accuracy of the data.

The ratings were conducted on all constructs basing on pre-established scales that were based on prior literature. A six-item measuring scale based on studies of cloud security and enterprise AI governance created by Khan et al. (2022) and AlHogail (2021) were used to measure secure multi-tenant AI architecture. Tenant trust took the form of five items borrowed items based on the organizational trust scales created by Gefen et al. (2003) and McKnight et al. (2011). The six items to gauge adoption of enterprise AI were founded on technology adoption and enterprise AI integration literature created by Vial (2021) and Dwivedi et al. (2021). Each of the items was scaled with the seven-point Likert scale (1 = strongly disagree, 7 = strongly agree) due to the greater response sensitivity and better variance capture of behavioral studies with seven-point scales (Hair et al., 2021). The questions in the questionnaires were slightly modified to fit the

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250-3552

Salesforce cloud environment with conceptual similarity to the original scales. The entire questionnaire is presented in the Appendix section.

To determine the reliability and the consistency of the measure, reliability and validity tests were carried out. The Alpha of Cronbach was between 0.812 and 0.901 which is higher than the recommended value of 0.70 and indicates a high degree of internal consistency reliability (Nunnally and Bernstein, 1994). The Composite Reliability (CR) values were found to be between 0.861 and 0.924 thus affirming construct reliability. Convergent validity was confirmed since the Average Variance Extracted (AVE) values were 0.602-0.748 range, which is higher than the standard range of 0.50 suggested by Fornell and Larcker (1981). Besides, the validity of discriminants was tested either with the FornellLarcker criterion or the HeterotraitMonotrait Ratio (HTMT). The square roots of the AVE values were higher than the inter-construct correlations, and all the HTMT values were below the acceptable level of 0.85, which established good discriminant validity (Henseler et al., 2015).

The data obtained at the stage of the collection were analyzed by SmartPLS 4 and SPSS 27 applications. Descriptive statistics, preliminary screening and exploratory analysis were initially performed using SPSS whereas structural equation modeling and testing of hypotheses were performed using SmartPLS 4. The choice of PLS-SEM was due to the fact that the purpose of the study was to predict the adoption of AI in an enterprise and at the same time, investigate mediation relationships between the latent constructs. Besides, PLS-SEM is especially appropriate when dealing with non-normal data distribution and intricate structural models and exploratory and prediction flows of research (Hair et al., 2022; Sarstedt et al., 2020). Path coefficients, coefficient of determination (R^2), predictive relevance (Q^2), effect sizes (f^2) and bootstrapping procedures were used to evaluate the structural model. To evaluate the relationship of path and mediation effects, a bootstrapping process, composed of 5,000 resolves, was undertaken. To provide strong statistical inference, confidence intervals were also checked as well as t-values.

The entire research process was done with a lot of consideration of ethics. The survey was voluntary and the respondents were aware of the academic intent of the study and upon filling out the questionnaire. All participants gave an informed consent electronically and responses were kept confidential. They did not collect any personally identifiable data and all the data were utilized solely in academic research. It was also explained to the respondents that their decision to leave during the process would not negatively affect them.

Common Method Bias (CMB) was estimated by multitude of procedural and statistical means since the data on all variables were taken on the same respondents. To begin with, the Single Factor Test provided by Harman was done using exploratory analysis of factors but the outcomes showed that a single factor only captured 34.7 percent of the total variance, which was less than the suggested standard of 50 percent (Podsakoff et al., 2003). Second, full collinearity checking was conducted through an analysis of the all latent constructs variance inflation factor (VIF). The values of VIF were also in 1.42 to 2.68, which is significantly lower than the 3.3 value defined as a proper value by Kock (2015). The results show that the Common Method Bias was not a significant issue in the given research.

4. Data Analysis and Results

SPSS 27 and SmartPLS 4 were used to analyze the gathered data of 412 respondents. The initial pre-descriptive statistics and correlation analysis were prepared with the help of SPSS, whereas the measurement model evaluation, structural model testing, mediation analysis, and predictive relevance assessment were done with the use of SmartPLS 4. An analysis was performed using the two-step PLS-SEM approach proposed by Hair et al. (2022), which requires measuring models evaluation and structural models evaluation.

The demographical information showed that 34.2% of those that answered were IT managers, 26.5% Salesforce administrators, 18.7% cybersecurity professionals, and 20.6% cloud architects and AI consultants. Concerning experience in the organization, 41.5% had over five years of

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250-3552

experience in working with Salesforce cloud ecosystems. Moreover, 63.1% of participants were the medium and large enterprise organizations that are actively using the AI-powered Salesforce applications.

Table 1: Respondent Profile

Demographic Variable	Category	Frequency	Percentage
Position	IT Managers	141	34.2%
	Salesforce Administrators	109	26.5%
	Cybersecurity Professionals	77	18.7%
	Cloud Architects / AI Consultants	85	20.6%
Experience	1–3 Years	98	23.8%
	3–5 Years	143	34.7%
	More than 5 Years	171	41.5%
Organization Type	SMEs	152	36.9%
	Large Enterprises	260	63.1%

Descriptive statistics and correlation analysis are presented in Table 2. The findings indicated positive correlations among secure multi-tenant AI architecture, tenant trust, and enterprise AI adoption. Correlation coefficients remained below 0.90, indicating the absence of multicollinearity concerns.

Table 2: Descriptive Statistics and Correlation Matrix

Constructs	Mean	SD	SMAIA	TT	EAIA
Secure Multi-Tenant AI Architecture (SMAIA)	5.81	0.87	1.000		
Tenant Trust (TT)	5.63	0.91	0.684	1.000	
Enterprise AI Adoption (EAIA)	5.74	0.84	0.652	0.719	1.000

The measurement model was evaluated using indicator reliability, internal consistency reliability, convergent validity, and discriminant validity. Factor loadings for all measurement items exceeded the recommended threshold of 0.70. Cronbach's Alpha values ranged from 0.812 to 0.901, while Composite Reliability values ranged between 0.861 and 0.924. Furthermore, Average Variance Extracted (AVE) values exceeded the threshold value of 0.50, confirming convergent validity.

Table 3: Reliability and Convergent Validity Results

Constructs	Items	Cronbach's Alpha	Composite Reliability	AVE
Secure Multi-Tenant AI Architecture	6	0.901	0.924	0.748
Tenant Trust	5	0.854	0.892	0.623
Enterprise AI Adoption	6	0.812	0.861	0.602

Discriminant validity was assessed using the Fornell–Larcker criterion and HTMT ratio. The square root of AVE values exceeded inter-construct correlations, confirming satisfactory discriminant validity. Similarly, HTMT values remained below the recommended threshold of 0.85.

Table 4: Fornell–Larcker Criterion

Constructs	SMAIA	TT	EAIA
SMAIA	0.865		
TT	0.684	0.789	
EAIA	0.652	0.719	0.776

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250-3552

Table 5: HTMT Ratio Results

Constructs	HTMT Value
SMAIA → TT	0.742
SMAIA → EAIA	0.718
TT → EAIA	0.801

The results confirmed that the measurement model demonstrated satisfactory reliability and validity. After establishing measurement adequacy, the structural model was evaluated using bootstrapping procedures with 5,000 resamples. Path coefficients, t-values, and p-values were examined to test the proposed hypotheses.

The findings revealed that secure multi-tenant AI architecture positively influenced enterprise AI adoption ($\beta = 0.318$, $p < 0.001$), supporting H1. Similarly, secure multi-tenant AI architecture significantly influenced tenant trust ($\beta = 0.684$, $p < 0.001$), thereby supporting H2. Tenant trust also demonstrated a significant positive effect on enterprise AI adoption ($\beta = 0.497$, $p < 0.001$), confirming H3.

Table 6: Structural Model Results

Hypotheses	Relationship	Beta (β)	t-value	p-value	Decision
H1	SMAIA → EAIA	0.318	5.972	<0.001	Supported
H2	SMAIA → TT	0.684	14.863	<0.001	Supported
H3	TT → EAIA	0.497	9.144	<0.001	Supported

The coefficient of determination (R^2) values indicated moderate explanatory power. Secure multi-tenant AI architecture explained 46.8% of the variance in tenant trust, while the combined effects of secure multi-tenant AI architecture and tenant trust explained 58.2% of the variance in enterprise AI adoption. Predictive relevance (Q^2) values exceeded zero, confirming acceptable predictive capability.

Table 7: Coefficient of Determination and Predictive Relevance

Endogenous Constructs	R^2	Interpretation	Q^2	Predictive Relevance
Tenant Trust	0.468	Moderate	0.311	Strong
Enterprise AI Adoption	0.582	Moderate to Strong	0.387	Strong

Effect size analysis showed that secure multi-tenant AI architecture exerted a substantial effect on tenant trust and a moderate effect on enterprise AI adoption. Tenant trust also demonstrated a moderate effect on enterprise AI adoption.

Table 8: Effect Size (f^2) Results

Relationship	f^2	Interpretation
SMAIA → TT	0.621	Large
SMAIA → EAIA	0.214	Moderate
TT → EAIA	0.337	Moderate to Large

The mediation effect of tenant trust was examined using bootstrapping procedures. The indirect effect between secure multi-tenant AI architecture and enterprise AI adoption through tenant trust was statistically significant ($\beta = 0.340$, $p < 0.001$). Since both the direct and indirect effects remained significant, the findings confirmed partial mediation.

Table 9: Mediation Analysis Results

Mediation Path	Indirect Effect (β)	t-value	p-value	Mediation Type
SMAIA → TT → EAIA	0.340	7.826	<0.001	Partial Mediation

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250-3552

Model fit indices were also examined to assess overall model adequacy. The Standardized Root Mean Square Residual (SRMR) value was 0.052, remaining below the recommended threshold of 0.08. Similarly, the Normed Fit Index (NFI) value was 0.917, indicating satisfactory model fit.

Table 10: Model Fit Indices

Fit Index	Obtained Value	Recommended Threshold	Result
SRMR	0.052	< 0.08	Acceptable
NFI	0.917	> 0.90	Acceptable

A robustness check was additionally conducted through alternative model testing by removing the mediating construct from the structural framework. The explanatory power of enterprise AI adoption declined substantially from $R^2 = 0.582$ to $R^2 = 0.394$, confirming the importance and stability of tenant trust within the proposed model. Sensitivity analysis further indicated that all path relationships remained significant across subsamples, thereby demonstrating the robustness and reliability of the findings.

5. Discussion

This work supports the conclusion that secure multi-tenant AI architecture is relevant to enhancing the adoption of AI in the enterprise scale in the Salesforce cloud industry in India both directly and indirectly according to tenant trust. The findings indicate that organizations are not only assessing the utility of the AI-enabled cloud systems based on their efficiency in operation or technological advancement, but also prioritizing governance assurance, transparency, and trustworthiness as key measures. This means that socio-technical factors dramatically influence the process of the adoption of enterprise AI in the multi-tenant ecosystems, and not just infrastructural competencies. In addition, the paper shows the strategic role of the establishment of trust in AI-driven cloud computing, especially in emerging digital economies where the questions of cybersecurity and regulatory issues still factor in the choice of technology used by organizations. On the whole, the results contribute to the rising party that AI governance and security architecture are now become the most critical factors in sustainable enterprise digital transformation.

The initial key observation was secure multi-tenant AI architecture positively impacted the adoption of AI in the enterprise. The results are in line with the previous research that highlights the relevance of cloud security and governance tools in fostering the acceptance of technology in the organization (Dwivedi et al., 2021; Vial, 2021). On the same note, Benbya et al. (2021) opined that the more technological infrastructures are reliable, scalable, and ensure system operations, the ready enterprises adopt AI-enabled system. Nevertheless, the current investigation builds on prior studies by narrowing on multi-tenant AI ecosystems in Salesforce cloud platforms as opposed to investigating cloud adoption in larger or more general settings. This is explicable by the Trust Theory, which advocates the more the organization is prone to deal with technologically complex systems in reduction of uncertainty and perceived vulnerability by means of credible institutional protective measures (Gefen et al., 2003). Such a relationship seems to be especially significant in the Salesforce cloud market in India where businesses are already in an environment that is quickly becoming digitized with growing cybersecurity threats, changing compliance needs, and highly reliant on outsourced cloud infrastructures. It is a probable theory that organizations perceive secure AI architecture as not only a technical potential but also to demonstrate institutional trustworthiness and stability governing in the long term. This offers a new line of evidence that the adoption of enterprise AI in transformative economies is becoming more predetermined by trust-based security demands and not just by a perceived utility or cost-effectiveness.

The second result showed that secure multi-tenant AI architecture goes a long way to promote tenant trust. This finding is consistent with the previous study that indicates that organizational trust in the online setting depends on the presence of security assurance, encryption, and transparency of governance in a positive manner (McKnight et al., 2011; AlHogail, 2021). Recent cybersecurity research also highlighted that the attitudes of responsibility, accessibility, and

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250-3552

reliability in the protection of data are key conditions in the formation of trust with AI-promised ecosystems (Sarker et al., 2021; Tawalbeh et al., 2020). Nevertheless, other previous researchers convinced that the skepticism of the AI systems by the organizations could not be entirely affected by the high level of technical protection since the uncertainty can be introduced due to the lack of algorithms transparency and the autonomy of decisions of the system (Kshetri, 2021). The current results, to some extent, refute this issue by indicating that secure architectural systems in Salesforce cloud settings can significantly decrease this level of uncertainty and enhance the organizational trustworthiness. This once again can be explained based on Trust Theory in the sense that institutional confidence is gained when organizations feel that technological systems are doing a good job potentially reducing risk and safeguarding strategic assets. Contextually, this observation echoes the growing sensibility of Indian businesses on data management and network resilience especially following the proliferation of cloud-native models of business and AI-driven automation of key economic domains including banking, health, and IT delivery. Thus, the results indicate that trust in AI-based multi-tenant systems is not just automatically established, but it will develop through obvious and credible security structures, which will be integrated into the platform architecture.

The third observation validated that the trust of tenants has a positive impact on the adoption of enterprise AI. This has been supported by research indicating trust as a salient indicator of technology acceptance and firm commitment in digital ecosystem (Gefen et al., 2003; Vial, 2021). Also, Dwivedi et al. (2023) highlighted that organizational confidence has become a crucial factor that predetermines the readiness of an enterprise to implement AI-based technology in strategic operations. However, there had been a few previous studies, which assumed that the primary determinant of the enterprise adoption decision is more about economic or technological preparedness than about trust-related ones (Khan et al., 2022). Contrary, the current study proves that trust has been extremely dominating in AI-enabled cloud settings, which are marked by complexity and uncertainty regarding the governance. It builds upon Trust Theory by offering empirical data that organizational trust can be more than an emotion or relationship but a strategic process that influences enterprise-level behavior related to the adoption of AI. In the Salesforce cloud sector of India subsector, the relationship seems to be particularly applicable as companies are increasingly using third-party cloud platforms to conduct business-critical processes, yet, at the same time, there is an upsurge in worries about the issues of data sovereignty, cybercrime, and the responsibility to govern AI. This implies that enterprises embrace AI technology with less fear in a scenario where cloud platform is institutionally trusted and governance-driven. As a result, trust will strategically enable digital transformation through AI instead of merely being a background organizational culture.

The mediation results also indicated that the trust of tenants partly mediates the correlation between the secure multi-tenant AI architecture and the enterprise AI adoption. This observation is one of the most significant contributions of the research as it offers the description of the underlying mechanism of how secure AI architecture is transformed into the behavior of organizational adoption. However, past literature tended to investigate direct correlations between cloud security and the consequences of technology adoption (Benbya et al., 2021; Gupta et al., 2022), with a relatively small emphasis placed on exploring how trust may be the transmission mechanism that operates in AI-enabled multi-tenant ecosystems. This paper thus builds on the Trust Theory by proving that security architecture not only affects the adoption of AI at the enterprise level, but also the creation of organizational faith and organizational perceived assurance. One more likely reason is that it is not necessarily the case that enterprises solely react to technical sophistication as such; it is a matter of trust, reliable, and credibility to governance. This mediation effect is contextually significant in the enterprise cloud setting in India due to the existence of several conditions where organizations tend to operate in a space of regulatory flux, system vulnerability to cyber threats and a fast-paced technological change. In this situation, trust

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250-3552

will be a stabilizing factor that will decrease uncertainty and enhance organizational readiness to implement AI-enabled cloud solutions. This observation thus offers fresh indications that trust is the leading socio-technical mediator between safe architecture and business attitude towards adopting AI.

The results are all cumulative to some of the existing theoretical discussions about the association between technological capability and organizational adoption in AI-based cloud-ecosystems. Although the past technology acceptance models, including TAM, focus more on explaining adoption in terms of perceived usefulness and ease of use (Davis, 1989), the current research proposes that the models might be flawed in reflecting governance-related issues related to AI-enabled multi-tenant space. Trust Theory is a much more detailed explanation as it specifically deals with uncertainty reduction, institutional reliability and perception of vulnerability in technologically complex eco systems. Nonetheless, the results also provide some boundary conditions of Trust Theory since organizational trust can be interacted with regulatory structures, industry sensitivity, or national policies on cybersecurity, which can be different situation-to-situation. This implies that future researchers should extend the investigation of how institutional environment and maturity of governance impacts the development of trust-based AI adoption processes in various countries and cloud markets.

6. Theoretical and Practical Implications

The results of this research lead to a number of significant effective implications to include in the work of enterprise administrators, cloud designers, cybersecurity experts, artificial intelligence governance experts, and policymakers working in the Salesforce cloud environment of India. First, the findings show that secure multi-tenant AI architecture plays a crucial role in enhancing AI adoption in the enterprise and businesses ought to consider security-focused infrastructure solutions when deploying AI-enabled cloud infrastructures. Secure architectural tools, which may include tenant isolation protocols, zero-trust access control, encryption tools, and AI-driven threat detection can help managers instill greater confidence in the organization and fast-track enterprise AI adoption. It especially applies to Indian companies that work in highly competitive and digit-heavy industries where an uncertainity around cybersecurity can deter the use of AI on a mass-scale basis. Thus, organizations should consider security architecture as a compliance desire but an element of sustainable digital transformation as well as enterprise innovation.

The results also indicate that the role of a tenant trust is instrumental to enhance the enterprise AI adoption. It implies that organizations must be keen on investing in trust-building processes as well as the development of technological infrastructure. To boost the trust of the tenants, enterprise decision-makers may create more transparency in AI governance, reinforce communication on the topic of data protection policy, and introduce explainable AI practices, which lessen uncertainties about using automated decision-making. Moreover, the cloud service provider and Salesforce implementation partners may come up with governance-owning AI frameworks that expressively illustrate accountability, reliability, and compliance preparedness. One possible reason is that businesses are becoming more receptive to using AI-enabled systems when the security systems are perceived as familiar, open, and institutionally trustworthy instead of technical systems. Trust management in organizations, therefore, needs to be incorporated in larger cloud governance measures to enhance the long-term enterprise AI acceptance.

The practical implications are also of great importance to policy makers and other regulatory organizations in charge of cloud governance in the growing cloud computing sector in India. The results suggest that secure AI ecosystems and organizational trust are tightly related to each other, which means that the regulation frameworks must go beyond the technical compliance criteria and fill them with governance transparency, cybersecurity assurance, and responsible AI practices. These results can inform policymakers to devise institutional regulations that can enhance safe deployment of AI in multi-tenant enterprise ecosystems, as well as bolster organizational trust in cloud-native technologies. In addition, regulators in the industry can assist in standardizing AI

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250-3552

governance certification and security auditing controls to lessen the doubt among firm consumers. Especially in the case of emerging economies such as India where the digital transformation often leaves the governance adaptation process and development of institutional trust far behind, such initiatives can become highly significant.

Regarding the industry, the study offers practical advice to Salesforce consultants, cloud service providers, and enterprise technology vendors that aim at enhancing the adoption of AI-enabled services within organizations. The study indicates that enterprises consider AI-based cloud platforms based on not only operations but also on liberated governance reputation and safety guarantee. Thus, cloud providers have a chance to enhance the competition in the market by incorporating trust-based design to AI-driven Salesforce solutions. This involves enhancing visibility at the tenant level, enhancing governance reporting, and adaptive cybersecurity structures that could help resolve emerging AI-related vulnerabilities. Moreover, the introduction of training programs on AI governance literacy and cybersecurity awareness can contribute to keeping organizations less doubtful about the need to adopt AI and become well-prepared to adopt it in the enterprise setting.

The research also has significant theoretical implications as it makes the extension of Trust Theory to the context of AI-enabled multi-tenant cloud systems. Established trust research has mostly concentrated on e-commerce or transactional online, or an overall technology adoption setting (Gefen et al., 2003; McKnight et al., 2011). By contrast, this paper uses Trust Theory in enterprise AI governance and secure cloud architecture of Salesforce cloud business in India. This puts the theory further by showing that organizational trust is not restricted to either interpersonal or transactional conditions but also plays the role of a strategic force in the process of entering an enterprise by a complex and security sensitive technology environment. The results thus give fresh pieces of evidence that trust is at centre of even the most sophisticated AI based ecosystem where even organizational decisions incorporate institutional reliability, governance assurance, and cyber risk testing.

The study also has a theoretical contribution in that the concept of tenant trust mediates the variables between secure multi-tenant AI architecture and enterprise AI adoption. Previous research tended to respond to the questions of direct associations between technological infrastructure and organizational performance with a relatively little focus on the socio-technical processes involved in adoption behavior formation (Benbya et al., 2021; Vial, 2021). The current results counter this weakness by showing that secure AI architecture impacts the enterprise adoption behaviors to some extent, because they involve the mechanisms of trust. It implies that the reaction of organizations to AI-supported cloud systems depends not only on its technological capacity but also on the ability to feel that there is regulated security and institutional guarantees. Thus, tenant trust inclusion offers a more detailed explanatory factor that reinforces the theoretical insight into the application of enterprise AI in the context of cloud-native.

The work also adds to the AI governance and cloud computing literature by uniting both infrastructural security outlooks and behavioral and organizational trust facets. Past studies tended to accept cloud security as a technical structure related either with an encryption mechanism, scalability, or an access privilege (Khan et al., 2022; Tawalbeh et al., 2020). Nonetheless, the current results indicate that safe AI architecture is also a symbolic indicator of governance that has an impact on the organizational views and strategic choices of technology. This brings in a more bold socio-technical eye that relates the capability of cybersecurity to organizational formation of trust and enterprise innovation. This strategy can help to fill the conceptual gap between the technology-focused and behavior-based research streams of literature on enterprise AI adoption.

One of the other valuable theoretical implications is connected to the contextual progress. The current literature on AI governance and cloud adoption has been mainly created in a Western or highly developed digital economy. This research is valuable as it offers empirical data of Salesforce cloud industry in India, thus increasing the geographical and institutional scope of the

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250-3552

Trust Theory. The current results demonstrate that the trust-based adoption mechanisms can still be greatly applicable in emerging digital economies, which are marked by the active technological growth, new cybersecurity policies, and institutional change. Such a contextual input is especially significant as the interaction of organizations with AI governance and cloud security can be highly different across countries and industries. Thus, the research makes a theoretical generalizability more robust and at the same time points to the significance of the context sensitivity in enterprise AI adoption research.

7. Conclusion

This paper has analyzed the linkage between secure multi-tenant AI architecture and enterprise AI adoption in light of Indian Salesforce cloud industry mediated by the elements of tenant trust. The study is based on the Theory of Trust seeking to elucidate the effects of organizational trust processes on the enterprise adoption decision-making in AI-enabled multi-tenant cloud solutions with complicated technology and unpredictable cybersecurity. These results indicated that secure multi-tenant AI architecture outperforms highly in enhancing the probability of enterprise AI adoption besides adding to the trust that tenants have in the AI architecture which in turn promotes the willingness of an organization to adopt AI-managed cloud architecture. More to the point, the research affirmed that tenant trust is a key socio-technical tool that connects safe AI architecture to behaviors in enterprise adoption.

The paper is an addition to the expanding body of research on AI governance as well as cloud computing and enterprise digital transformation by applying the Theory of Trust to AI-facilitated multi-tenant cloud environments. Contrary to other technology-oriented researches that have mostly concentrated on the infrastructural performance or operational efficiency of the technology, the current study has concentrated on the strategic nature of trust development in influencing the decision to adopt AI within companies. This is an important contribution in that it shows that technical capability is not the only factor that makes organizational responses to AI-enabled systems work out, with the assurance of governance, security credibility, and institutional reliability playing significant roles, as well.

In practice, the results can offer beneficial insights to managers and cloud service providers of enterprises, AI governance experts, and policymakers aiming to build organizational trust in AI-enhanced cloud ecosystems. The research proposes that the enterprises could enhance the results of AI adoption by implementing trust-related governance frameworks and security-focused architectural designs to their cloud systems. In the fast-growing digital economy of India, the findings can provide organizations with insights in a timely manner when they are trying to find a balance between technological innovation and cybersecurity reassurance and building trust in the institution.

8. Limitations and Future Research

Although the present research has its theoretical and practical input, some limitations to it can be identified. To begin with, the study was examined solely in the Salesforce cloud industry of India which could restrict the generalization of the study to various national, institutional and industrial settings. The responses of organizations to ensure the security of AI architecture and to gain trust of tenants might differ significantly among countries with varying regulatory environments, digital maturity, and cybersecurity regulatory frameworks. Thus, despite the fact that the findings are giving significant insights into the emerging digital economies, there should be caution when generalizing the findings to highly developed or institutionally distinct cloud ecosystems.

Secondly, the research used cross-sectional survey data obtained at a single time of professionals working in enterprises. Although this was suitable in testing the relationships among the latent constructs utilizing PLS-SEM, this method also limits the capability to derive relationships among secure multi-tenant AI architecture, tenant trust and enterprise AI adoption on a long-term basis. Trust in organizations and the uptake behavior of AI could change over time as business organizations have more experience with AI-enabled cloud computing or could face different

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250-3552

cybersecurity issues. In turn, temporal stability of the relationships observed still presents a significant limitation.

Third, the study employed self-reported data in questionnaires and this could create a side effect of biasing response or have a perceptual subjectivity in respondent despite the procedures remedies and Common Method Bias tests. Even though the scales used to measure the different variables had been modeled on the existing literature, and had proved acceptable reliability and validity, there is a possibility that the opinions of the respondents are not the best measure to get a real picture of the organizational security practices/technologies. The most likely rationale is that the expectations of enterprise professionals regarding AI governance and their trust might vary based on their role in an organization, their technological background or their cybersecurity history.

The second limitation speaks of a conceptual focus of the work. In its particular study on secure multi-tenant AI architecture and enterprise AI adoption, the research investigated the ability of the tenant trust as a mediating variable. Although this offered a theoretically grounded explanation that is in line with the Trust Theory, other factors that could have been of relevance within the organization or institution were not included in the framework. Thus, the framework is to be understood as a specialized socio-technological account as opposed to a completely exhaustive portrayal of enterprise AI adoption behaviour in cloud environments.

The restrictions provide a number of valuable future research directions. To start with, the proposed framework should be tested in various countries and industries in the future to assess the universality of the results. Comparative research on advanced and new digital economies can be used to gain more insight into how institutional maturity, cybersecurity laws, and cultural variations can affect mechanisms of trust in AI adoption. Further research can also expand the model to other sectors of cloud computing besides Salesforce ecosystems, such as cloud computing used in health care, financial technology systems or infrastructure, or AI systems in the public sector.

Second, longitudinal research designs need to be considered in future studies aimed at studying the dynamics of organizational trust and enterprise AI adoption with time. Longitudinal designs could also be more causal in the sense that they can offer the chance of the relationship between secure AI architecture and enterprise adoption behavior as well as record changes, which may be linked to technological adaptation, governance evolution, or cybersecurity incidents. These designs can also reinforce the theoretical knowledge on the creation of trust in evolving AI-supported cloud systems.

Third, one can take into account other theoretically justified constructs in the future to increase the explanatory ability of the model. The AI governing transparency, cybersecurity preparedness, pressure exerted on regulatory compliance, organizational resilience, or the explainable AI capability may be better-explaining variables on the process of adopting AI in an enterprise. But these extensions must be kept to a theoretical level, to prevent fragmentation of concepts, and to maintain coherence in analysis.

Lastly, subsequent research techniques can be improved with the use of mixed-method research or multi-source techniques. Open-ended interviews with enterprise decision-makers, cyber experts and cloud architectures might yield more contextual information as to how organizations see trust, governance assurance and AI security in multi-tenant ecosystems. Improving contextual interpretation and enhancing the theoretical refinement of AI-assisted cloud governance studies which involve the integration of both quantitative and qualitative evidence could thus enhance the studies.

References

- AlHogail, A. (2021). Improving IoT technology adoption through improving consumer trust. *Technological Forecasting and Social Change, 172*, 121024. https://doi.org/10.1016/j.techfore.2021.121024

- Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials, 21*(2), 1851–1877. https://doi.org/10.1109/COMST.2019.2891891
- Benbya, H., Pachidi, S., & Jarvenpaa, S. (2021). Artificial intelligence in organizations: Implications for information systems research. *Journal of Business Research, 124*, 547–560. https://doi.org/10.1016/j.jbusres.2020.09.065
- Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly, 37*(2), 471–482. https://doi.org/10.25300/MISQ/2013/37:2.3
- Chin, W. W. (1998). The partial least squares approach to structural equation modeling. In G. A. Marcoulides (Ed.), *Modern methods for business research* (pp. 295–336). Lawrence Erlbaum Associates.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340. https://doi.org/10.2307/249008
- Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., & Williams, M. D. (2021). Artificial intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management, 57*, 101994. https://doi.org/10.1016/j.ijinfomgt.2019.08.002
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.1177/002224378101800104
- Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51–90. https://doi.org/10.2307/30036519
- Gupta, M., Gupta, S., & Singhal, A. (2022). Artificial intelligence adoption in Indian organizations: The moderating role of organizational culture. *Journal of Enterprise Information Management, 35*(6), 1715–1738. https://doi.org/10.1108/JEIM-10-2021-0435
- Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2021). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). Sage Publications.
- Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review, 31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8
- Huang, M. H., & Rust, R. T. (2021). A strategic framework for artificial intelligence in marketing. *Journal of the Academy of Marketing Science, 49*(1), 30–50. https://doi.org/10.1007/s11747-020-00749-9
- IBM Security. (2021). *Cost of a data breach report 2021*. IBM Corporation. https://www.ibm.com/reports/data-breach
- Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer trust in an internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication, 5*(2), JCMC526. https://doi.org/10.1111/j.1083-6101.1999.tb00337.x

- Khan, M. A., Salah, K., & Jayaraman, R. (2022). Blockchain-based secure data sharing in cloud computing: A survey. *Future Generation Computer Systems, 131,* 140–151. https://doi.org/10.1016/j.future.2022.01.012
- Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration, 11*(4), 1–10. https://doi.org/10.4018/ijec.2015100101
- Kshetri, N. (2021). Evolving uses of artificial intelligence in human resource management in emerging economies. *International Journal of Information Management, 57*, 102099. https://doi.org/10.1016/j.ijinfomgt.2020.102099
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334–359. https://doi.org/10.1287/isre.13.3.334.81
- Modi, K., & Patel, H. (2022). Multi-tenant cloud architecture optimization for enterprise systems. *Cluster Computing, 25*(4), 2985–3001. https://doi.org/10.1007/s10586-022-03688-z
- Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *Journal of Marketing, 58*(3), 20–38. https://doi.org/10.1177/002224299405800302
- Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.
- Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879
- Porter, M. E., & Heppelmann, J. E. (2015). How smart, connected products are transforming companies. *Harvard Business Review, 93*(10), 96–114.
- Rai, A., Constantinides, P., & Sarker, S. (2019). Next-generation digital platforms: Toward human-AI hybrids. *MIS Quarterly, 43*(1), iii–ix. https://doi.org/10.25300/MISQ/2019/13700
- Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.
- Sarstedt, M., Hair, J. F., Cheah, J. H., Becker, J. M., & Ringle, C. M. (2020). How to specify, estimate, and validate higher-order constructs in PLS-SEM. *Australasian Marketing Journal, 27*(3), 197–211. https://doi.org/10.1016/j.ausmj.2019.05.003
- Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. *Journal of Big Data, 8*(1), 1–27. https://doi.org/10.1186/s40537-021-00446-1
- Shmueli, G., Sarstedt, M., Hair, J. F., Cheah, J. H., Ting, H., Vaithilingam, S., & Ringle, C. M. (2019). Predictive model assessment in PLS-SEM. *European Journal of Marketing, 53*(11), 2322–2347. https://doi.org/10.1108/EJM-02-2019-0189
- Taleb, T., Samdanis, K., Mada, B., Flinck, H., Dutta, S., & Sabella, D. (2017). On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration. *IEEE Communications Surveys & Tutorials, 19*(3), 1657–1681. https://doi.org/10.1109/COMST.2017.2705720
- Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT privacy and security: Challenges and solutions. *Applied Sciences, 10*(12), 4102. https://doi.org/10.3390/app10124102
- Teece, D. J. (2018). Business models and dynamic capabilities. *Long Range Planning, 51*(1), 40–49. https://doi.org/10.1016/j.lrp.2017.06.007

- Vial, G. (2021). Understanding digital transformation: A review and research agenda. *The Journal of Strategic Information Systems, 30*(2), 101626. https://doi.org/10.1016/j.jsis.2020.101626
- Wamba, S. F., Queiroz, M. M., Wu, L., & Sivarajah, U. (2020). Big data analytics-enabled sensing capability and organizational outcomes. *International Journal of Information Management, 50*, 1–15. https://doi.org/10.1016/j.ijinfomgt.2019.04.015
- Wirtz, B. W., Weyerer, J. C., & Sturm, B. J. (2020). The dark sides of artificial intelligence: An integrated AI governance framework for public administration. *International Journal of Public Administration, 43*(9), 818–829. https://doi.org/10.1080/01900692.2020.1749851
- Yoo, Y., Boland, R. J., Lyytinen, K., & Majchrzak, A. (2012). Organizing for innovation in the digitized world. *Organization Science, 23*(5), 1398–1408. https://doi.org/10.1287/orsc.1120.0771