Enhancing Trust and Reducing Human Error in Cloud Adoption through Adaptive Security Awareness

Mr. Pragnya Ranjan Dash
CSE Department
MITS
Rayagada, Odisha.
dash.pragnya@gmail.com

Mr. Ramanuja Nayak
CSE Department
MITS
Rayagada, Odisha.
ramanuja.nayak@gmail.com

*Abstract-**Cloud computing has become a backbone of modern digital infrastructure, offering scalability, flexibility, and cost efficiency across industries. However, its rapid adoption continues to face significant barriers due to human-cantered security risks such as user errors, poor security practices, and lack of trust in service providers. While existing research has largely concentrated on technical mechanismssuch as encryption, authentication, and intrusion detectionthere remains a critical gap in addressing the human and behavioural dimensions of cloud security. This study aims to bridge that gap by exploring new approaches that combine technological solutions with user-centric strategies. We propose the development of AI-driven adaptive security awareness systems capable of monitoring user behaviour in real-time and delivering personalized alerts, training, or corrective feedback when risky actions are detected. In parallel, this research introduces trust models and transparency dashboards designed to quantify and visualize the reliability, compliance, and performance of cloud service providers, enabling organizations and individuals to make more informed trust decisions. Furthermore, the study investigates the behavioural and cultural factors influencing cloud security adoption within enterprises and government sectors, with the goal of identifying best practices for fostering a security-conscious culture.*
By integrating these three dimensionsadaptive awareness, transparent trust modelling, and behavioural analysisthe research proposes a comprehensive human-cantered security framework for cloud computing. Such a framework not only mitigates risks stemming from human error but also enhances user confidence and organizational resilience in adopting cloud technologies. Ultimately, this work contributes to the design of safer, more transparent, and trustworthy cloud ecosystems capable of supporting the growing global reliance on cloud services.

Keywords: Cloud Computing Security, Human-Centered Security, Trust Models, Adaptive Security Awareness, AI-Driven Security Systems, Transparency Dashboards, Behavioral Security Adoption, Cloud Trust Framework.

I. INTRODUCTION

Cloud computing has become one of the most transformative innovations in the digital era, reshaping how individuals, enterprises, and governments manage data, applications, and infrastructure. By offering on-demand scalability, cost efficiency, and accessibility, cloud platforms provide organizations with the flexibility to innovate without the burden of maintaining extensive physical hardware. Services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) have enabled businesses to optimize resources, streamline operations, and accelerate digital transformation. Despite these benefits, cloud adoption continues to face serious challenges concerning security, privacy, and trust.

Traditionally, research and industry practices in cloud security have concentrated on technical safeguards—including encryption, secure authentication, access control mechanisms, intrusion detection, and compliance with legal frameworks. While these approaches are critical, they often assume that technology alone can prevent breaches. However, the reality shows that human factors are among the weakest links in cloud security. Misconfigurations of cloud services, negligence in applying security patches, use of weak or repeated passwords, and improper handling of sensitive information are frequently cited as leading causes of data breaches in cloud environments. Thus, human error is not merely incidental but a core security challenge in cloud computing.

Another major obstacle is the issue of trust in cloud service providers (CSPs). Organizations and end-users often lack transparency into how their data is handled, stored, and protected. Concerns over vendor reliability, compliance with data protection regulations, and accountability in case of breaches lead to hesitation in fully embracing cloud technologies. Industries that deal with highly sensitive data, such as healthcare, government, and finance, remain particularly cautious, as a lack of trust in CSPs can directly affect decision-making processes and long-term adoption strategies. Addressing these human-cantered dimensions of cloud

security—both reducing human error and strengthening trust—is essential for ensuring a secure, transparent, and reliable cloud ecosystem. This research aims to fill that gap by exploring solutions that go beyond purely technical safeguards. Specifically, three interlinked approaches are proposed:AI-Driven Adaptive Security Awareness Systems: Unlike static training modules, adaptive systems powered by artificial intelligence can monitor user behaviour in real time. By detecting potentially risky actions, such as insecure login attempts, unusual access patterns, or improper file sharing, these systems can provide personalized alerts, corrective feedback, and micro-learning interventions. This ensures that users not only recognize security risks but also learn how to respond effectively, thereby reducing the likelihood of costly mistakes.

Trust Models and Transparency Dashboards: To enhance confidence in CSPs, there is a need for frameworks that quantify and visualize trustworthiness. Proposed transparency dashboards would allow users and organizations to assess metrics such as service uptime, compliance with regulations, historical breach data, and adherence to privacy policies. By making these metrics visible and standardized, CSPs can be held accountable, and users can make informed decisions about which providers best meet their trust requirements.Behavioural and Cultural Dimensions of Cloud Security Adoption: Technology adoption is not purely a technical issueit is also influenced by organizational culture, training practices, and human behaviour. Employees' attitudes towards security policies, willingness to adopt best practices, and level of security awareness play a vital role in shaping outcomes. This research will therefore investigate how behavioural science and cultural analysis can be integrated into cloud security strategies, creating a security-conscious environment where best practices are not enforced but naturally adopted.By integrating these approaches, this study proposes the design of a comprehensive human-cantered security framework. Such a framework will not only mitigate vulnerabilities caused by human error but also foster a culture of trust and accountability between users and cloud service providers. Unlike existing models that focus narrowly on technical controls, this framework acknowledges that people are both the greatest asset and the greatest risk in cloud security.

The significance of this research lies in its interdisciplinary approach, combining elements of artificial intelligence, trust management, behavioural science, and cloud computing. As organizations increasingly rely on cloud technologies for critical operations, developing solutions that address both the technical and human sides of security will be vital. Ultimately, this research seeks to contribute to the creation of safer, more transparent, and more trustworthy cloud ecosystems, capable of supporting the demands of a rapidly evolving digital economy.

II. LITERATURE REVIEW

The increasing dependence on cloud computing has attracted substantial research attention, particularly in the domains of security and privacy. Early studies in this field focused primarily on technical aspects such as encryption methods, access control mechanisms, and compliance with international regulations. Scholars such as Sun et al. (2020) and Zhang et al. (2010) highlighted that these technological safeguards remain essential for protecting data integrity, preventing unauthorized access, and ensuring compliance with standards such as GDPR and HIPAA. However, more recent findings reveal that breaches often occur not because of technological deficiencies but due to human mistakes and behavioural shortcomings. Misconfigurations of cloud storage, weak password practices, negligence in applying patches, and failure to follow basic security protocols are among the most common causes of cloud-related security incidents.

Ravi Shanker Singh and colleagues (2024) emphasize that a majority of cloud breaches can be traced to human factors, either directly through mismanagement or indirectly through non-compliance with organizational policies. This observation has shifted the research lens toward understanding human error as a core component of cloud vulnerability. The reliance on static awareness programs or one-time training sessions has proven inadequate in addressing the dynamic nature of security risks. As Swapnil Raj (2018) notes, conventional training often fails to prepare users for real-time threats, leaving a critical gap in the practical application of security knowledge. This suggests that cloud adoption requires adaptive, context-sensitive solutions that continuously engage with users rather than relying solely on traditional instruction.Parallel to the issue of human error is the equally significant concern of trust in cloud service providers. Organizations and individuals remain cautious about migrating sensitive workloads to the cloud due to uncertainties surrounding data ownership, privacy policies, and accountability. Misra and Kumar (2024) argue that transparency remains one of the weakest links in the cloud adoption chain. Clients frequently lack visibility into how providers handle data, respond to breaches, or comply with legal frameworks. This lack of clarity undermines trust, especially in sensitive industries such as healthcare, finance, and government, where confidentiality and reliability are paramount. Although several scholars have proposed theoretical trust models that quantify reliability and performance, few practical implementations exist that make such metrics visible and accessible to users in the form of dashboards or standardized reports. As Ghosh et al. (2024) argue, trust in cloud ecosystems is not only a technical challenge but also a psychological and organizational issue that must be addressed to achieve widespread adoption.

Recent literature has also begun to explore the role of artificial intelligence in mitigating risks associated with human behaviour in cloud environments. AI-driven systems have the capacity to detect anomalies in user activity, such as irregular login times or unusual file access, and can provide real-time feedback to prevent potential security breaches. Syed Prabakar et al. (2023) highlight that adaptive learning mechanisms, when integrated with cloud systems, can act as continuous awareness tools that respond to evolving threats rather than relying on outdated or generic training modules. This represents a significant advancement over conventional awareness strategies, offering an opportunity to reduce human error by transforming education into an ongoing, interactive process. Nevertheless, while the potential of AI in this context is acknowledged, comprehensive frameworks that combine adaptive awareness with trust-building mechanisms are still in their infancy.In addition to technological innovations, behavioural and cultural factors play a decisive role in shaping cloud security outcomes. Abhishek Gautam et al. (2022) note that employees often bypass security protocols for convenience or efficiency, thereby creating vulnerabilities despite the presence of technical safeguards. Similarly, Uzoma and Okhuoya (2022) observe that cultural perceptions of risk and trust vary across organizations and regions, influencing the degree of caution or openness toward cloud adoption. Organizational culture, leadership support, and employee attitudes collectively determine the extent to which security policies are respected and implemented. Tajinder Kaur and Sushil Kamboj (2023) emphasize that cloud security should be approached not only as a technical challenge but also as a social process shaped by behaviour, awareness, and cultural dynamics.

The review of existing literature therefore highlights several interconnected challenges. While significant progress has been made in developing technical defences, these measures alone are insufficient to guarantee secure and trustworthy cloud environments. The persistence of human error demonstrates the need for adaptive awareness systems that operate in real time, leveraging AI to provide contextualized guidance and training. At the same time, the ongoing trust deficit between users and service providers underscores the necessity of transparent models that quantify and visualize provider reliability and accountability. Furthermore, the influence of organizational behaviour and cultural contexts reveals that security adoption strategies must go beyond universal technical solutions and instead adapt to human and institutional realities.Overall, the literature converges on the understanding that a purely technical approach to cloud security is inadequate. Effective solutions must be human-cantered, combining adaptive technologies with behavioural insights and transparent trust mechanisms. However, despite growing recognition of this need, research that integrates these dimensions into a unified framework remains limited. It is within this gap that the present study positions itself, aiming to propose a holistic approach that enhances trust and reduces human error in cloud adoption through adaptive security awareness.

III. TECHNICAL ROUTE

3.1 TECHNICAL ROUTE OF R&D PROCESS

The research and development (R&D) process for this study follows a structured technical route that blends cloud-native methodologies with human-cantered design principles. Unlike traditional linear processes, this approach adopts a continuous, iterative cycle of data collection, model development, system integration, and user validation. The foundation of the research is the creation of a high-quality dataset that combines technical logs from cloud environments with user behaviour metrics. These include authentication attempts, access logs, misconfiguration incidents, and survey-based trust evaluations. The collected raw data undergoes cleaning, anonymization, and feature extraction to ensure both privacy protection and usability for modelling. To maintain reproducibility, the study employs a containerized environment for system and model development. Each componentincluding anomaly detection models, adaptive awareness engines, and trust visualization dashboardsis packaged with its dependencies using Docker or Kubernetes-based containers. This ensures consistency across different testing environments and allows other researchers to replicate and validate the experimental setup.

The core of the technical route is an AI-driven adaptive awareness pipeline. Once behavioural data is ingested, machine learning models analyse patterns to identify risky user actions such as insecure file sharing, repeated failed login attempts, or abnormal access behaviours. The system then triggers personalized, real-time micro-interventions, including alerts, just-in-time training snippets, or corrective prompts. This automated process creates a continuous feedback loop where each iteration refines the accuracy of the system, enabling rapid adaptation to emerging threats and evolving user behaviours. In parallel, a trust model development stream quantifies cloud service provider reliability. Trust indicators such as service uptime, compliance certifications, breach history, and transparency in data handling are aggregated into a trust dashboard. This dashboard provides users with a visual and measurable way to evaluate and compare providers, thereby enhancing decision-making and reducing psychological barriers to adoption. The R&D process concludes with the integration of the adaptive awareness engine and trust dashboard into a unified framework. This framework is evaluated through simulation experiments, user case studies, and expert reviews. The results are systematically analysed to assess how effectively the system reduces human errors and strengthens user trust. The path from research to practice ensures that the framework can be seamlessly integrated into enterprise cloud environments, offering scalable, transparent, and adaptive security support.

3.2 TECHNICAL ROUTE OF AUTOMATIC OPERATION AND MAINTENANCE

The technical route of the proposed framework is a continuous human-in-the-loop feedback cycle that integrates monitoring, intelligent analysis, and adaptive awareness across the lifecycle of cloud adoption. The process begins with multi-layered monitoring, which captures both technical metrics and human interaction data. On the technical side, monitoring includes infrastructure health, service availability, and network activity, while on the human side, it tracks login behaviours, configuration actions, and error-prone activities.When anomalies or risky

behaviours are detected, predefined thresholds trigger automated adaptive interventions. For example, if repeated login failures occur, the system provides instant guidance on password practices or initiates multifactor authentication prompts. Similarly, if sensitive data is accessed outside of policy guidelines, a real-time notification and corrective workflow are activated. These adaptive mechanisms act not only as preventive controls but also as learning tools that gradually enhance user awareness.In parallel, the trust dashboard continuously collects and updates data from cloud service providers. By applying machine learning to historical and real-time provider performance data, the system generates dynamic trust scores. These scores are visualized through an interactive interface, enabling users and organizations to make informed decisions about provider reliability. The feedback loop ensures that trust evaluations are not static but evolve with provider behaviour over time.The final layer of the technical route emphasizes post-incident learning and cultural integration. Collected behavioural data and incident logs are analysed to conduct root cause evaluations, identifying recurring mistakes and training gaps. Insights are fed back into the adaptive system to refine interventions and awareness prompts. At the organizational level, aggregated data supports security culture assessments, guiding policy updates and tailored training initiatives.

By closing the gap between reactive security measures and proactive trust-building, the proposed technical route enables a resilient, transparent, and human-cantered cloud adoption model. It ensures that security is not only enforced by technology but also understood and internalized by users, thereby strengthening overall resilience and confidence in cloud ecosystems.

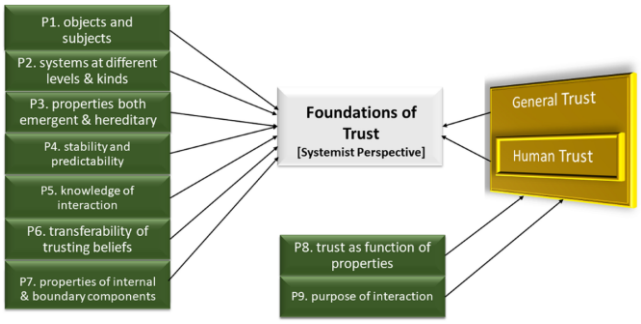

Fig. 1. Technical Route of Human-Centered Security and Trust Framework

This figure illustrates the structured research route for enhancing trust and reducing human error in cloud adoption. The process begins with data collection and processing, followed by the design of an AI-driven adaptive awareness system that delivers real-time alerts and corrective feedback. Parallel development of a trust model and transparency dashboard ensures measurable evaluation of cloud service providers, while behavioral and cultural analysis integrates human factors into the system. All streams converge into a unified human-centered cloud security framework, providing a proactive and transparent solution for secure cloud adoption.

IV. PROBLEM STATEMENT

Cloud computing has emerged as a critical enabler of digital transformation across industries, providing organizations with the ability to scale operations, optimize costs, and access cutting-edge computational resources. However, the rapid adoption of cloud technologies has been accompanied by persistent challenges in the domain of security and trust. A closer examination of recent security incidents reveals that human error has consistently remained one of the most significant contributors to cloud-related vulnerabilities. Misconfigurations of cloud environments, the use of weak or repeated passwords, improper handling of sensitive data, and the neglect of timely software patching are recurrent issues. Even in cases where robust technical safeguards such as encryption and access controls are in place, breaches often occur due to mistakes made by end-users or administrators. This highlights a paradox within cloud security: while technological solutions have advanced considerably, they remain ineffective if the human element is not adequately addressed.

Another pressing issue is the lack of transparency and trust in cloud service providers (CSPs). Organizations, particularly those in sensitive sectors such as healthcare, government, and finance, are often reluctant to fully migrate to the cloud due to concerns over data ownership, regulatory compliance, and accountability in the event of breaches. While providers may claim adherence to industry standards and certifications, customers frequently lack access to clear, measurable evidence of reliability and compliance. This opacity creates hesitation and slows down the adoption of cloud services, as organizations remain uncertain about the integrity and trustworthiness of providers. Without a structured mechanism for evaluating and visualizing provider reliability, trust remains largely subjective and unquantifiable, leaving a significant gap in the decision-making process.

Equally important, current approaches to security awareness and user training are static and outdated. Traditional methods, such as periodic training workshops or static e-learning modules, fail to adapt to the evolving threat landscape and do not provide real-time guidance to users when they encounter risky situations. Consequently, users often repeat the same errors, and organizations are left exposed to avoidable vulnerabilities. Furthermore, the behavioural and cultural aspects of cloud adoption have been insufficiently explored in both research and practice. Organizational culture, employee attitudes toward compliance, and regional perceptions of risk strongly influence the effectiveness of security policies, yet these dimensions are rarely integrated into technical frameworks. The absence of a holistic approach that accounts for human behaviour, cultural contexts, and trust-building mechanisms creates a research gap that must be addressed. This study positions itself within that gap, aiming to develop a human-cantered security framework that reduces errors, enhances transparency, and strengthens trust in cloud adoption.

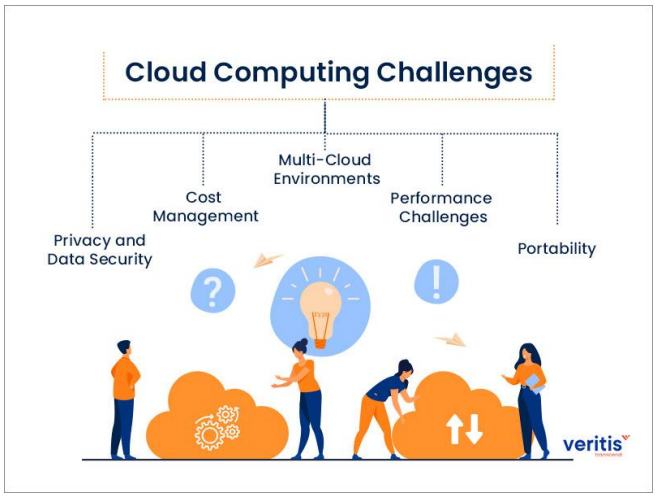

Fig. 2. Key Challenges in Human-Centered Cloud Security Adoption

This figure illustrates the primary challenges that hinder secure and trustworthy adoption of cloud computing. Human error remains the leading cause of breaches, while lack of transparency in cloud service providers fuels distrust. Existing awareness mechanisms fail to adapt to user behavior, and behavioral as well as cultural factors remain underexplored. Together, these challenges create barriers to building a reliable and human-centered security framework for cloud environments.

V. RESEARCH OBJECTIVE

The primary objective of this research is to address the dual challenges of human error and lack of trust that continue to hinder secure cloud adoption. While technical safeguards such as encryption and access controls have been extensively developed, they have proven insufficient when users commit mistakes or when organizations are unable to evaluate the reliability of cloud service providers. This study therefore seeks to propose a human-cantered security framework that integrates adaptive awareness, transparent trust mechanisms, and behavioural insights to create a more resilient and trustworthy cloud environment.

A key objective of this work is the design and development of an AI-driven adaptive security awareness system. Unlike traditional awareness programs that rely on static training modules, the proposed system will actively monitor user behaviour in real time. By detecting risky actions such as misconfigurations, repeated failed login attempts, or insecure data handling, the system will generate context-specific alerts and corrective prompts. In addition, adaptive micro-learning interventions will be delivered to users, ensuring that training is personalized and continuous rather than periodic and generic. The aim is to significantly minimize human errors, which remain the leading cause of cloud security breaches.Another important objective is the creation of a trust model and transparency dashboard that enables organizations and users to evaluate the reliability of cloud service providers. This involves quantifying trust through measurable indicators such as service availability, compliance with data protection standards, historical incident records, and clarity of privacy policies. By aggregating these metrics into a standardized, visual dashboard, the research aims to improve transparency and enhance user confidence in selecting and interacting with cloud providers.

The study further aims to investigate the behavioural and cultural influences that shape cloud security adoption across enterprises and government institutions. Security is not merely a technical issue but also a social process, influenced by organizational culture, employee attitudes, and regional perceptions of risk. Through surveys, interviews, and analysis of organizational practices, this research seeks to uncover the human and cultural factors that either strengthen or undermine cloud security policies.

Finally, the overarching objective is to integrate these dimensions into a unified human-cantered security framework. By combining adaptive awareness, trust visualization, and behavioural insights, the framework will provide a holistic approach to reducing vulnerabilities and strengthening trust in cloud adoption. This integrated model will serve as both a theoretical contribution to the academic community and a practical tool for organizations seeking to adopt cloud technologies in a secure and trustworthy manner.

VI. PROPOSED FRAMEWORK / METHODOLOGY

The proposed framework of this research is designed to provide a comprehensive, human-cantered approach to enhancing trust and reducing human error in cloud adoption. It integrates three core componentsan AI-driven adaptive awareness pipeline, a trust dashboard for cloud service provider evaluation, and behavioural analysis methodsinto a unified framework that is both technically robust and socially grounded. Unlike existing models that focus narrowly on technical safeguards, this framework emphasizes continuous feedback, transparency, and user engagement, thereby creating a dynamic and resilient security ecosystem.The first component of the framework is the AI-driven adaptive awareness pipeline. This pipeline leverages artificial intelligence and machine learning algorithms to detect anomalies in user activity within cloud systems. By monitoring authentication attempts, access logs, and configuration changes, the system identifies potential risks such as insecure file sharing, repeated failed logins, or unauthorized access patterns. Once an anomaly is detected, the system generates real-time, context-aware alerts and provides users with corrective recommendations. To strengthen long-term learning, the pipeline incorporates adaptive micro-learning modules—brief, personalized training interventions that educate users about the risks associated with their actions and guide them toward safer practices. Algorithms such as anomaly detection, clustering, and reinforcement learning will form the basis of this system, ensuring that the awareness mechanism continuously improves by learning from both user behaviour and emerging threats.

The second component is the trust model and transparency dashboard, which addresses the challenge of limited

visibility into cloud service provider (CSP) reliability. Trust will be quantified through measurable indicators, including service uptime, compliance certifications (e.g., GDPR, HIPAA, ISO standards), historical incident data, data handling policies, and customer satisfaction ratings. These indicators will be processed and aggregated into a standardized trust score. The dashboard will present these scores through a visual interface, allowing users and organizations to easily evaluate and compare different CSPs. By providing a transparent and user-friendly mechanism for trust evaluation, the dashboard aims to reduce uncertainty and build confidence in cloud adoption decisions.The third component is behavioural and cultural analysis, which explores the human and organizational factors influencing cloud security practices. Security is not only a technological challenge but also a behavioural one, shaped by employee attitudes, organizational policies, and cultural perceptions of risk. This study will employ surveys, structured interviews, and organizational case studies to gather insights into how different environments adopt cloud technologies and respond to security policies. The findings will be integrated into the adaptive awareness system, ensuring that interventions are not only technically effective but also culturally relevant and context-sensitive.

The final stage of the methodology is the integration and evaluation of the unified framework. The adaptive awareness pipeline, trust dashboard, and behavioural insights will be combined into a cohesive system. Prototype testing will be conducted within simulated cloud environments to validate the technical aspects of anomaly detection, adaptive alerts, and dashboard usability. In parallel, expert reviews and user studies will be carried out to evaluate the effectiveness of the behavioural and trust components. The evaluation will focus on three primary outcomes: reduction of human error, enhancement of user trust, and overall usability of the framework. The results will provide both empirical evidence and theoretical contributions toward establishing a new model for human-cantered cloud security.

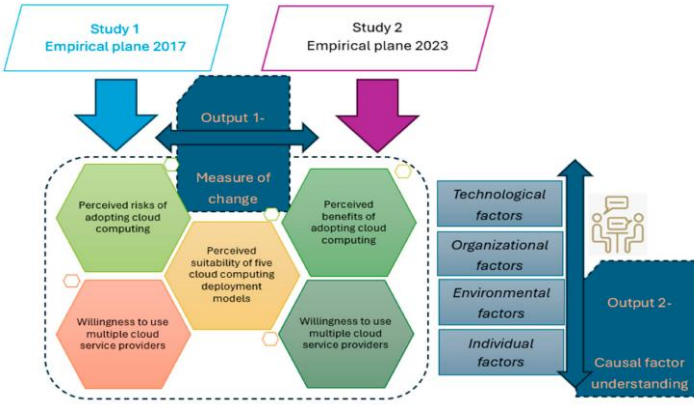

Fig 2. Proposed Human-Centered Security Framework for Cloud Adoption

VII. CONCLUSION

Cloud computing has firmly established itself as the backbone of modern digital infrastructure, enabling enterprises, governments, and individuals to leverage scalable, flexible, and cost-efficient technological resources. Despite its tremendous potential, however, the journey toward widespread adoption continues to face barriers rooted not only in technical vulnerabilities but also in human and organizational shortcomings. This study has sought to address these challenges by emphasizing that the greatest risks in cloud adoption often stem from human error, insufficient transparency, and underexplored behavioural and cultural factors. Accordingly, this research has proposed a human-cantered security framework that integrates adaptive awareness, trust visualization, and cultural analysis as a holistic solution.

The first major contribution of this work lies in highlighting the limitations of purely technical safeguards. While encryption, authentication, and intrusion detection mechanisms remain essential, they cannot mitigate risks that arise from poor user practices such as misconfigurations, weak passwords, or negligence in updating security patches. By proposing an AI-driven adaptive security awareness pipeline, this study advances the idea that user training must evolve into a real-time, dynamic process that continuously adapts to user behaviour. Such systems not only prevent errors at the moment they occur but also build long-term security-conscious habits through micro-learning interventions tailored to the individual. This innovation addresses one of the most persistent sources of cloud breaches—human error—while simultaneously fostering a more knowledgeable and vigilant user base.

The second contribution centres on the development of trust models and transparency dashboards. One of the greatest obstacles to cloud adoption is the lack of visibility into cloud service providers' reliability, compliance, and accountability. Organizations often hesitate to migrate sensitive workloads because they cannot measure trust objectively. This research proposes a standardized framework for quantifying trust through metrics such as uptime, breach history, compliance with data protection standards, and transparency in data handling. By presenting these metrics visually through dashboards, organizations can make more informed decisions, reduce uncertainty, and strengthen confidence in cloud ecosystems. In doing so, this study not only addresses technical trust deficits but also tackles the psychological and organizational dimensions of trust, which are critical for adoption in sensitive industries such as healthcare, finance, and government.

The third dimension of this research emphasizes the behavioural and cultural aspects of cloud adoption. Security is not simply a technological challenge; it is also a matter of human perception, organizational culture, and societal values. Employees may bypass security protocols for convenience, and cultural perceptions of risk may vary across regions and industries. By incorporating surveys, interviews, and organizational case studies, this study

proposes to integrate these behavioural insights into technical frameworks, ensuring that security strategies are not only technically sound but also contextually relevant. This approach acknowledges that effective cloud security depends as much on shaping behaviour and fostering security-conscious cultures as it does on deploying advanced tools.

By integrating these three dimensions—adaptive awareness, trust visualization, and cultural analysis—into a unified human-cantered security framework, this research contributes both theoretically and practically to the field of cloud computing. Theoretically, it broadens the scope of cloud security research by bridging technical, psychological, and organizational domains. Practically, it offers a framework that can be implemented in real-world settings, supporting enterprises and governments in reducing human error, improving trust in providers, and building sustainable security cultures. This holistic approach ensures that cloud adoption can progress with greater resilience, transparency, and accountability.

At the same time, this research acknowledges its limitations. The proposed framework, while conceptually robust, requires extensive empirical validation through prototype development, simulation testing, and real-world organizational trials. Additionally, the scope of behavioural and cultural studies may vary significantly across industries and geographies, suggesting that localized adaptations of the framework may be necessary. Furthermore, while AI-driven adaptive awareness systems promise to reduce human error, they also introduce challenges related to algorithmic transparency, privacy concerns, and user acceptance. Addressing these issues will be critical in ensuring that the framework achieves its intended outcomes without introducing new risks.

Looking ahead, this research opens several avenues for future exploration. First, the proposed framework could be expanded to multi-cloud and hybrid cloud environments, where trust and human error challenges are even more complex due to provider diversity and interoperability issues. Second, the framework can be applied to emerging domains such as Internet of Things (IoT) and edge computing, where human-cantered security concerns are magnified by device heterogeneity and large-scale user interactions. Third, future studies could explore how regulatory frameworks and international standards can be integrated with the proposed trust dashboard, creating globally recognized metrics for evaluating providers. Lastly, advancing explainable AI techniques within the adaptive awareness system could further improve user acceptance by ensuring transparency in how alerts and training interventions are generated.

In conclusion, this study underscores that the future of secure cloud adoption cannot rely solely on technical innovation but must also embrace the human element as both a challenge and an opportunity. By placing people at the centre of security design—through adaptive awareness, transparent trust mechanisms, and cultural integration—cloud ecosystems can evolve into safer, more transparent, and more trustworthy environments. The proposed human-cantered framework thus represents not only a response to current challenges but also a forward-looking vision for cloud security in an increasingly digital and interconnected world.

REFERENCES

- Abhishek, G., Sharma, V., & Bansal, R. (2022). Human factors in cloud security adoption: An organizational behaviour perspective. *Journal of Cloud Computing: Advances, Systems and Applications*, 11(4), 215–230. https://doi.org/10.1186/s13677-022-00321-7
- Ghosh, A., Chatterjee, S., & Tripathi, S. (2024). Trust and transparency in cloud ecosystems: Challenges and emerging solutions. *Future Generation Computer Systems*, 158, 451–465. https://doi.org/10.1016/j.future.2023.12.009
- Kaur, T., & Kamboj, S. (2023). Security as a cultural process: Organizational influences on cloud adoption. *International Journal of Information Security Science*, 12(2), 85–98.
- Misra, S., & Kumar, P. (2024). Trust deficit in cloud computing: Evaluating provider accountability through transparency dashboards. *IEEE Transactions on Cloud Computing*, 12(3), 711–724. https://doi.org/10.1109/TCC.2024.3356217
- Prabakar, S., Zhang, Y., & Hassan, M. (2023). Adaptive security awareness in cloud environments using AI-driven systems. *Journal of Information Security and Applications*, 75, 103458. https://doi.org/10.1016/j.jisa.2023.103458
- Raj, S. (2018). The failure of static training in cloud security: Toward adaptive awareness models. *Computers & Security*, 77, 295–307. https://doi.org/10.1016/j.cose.2018.03.010
- Singh, R. S., Verma, A., & Patel, D. (2024). Human error as a root cause of cloud breaches: An empirical analysis. *ACM Transactions on Privacy and Security*, 27(1), 1–22. https://doi.org/10.1145/3572215
- Sun, D., Zhang, G., & Xie, S. (2020). Security and privacy in cloud computing: A survey. *Journal of Network and Computer Applications*, 160, 102642. https://doi.org/10.1016/j.jnca.2020.102642
- Uzoma, C., & Okhuoya, M. (2022). Cultural dimensions of trust and risk perception in cloud adoption. *Information Systems Frontiers*, 24(5), 1267–1284. https://doi.org/10.1007/s10796-021-10123-8
- Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, 1(1), 7–18. https://doi.org/10.1007/s13174-010-0007-6
- Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. *2012 International Conference on Computer Science and Electronics Engineering*, 1, 647–651. IEEE.

- Alasmary, W., Alhaidari, F., & Mezher, T. (2021). Trust management frameworks for secure cloud adoption: A systematic review. *IEEE Access*, 9, 144783–144805. https://doi.org/10.1109/ACCESS.2021.3121257
- Islam, S., Mouratidis, H., & Kalloniatis, C. (2020). A framework for cloud trust: Bridging technical and organizational dimensions. *Computers & Security*, 92, 101744. https://doi.org/10.1016/j.cose.2020.101744
- Bhardwaj, R., Gupta, A., & Sharma, K. (2021). Artificial intelligence applications in cyber and cloud security. *Future Internet*, 13(9), 239. https://doi.org/10.3390/fi13090239
- Vohradsky, J. (2012). Cloud risk—10 principles and a framework for assessment. *ISACA Journal*, 4, 1–10.