This paper gives an overview of Amazon Web Services (AWS) cloud platform. It highlights the services that enhance data security in the public cloud and concludes by describing some scenarios where cloud computing may not be the best choice for a business.

Amazon Web Services (AWS) is a secure cloud platform that offers several featured services including computing power, network, database storage and many more functionalities to help industries scale and grow. On the AWS cloud platform, customers can run their software applications on servers within Amazon infrastructure and only pay for the services they use for as long as they use them. AWS has a systemic cloud structure with services organised into different categories, each category containing one or more services. Therefore, AWS customers can select services from these different categories to develop solutions as their business needs require.

AWS is a highly secure cloud platform as it offers tools and services that help to secure all stored data in the cloud. Applications and infrastructure security are critically essential elements in the AWS cloud. One of the most critical services for improving AWS cloud security is the Identity and Access Management (IAM) service, which allows the customers to manage which users have access to resources as well as assigning specific tasks for each user. Since the account root user can perform any task on the AWS account, IAM service recommends AWS customers to protect their main account by locking down the root user and not using it for daily tasks to keep it safe for control over the cloud. The IAM service gives customers the ability to replace the practical functionality of the account root user by creating IAM users and groups for their daily administration tasks. Consequently, authentication is a necessary factor for controlling access on AWS cloud. When users try to access a remote application to AWS resources, they will need to verify themselves by providing their username and password. Further, the AWS IAM service enables customers to set a password policy forcing their users to create strong passwords.

Most importantly, AWS follows the principle of least privilege, which gives users and groups only the minimum permissions needed for their tasks. This, in turn, ensures that AWS customers can efficiently manage resource access for several users with different access needs through IAM groups. Another security feature is Multi-factor authentication (MFA) which extends the authentication process by asking the user to provide a temporary token sent through a pre-set device when logging in to their accounts. Not only that, but AWS also guarantees to secure data traffic on the cloud by encrypting remote login sessions in the Secure Shell (SSH) protocol. A user will be able to create access keys through the AWS Management Console and store them in their machines. Subsequently, they can initiate a secure connection to access their resources such as Amazon Elastic Compute Cloud (EC2).

Encryption applies to any data in AWS services. Once the data is encrypted, the resources will be unreadable without the decryption key. AWS offers a Credential Report as an additional security feature that contains information about the state of the account security such as when users last logged in and whether they have MFA enabled and many metrics that assist AWS customers in monitoring their account security effectively. Security is a shared responsibility between AWS and its customers. The AWS shared responsibility model is designed to support the security of Amazon's cloud infrastructure. For example, AWS provides security groups as one of the tools for securing customer's EC2 instances. By creating a security group in a Virtual Private Cloud (VPC), it checks the incoming and outgoing traffic to the instances in the network. As part of the AWS shared responsibility model, customers are responsible for configuration to meet their security needs.