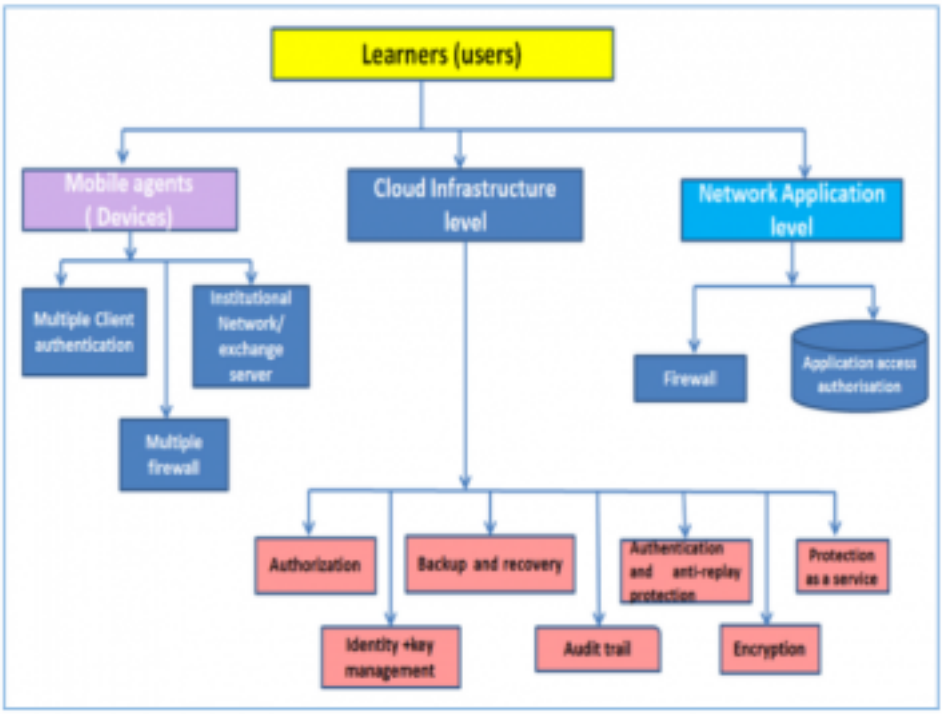
As we continue to progress toward more and more connectedness and sharing, we also need to consider how this exposes us to new challenges. Not so long ago, our biggest challenge with elearning was to make sure that we didn't lose our laptop. All of our personal information was on a single device and physical and digital security had significant overlap. If we protected our physical device, we had done a good job of protecting our digital information. As we get to share and store more and more of our information in the "cloud" as our devices get smaller and more portable - the overlap between physical and digital security and privacy diverges. As discussed by Adejo, there are numerous vulnerabilities to our data in the cloud, including: man in the middle attacks, denial of service attacks, SQL injection, unauthorized access, malware and many, many more (Adejo, 2018, p. 5).

To address many of these issues, Adejo provides a framework for data protection and security architecture (Adejo, 2018, p. 7). Such a framework is valuable for multiple audiences and purposes, including:

- Software vendors and developers
- Solution configuration, deployment and operation
- Teachers and institutions evaluating purchase/use
- Students that expect privacy and security

The following figure from Adejo provides an overview of the framework - highlighting perspectives (design, cloud and application) as well as key items to be considered within each perspective. As we consider other frameworks including ideas such as content, learning styles, beliefs, culture and other perspectives - we also need to keep in mind security and privacy. Failure to keep data secure and private will leave our students vulnerable and negate other investments and jeopardize the success of mobile learning.



Reference

Adejo, O. W. (2018). E-Learning to m-Learning: Framework for Data Protection and Security in Cloud Infrastructure.