PART B RESEARCH PAPER REVIEW

TOPIC: IDENTITY AND ACCESS MANAGEMENT IN CLOUD ENVIRONMENT: MECHANISM AND CHALLENGES

At the beginning of the paper, the author explains about different kinds of cloud architectures and along with that the author also takes us through the possible vulnerability and the security concerns which cloud have. The author covers many types of attacks, discovered and undiscovered attacks, and data leaks with possible breaches which could result in major capital loss or be a vital privacy issue. The author not only describes the vulnerability but also gives us some points and precautions which we could take in the context and be on the safer side of all this like author suggested to use IAM(Identity and Access Management) tools which allows authorization and authentication of the user and limits the access for each user according to their eligibility.

The paper majorly focuses on the security of the cloud with more weight on the Authentication factor. Expensive and secure systems use biometrics like fingerprint, retina scan, or facial recognition to make their system more robust and stay away from the potential illegal access of the system. Along with that, we have multi-factor authentication (Google), SSH code for secure login, pin, and password with OTP and Physical Chips to access the systems.

Talking about the incidents where mismanaged access bankrupted a whole organization. There was a case study where in an organization all the workers had the same access level in the systems and this resulted in the leaking of data from the organization and indeed bankruptcy of that organization. This could be solved with multi Access systems. Taking another example of myself where I got a mail which seemed suspicious but I neglected that mail and added the details including password and all my mailing accounts were frozen, I didn’t have any financial information in that account so I was saved still this happened. Now having a chip authentication in which users can only login into an account with a password and chip at the same time could save me.

In the majority of a scenario like this IAM could potentially save the life with the methods mentions on the top. Today we are updating fast and cooping up with the technology innovation. Nowadays online crimes like data leaks could potentially put us into mental strain and to commit this crime the person doesn’t need to physically come near to you, they could commit the crime thousands of miles away from us. In today's day and age, there are many ways hackers and online criminals access data that should not be accessed by them.

By Intercepting the communication channel the most famous and oldest attack is “Man in the Middle”, just like 70’s movies where the conversation between tho military personals was tapped by the other group. Another is the Brute Force attack which works with some personal information of the user and then generates a large set of data for passwords and then injects everyone and forcefully breaks the lock. Nowadays all websites are using cookies to save the data and criminals are using these cookies to get the data that could be used in data set generation. And if nothing works then with an immense number of face requests hackers bottleneck the servers.

Recommendations made like IAM, multifactor authentication along with biometrics and physical chips to log in could solve the issue. The paper summarizes to prove that the cloud indeed is changing the perception or vision which we had to the world and the future is the cloud but it comes with some serious drawbacks like security and privacy issues. Using these recommendations we could make could system more robust and solid against attacks.

Dhruv Doshi (B00883311)