CLOUD SECURITY

NAME A.GEETHA

DEPARTMENT: COMPUTER SCIENCE AND ENGINEERING

COLLEGE NAME :THE KAVERY ENGINEERNG COLLEGE

OUTLINE

- PROBLEM STATEMENT
- PROPOSED SYSTEM /SOLUTION
- SYSTEM DEVELOPMENT APPROACH
- ALGORITHM AND DEPLOYMENT
- RESULT
- CONCLUSION
- FUTURE SCOPE
- REFERENCES

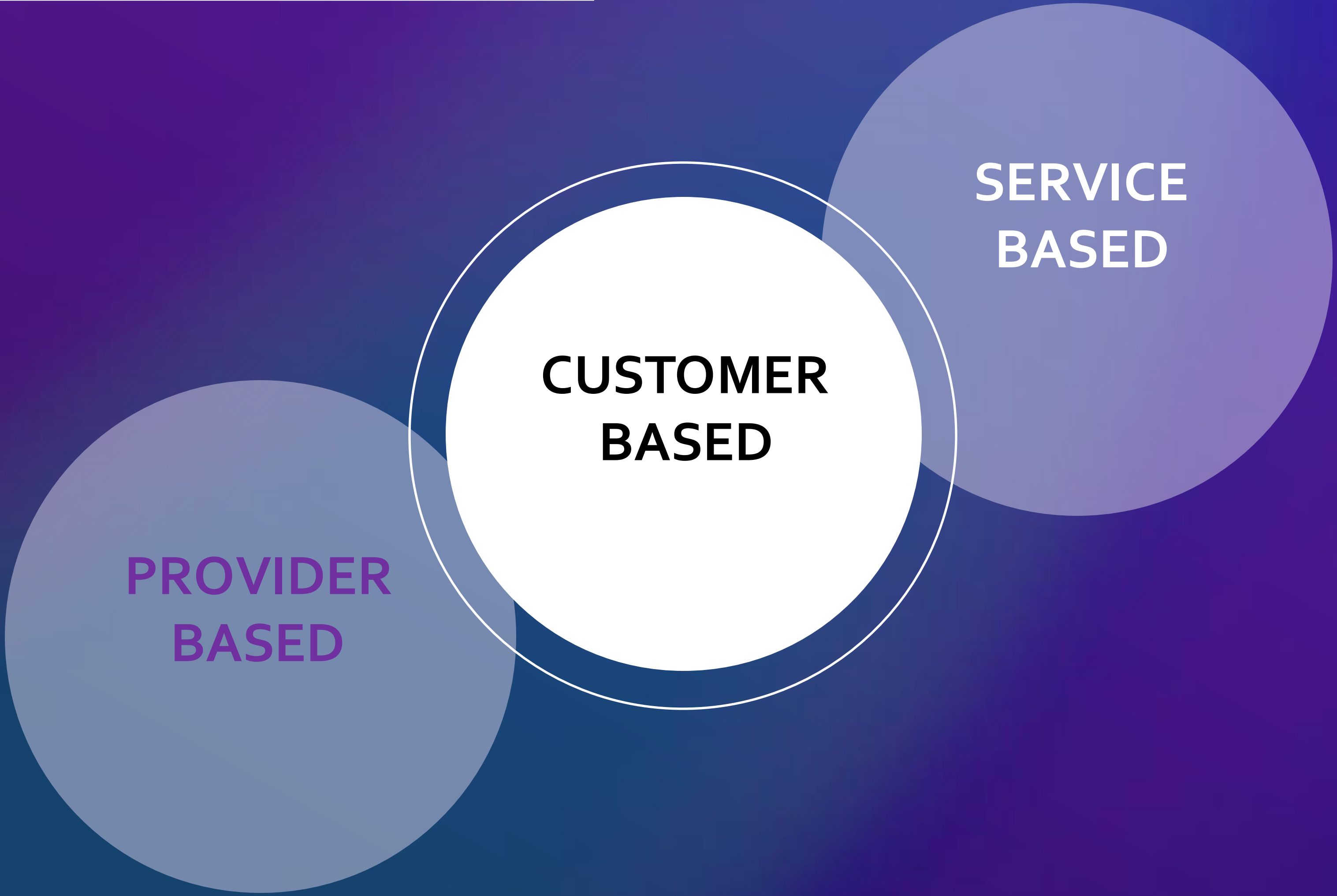
PROBLEM STATEMENT

Problem Statement

The data is at risk of being accessed by intruders whether they may access the network or the cloud. There is an impending risk of sensitive data being accessed by unauthorized personnel.

PROPOSED SYSTEM /SOLUTION

Ensuring the confidentiality, integrity, and availability of sensitive data in cloud environments relies heavily on the robust management of cryptographic keys.



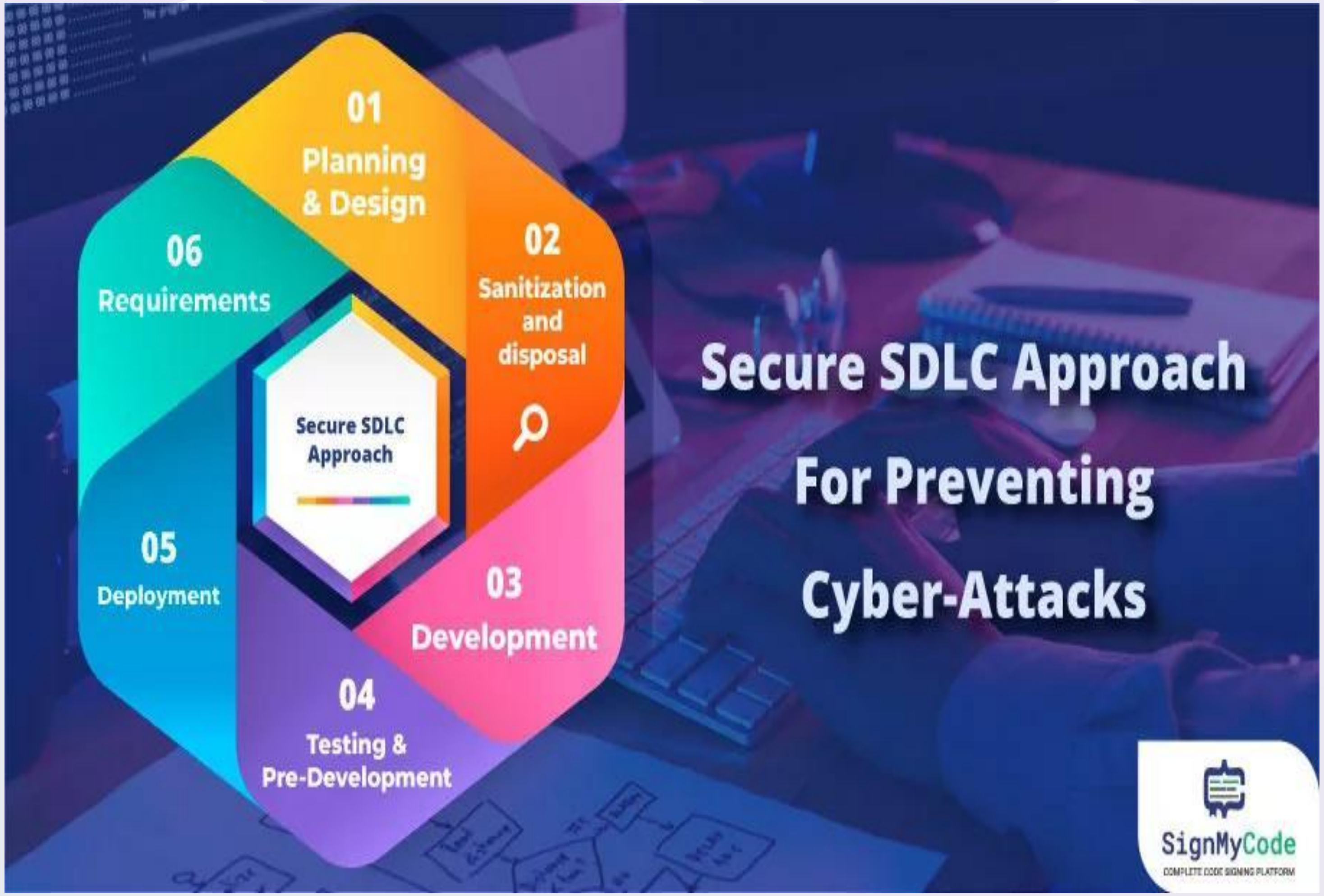
SERVICE BASED

CUSTOMER BASED

PROVIDER BASED

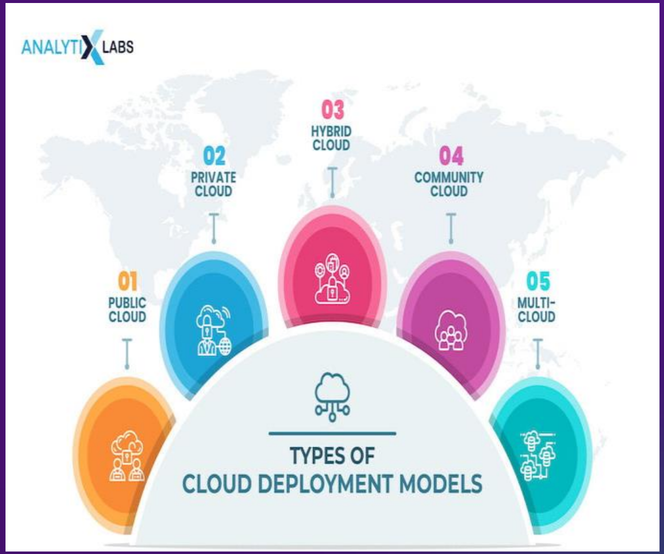
SYSTEM DEVELOPMENT APPROACH

Systems development is the process of defining, designing, testing, and implementing a new software application or program. It could include the internal development of customized systems, the creation of database systems, or the acquisition of third party developed software.



01
Planning & Design
02
Sanitization and disposal
03
Development
04
Testing & Pre-Development
05
Deployment
06
Requirements
Secure SDLC Approach
Secure SDLC Approach For Preventing Cyber-Attacks
SignMyCode
COMPLETE CODE SIGNING PLATFORM

ALGORITHM AND DEPLOYMENT



- Cloud computing appear to be a very popular and interesting computing technology. Every third person is using cloud computing directly or indirectly for example e-mail, most commonly used application of cloud computing, you can access your mail anywhere anytime. Your e-mail account is not visible on your personal computer but you have to access that with the help of internet. Like e-mail cloud computing provide many other services such as storage of any kind of data, access to different applications, resources etc.
- So users can easily access and store data with low cost and without worrying about how these services are provided to user. Due to this flexibility everyone is transferring data to cloud. To store data on cloud user has to send their data to the third party who will manage and store data. So it is very important for the company to secure that data. Data is said to be secured if confidentiality, availability, integrity is present.
- To store data on cloud user has to send their data to the third party who will manage and store data. So it is very important for the company to secure that data. Data is said to be secured if confidentiality, availability, integrity is present. To secure data we have different algorithms. In this paper we will discuss the different cryptography of algorithms

RESULT

- Cloud security is the protection of data stored online via cloud computing platforms fron theft, leakage, and deletion. Methods of providing cloud security include firewalls, penetration testing, obfuscation, tokenization, virtual private networks (VPN), and avoiding public internet connections

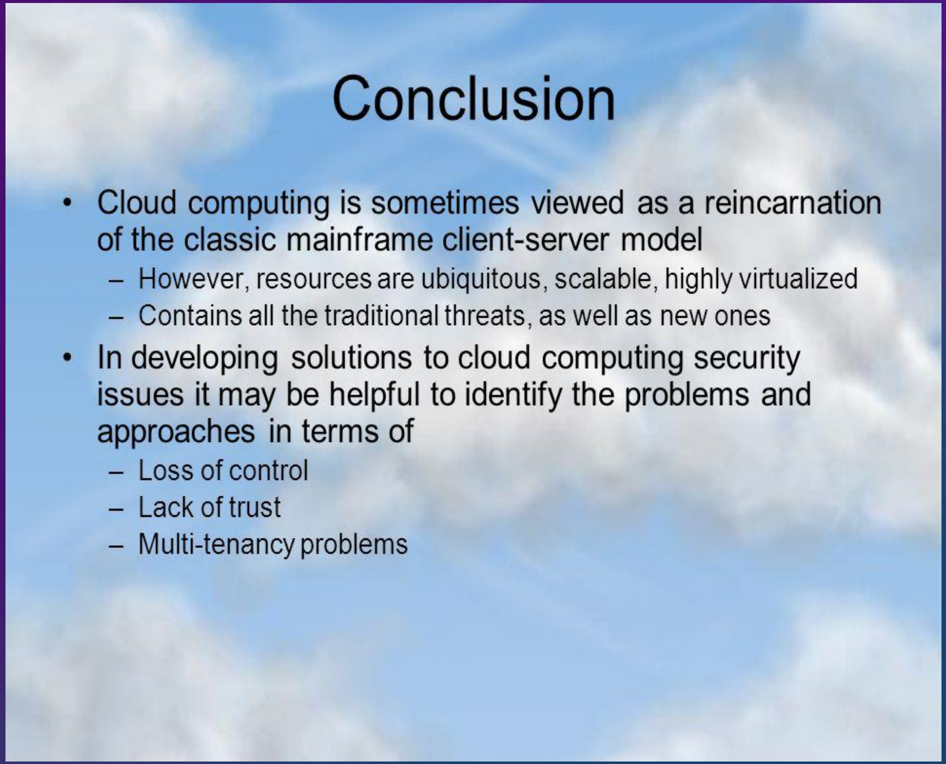
- Ex: Dropbox, Gmail, Facebook.

- Ex: Maropost for Marketing, Hubspot, Adobe Marketing Cloud.

- Ex: SlideRocket, Ratatype, Amazon Web Services.

- Ex: ClearDATA, Dell's Secure Healthcare Cloud, IBM Cloud.

CONCLUSION



Conclusion

- Cloud computing is sometimes viewed as a reincarnation of the classic mainframe client-server model
  - However, resources are ubiquitous, scalable, highly virtualized
  - Contains all the traditional threats, as well as new ones
- In developing solutions to cloud computing security issues it may be helpful to identify the problems and approaches in terms of
  - Loss of control
  - Lack of trust
  - Multi-tenancy problems

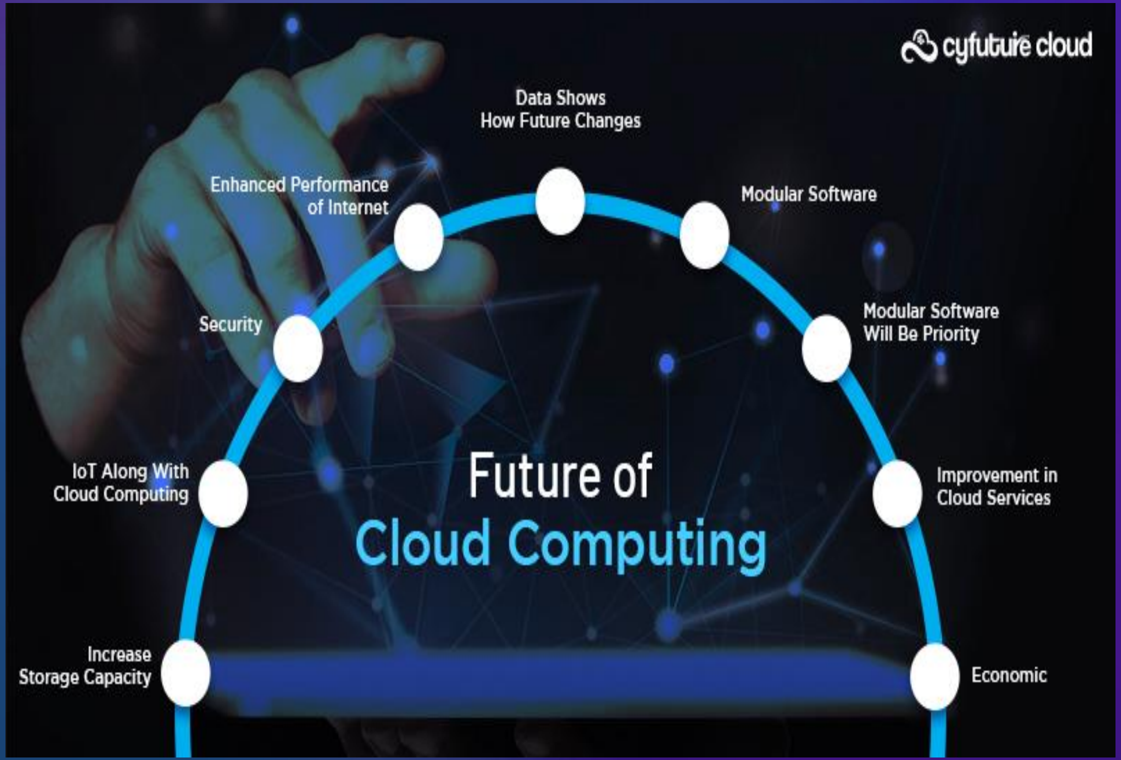
1. Cloud computing will affect large part of computer industry including Software companies, Internet service providers. Cloud computing makes it very easy for companies to provide their products to end-user without worrying about hardware configurations and other requirements of servers.

2. The cloud computing and virtualization are distinguished by the fact that all of the control plane activities that center around creation, management, and maintenance of the virtual environment.

FUTURE SCOPE

- The future of cloud security will see advancements in trends that are focused on improving digital fortifications. AI-driven threat detection zero-trust platforms, and other automated security measures have immense potential in helping mitigate emerging threats.

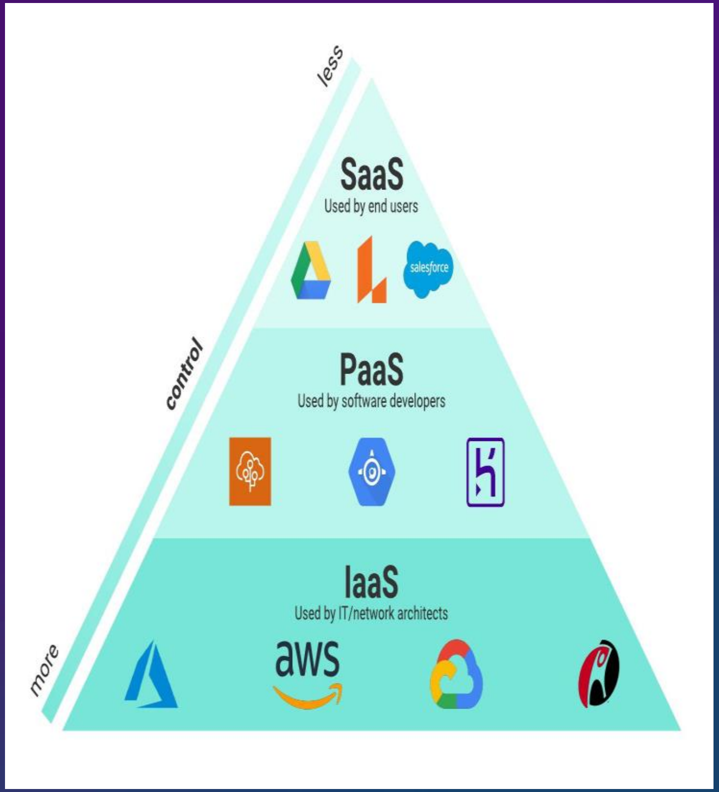
- The future scope of cloud security is quite promising, as more and more businesses and individuals are moving their data and applications to the cloud. This trend is likely to continue, creating a growing need for robust cloud security measures. As technology advances, we can expect to see the development of more sophisticated security tools and techniques to protect cloud-based systems and data. This may include advancements in encryption, identity and access management, threat detection, and compliance monitoring.


cyfuture cloud
Data Shows How Future Changes
Enhanced Performance of Internet
Modular Software
Security
Modular Software Will Be Priority
IoT Along With Cloud Computing
Future of Cloud Computing
Improvement in Cloud Services
Increase Storage Capacity
Economic

REFERENCES

- The Cloud Security Alliance (CSA) reference model defines these responsibilities. It state that IaaS is the most basic level of service, followed by PaaS and then SaaS. Each of ther inherits the security intricacies of the predecessor, which also means that any concerns a propagated forward.

- The cloud computing reference model is an abstract model that divides a cloud computi environment into abstraction layers and cross-layer functions to characterize and standardize its functions. This reference model divides cloud computing activities and functions into three cross-layer functions and five logical layers.



thank you