# IEEE Review on “Potential Risk: Hosting Cloud Services Outside the Country” by A.S. Hovan George , Dr. A. Shaji George

## Introduction

The complexity of cloud computing and the benefits and problems that come with localizing cloud data are examined in this essay, with a focus on geopolitical conflicts like the current war between Russia and Ukraine. It starts out by stressing how ubiquitous cloud computing is in contemporary life and company processes, and how it helps to drive cost reductions and efficiency.

## Methodology

Highlighting how ubiquitous cloud computing is in today's world and how it helps businesses run more efficiently and affordably.We look into cloud data localization in depth and separate it from cloud data residency. Localization is the process of storing data in the location from where it comes. Clarified are the purposes and legal requirements of cloud data localization, highlighting the significance of this process for maintaining data privacy and compliance.

## Results and Discussion

To safeguard sensitive and confidential information created by their inhabitants, nations are enacting laws pertaining to data residency. Based on the rules of the nation, these requirements require data storage in the country of origin. Data generation, usage, storage, sharing, archiving, and destruction are all part of its life cycle. The usefulness of data residency in protecting data, however, is up for question if cloud centers or SaaS providers have access to the data in a separate jurisdiction.

## Conclusion

In the expanding digital economy, organizations need to pay close attention to data transfer regulations and cloud data localization. Although cloud computing has benefits, there are hazards and difficulties as well. When using cloud services, governments and other businesses are often concerned about data security. The Russian War illustrated the dangers of using the cloud. As cloud solutions become more prevalent, nations are susceptible to digital crises, and policymakers must be prepared to assess security risks when hosting cloud services outside their borders.