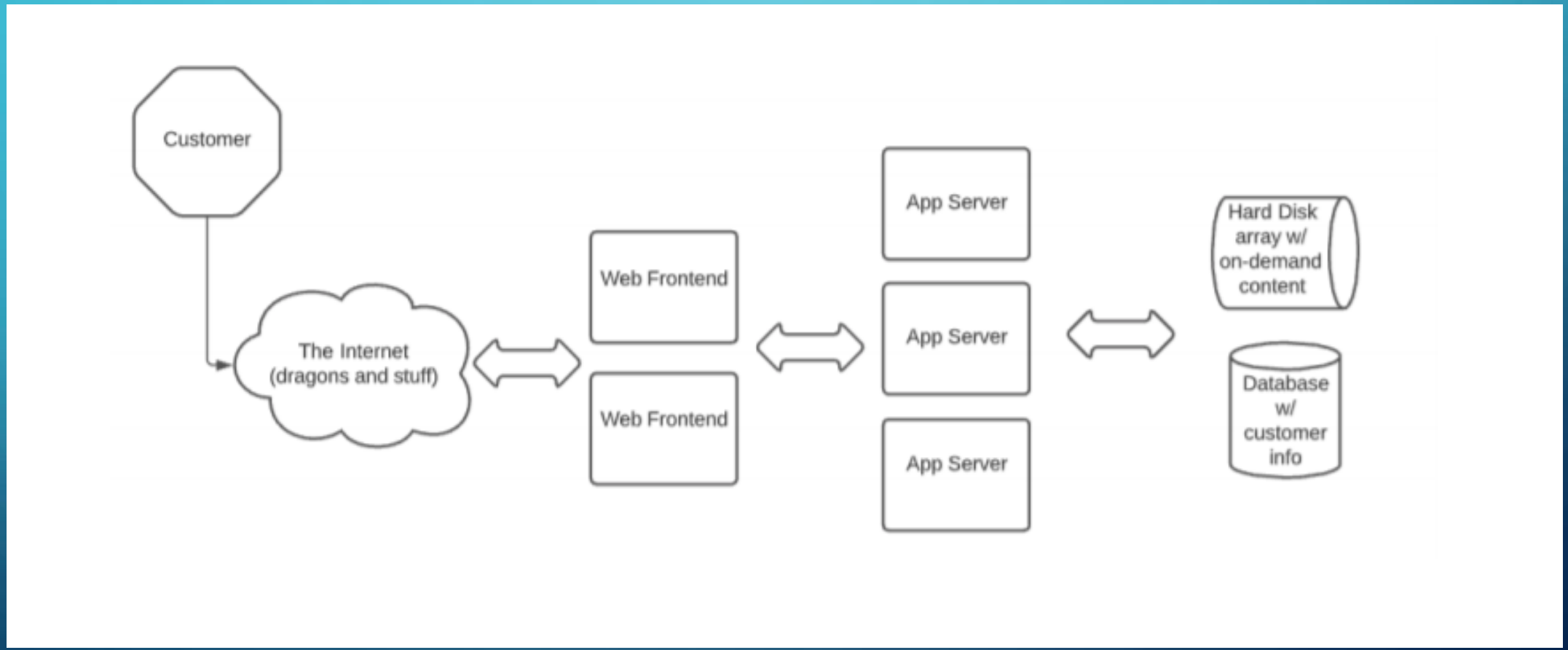
ENPM809J MIDTERM

CLOUD MIGRATION PROPOSAL FOR COBRA KAI

AKSHAY MANOJ UID:116921169

CURRENT ARCHITECTURE



ISSUES WITH CURRENT ARCHITECTURE

- Limited app servers:
  - Vulnerable to DDoS
  - Bad load balancing
  - Performance bottle neck
- Storing data in one place:
  - Vulnerable to data theft
  - Vulnerable to high down times if database servers go down
  - Need better maintenance
  - Bottleneck for parallelly accessing data and records

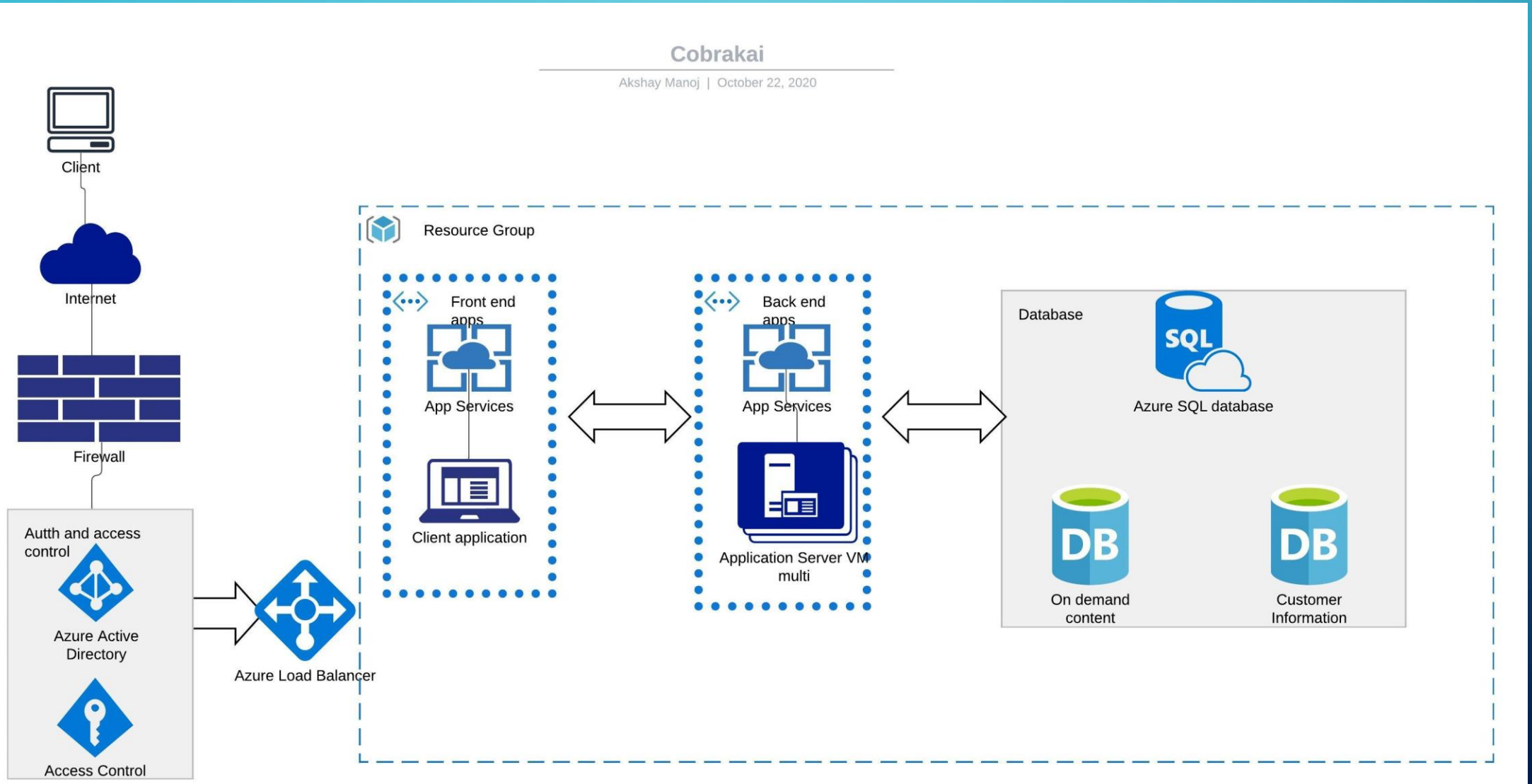
CHANGES NEEDED IN WORKING MODEL

- Need a patching strategy :
  - To update software and fix bugs in an ordered and controlled manner
- Need a Backup strategy:
  - Important client information and proprietary video content would need to be periodically backed up.
- Need to add access permission hierarchy:
  - Add Roles and grant access privileges according to the roles
- Need to have PCI compliance level 4:
  - Payment forms need to be PCI compliant to avoid any legal issues with the corresponding banks and credit card companies

WHY MOVE TO CLOUD?

- Easy to scale up so that the website can handle increasing traffic:
  - Configure a load balancer.
- Reduces infrastructure overhead
- Costs less to expand and maintain storage
- Server upgrades and backups can be easily managed:
  - Data is more resilient to thefts and loss
  - Code changes are in a controlled environment
- Manage access control:
  - We can add roles and Identity access management into the cloud services
- Security:
  - Buy and configure cloud firewalls against network level threats
  - Configure data stores for better data security
  - Proper user and role configuration to avoid unauthorized actions.

PROPOSED ARCHITECTURE



NEW COMPONENTS

- Azure Firewall to block unwanted traffic
- Access and Authentication management using Azure AD and Access control
- Azure Load balancer
- App services and Client app instances
- App services and App server VM's
- Azure Database instances

HOW DOES THIS HELP?

- Azure firewall : Will block incoming traffic from unwanted ip addresses or domains
- Azure AD : Provide more security , by restricting access and assigning roles to users.(Provides Identity access management)
- Azure Load balancer, VM, App services : Can be configured to scale up or scale down the system as per the load and the need
- Azure database : Provides a separate instance of the database so that the data access bottle neck is resolved to some extent

MIGRATION STRATEGY

- Assess and identify services that can be moved to the cloud.
- Set up KPIs for the identified services.
- Establish baseline for performance.
- Setup configuration for patching and backup
- Duplicate infrastructure components onto cloud platform.
- Transfer services slowly onto cloud platform while testing for performance gains.
- Duplicate data from databases into the cloud databases.
- Retrain developers and testers to start using the cloud version of the app.

PATCHING STRATEGY

- Azure app services have integration with git so patching and versioning of code is easier
- Release code to production in versions
- Separate development ,testing and production environments. (Can just be single VM each for dev and test environments)
- Retrain developers to write secure code, retrain testers to test for security flaws.
- Add levels of approvals before code reaches production.
  - Code changes and bug fixes must be approved by higher level management
  - Bugs must be fixed depending on impact and severity of the issue.

BACKUP STRATEGY

- Azure SQL database comes with an Azure backup service
- Service can be configured to -
  - Create store points in the data base on the cloud platform
  - Periodically backup data from the database to an Azure RDS for up to 30 days.
- Once data from the physical server is migrated to the cloud database we can setup the backup service.
- Information like Customer PPI should be backed up in case of a data theft or a data loss incident.

ROLE BASED ACCESS PRIVILEGES

- Setup roles in Azure AD:
  - Administrator, developer, customer, management etc.
- Provide access privileges to roles:
  - Customer should only be able to use the application
  - Developer should be able to use application, modify & view code and view configuration
  - Administrator should be able to View and modify configuration, view code and use application.
  - Management should be able to pull reports and usage information for the cloud services apart from being able to view code, view configuration and view the application.
- Control the flow of information across Users by configuring the roles properly in Azure AD.

COST TO COMPANY WITH CURRENT MODEL

- Upfront cost of running the website: $4000
- Monthly upkeep : $2800
- Loss suffered in last DDOS attack : $1500
- Projected Loss due to customer data theft : $1000 per customer

POST MIGRATION COST TO COMPANY(MONTHLY)

- Azure AD ~$400.00
- Azure database with monthly backups ~$800
- Upto 10 Windows server VM ~$400
- Azure app service module ~$55
- Azure app gateway ~$0
- Azure firewall ~$900
- These are rough estimates because we can choose to pay as you go which will change cost based on usage of services.

REFERENCES

- Pricing calculator : https://azure.microsoft.com/en-us/pricing/calculator
- https://www.skyhighnetworks.com/cloud-security-blog/pci-compliance-in-the-cloud-a-beginners-guide-with-29-resources-for-it-professionals-new-to-pci/
- https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices
- https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles
- https://cloudacademy.com/blog/cloud-migration-benefits-risks/
- https://blog.newrelic.com/engineering/cloud-migration-checklist/
- https://app.lucidchart.com/