IAM (Integrity & Access Management) Case Study Report:

Company:
Incepted in mid-1800s, the organisation is India’s largest media conglomerate that publishes the world’s largest circulating English daily newspaper and the world’s second largest circulating English Business daily newspaper.
With over 11,000 employees spread across the country, the organisation is widely considered as India's most diversified media company with brands across Publishing, TV, Internet, Radio and Outdoor domains.

Problem:
With a majority of its workforce compelled to work from home due to the COVID-19 pandemic, the organisation wanted to secure the remote access of its 2500 VPN users by implementing an advanced Identity and Access Management (IAM) solution with a three-layer authentication mechanism for safely accessing its corporate resources and critical business applications.
To facilitate anytime, anywhere secure access, the organisation was keen to enforce foolproof network security with strong VPN authentication and user access controls at a granular level for all corporate resources.
Taking into considering that a vast number of its employees used their personal devices to connect to their VPN network, the organisation was keen to implement an IAM solution that was not only device and OS agnostic, but also include multiple authentication options for quick and seamless access across mobile phones, desktops, laptops and tablets.

The Solution:
Since the Covid situation was new and the company has to develop a solution to the situation so that employees could work from home.The employees should require a stable and secure VPN solution for accessing the company's data from their homes.The company also had to prevent any un-authorized access to data,and security was a must in this situation.
Thales provied them a solution for their problems by developing an advance IAM solution for their problem
they used company's database for help for building an Role based access control and the user based on their ID's have different roles assigned and authorization given according to the company's requirement there was Zero trust in system.They developed multifactored authorization in the VPN solution and used their own cloud for managing the stability and security they implemented federated identity management so that the user had to only login once through their device in cloud and able to access the company's data and service the data security is managed by both company and cloud has only data related to access control(login id's and the access given to that id), the user could also login with their pin or biometrics after they store the login info in their primary device with single sign-on mechanism with any device mobile,laptop etc..They can access the data which is ment to be accessed by thier id with the different services provided by Organization.So after the implementaion of this solution the problem was solved. The employees had stable and secure remote access,the company has centralised access control and better user experience with thales app(SafeNet MobilePASS+).

Understandings:
Single Sign-on mechanism:
With SafeNet Trusted Access, the organisation was able to secure the remote access of its VPN users while eliminating password hassles through its Single Sign-on mechanism.

Centralised Access Control:
The organisation’s IT Team was now able to centrally manage and view access events for multiple business applications while allowing users to log in to cloud and web apps without the need to reauthenticate themselves each time

Multifactored authentication done while the user is logging in like otp and biomerics for seamless access in mobile devices.
There was a role base access control in the system so only the user who is required to access different files they are allowed if they had access given to them (Zero trust) .Segregation of duties were done and different users were allowed to peform different task based on their identity.Federated Identity management used so that user after verification done in cloud easily able to access the organizations cloud data without re-authorization.there was accuntibility of every task peformed by a specific user that is loggged in the system.

When anyone is trying to login in the website through mobile or laptop through their home, their authentication is done in cloud(Thales cloud) with their id's and passwords and otp's sent to their mail and mobile number for security puposes using multifactored authentication.The cloud was providing a stable VPN platform for accessing the organization data in their home securely.After the authentication of user is done he will get connected to organization cloud,every activity including which file sent or recieved,the login and logout time of employee(user) is logged(accounted) in the organization so accountablity is maintained throughout.Since organization has Segregated duties the employee has only access to those information or data which is provided by organization.They won't be able to access any other data without permission of organization.If the authorization is not been provided to the employee this action is also accounted in organizations cloud.

AAA (Authentication Authorization and Accountibility) concept was used to solve the problem.

By Priyanshu Koche