Title

A
Project Report
submitted in partial fulfillment of the
requirements for the award of the degree of

BACHELOR OF TECHNOLOGY

In

COMPUTER SCIENCE & ENGINEERING
with

Specialization in CCVT

by

SAP ID	Roll No.	Name
500083069	R2142201163	Sourabh Kumar Singh

under the guidance of
Mr. Saurabh Shanu
Assistant Professor - Senior Scale,
Systemics Cluster
School of Computer Science

Systemics Cluster
School of Computer Science
University of Petroleum & Energy Studies
Bidholi, Via Prem Nagar, Dehradun, UK
April – 2023

CANDIDATE’S DECLARATION

We hereby certify that the project work entitled **“Title”** in partial fulfilment of the requirements for the award of the Degree of BACHELOR OF TECHNOLOGY in COMPUTER SCIENCE AND ENGINEERING with specialization in CCVT, and submitted to the Systemics Cluster at School of Computer Science, University of Petroleum & Energy Studies, Dehradun, is an authentic record of my work carried out during the period from **January**, **2023** to **April, 2023** under the supervision of **Mr. Saurabh Shanu,** Assistant Professor - Senior Scale, Systemics Cluster, School of Computer Science.

The matter presented in this project has not been submitted by me for the award of any other degree of this or any other University.

Name:	**Sourabh Kumar Singh**
SAP ID:	**500083069**

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Date: 23 April 2023

Mr. Saurabh Shanu
(Subject Faculty)

School of Computer Science

University of Petroleum & Energy Studies, Dehradun

Project Based | I | **Learning:**

PROJECT TITLE: Security Management System On AWS

ABSTRACT (250-300 words)

Cloud computing has grown in popularity as a popular option for businesses looking for effective and affordable solutions to manage their IT infrastructure. However, as organisations rely more on cloud-based services, security concerns have increased as well. As a result, they are continuously looking for solutions to safeguard their sensitive data and avoid security breaches.

An extensive and scalable method to address security risks in the cloud is offered by the security management system on Amazon Web Services (AWS). AWS provides a range of security services, including data encryption, network security, identity and access management, and threat detection, to help businesses create secure and legal cloud architectures.

Based on a shared responsibility paradigm, AWS is in charge of protecting the underlying infrastructure, while customers are in charge of protecting their applications and data. AWS offers a collection of best practises and tools that customers may utilise to create and maintain their security posture in order to assist them satisfy their security requirements.

Customers can monitor their infrastructure for security threats, compliance infringements, and other potential hazards using services like AWS Security Hub, AWS Config, and AWS GuardDuty, which are all part of the AWS security management system. Additionally, AWS provides a variety of compliance certifications and attestations, such as ISO, SOC, HIPAA, and PCI, which can assist clients in meeting legal obligations.

As a result, managing security threats in the cloud is made simple and scalable by the AWS security management system. Organisations may create secure and compliant cloud infrastructures and shield their sensitive data from security breaches by utilising AWS security offerings and best practises.

Keywords: Shared Responsibility Model , Identity & Access Mnagement, Compliance, Threat Detection, Encryption

Contents

INTRODUCTION

Security Management System

Security management is becoming more and more crucial as more businesses migrate their workloads to the cloud. Organisations may secure their cloud infrastructure and safeguard their data with the help of a wide range of security services and capabilities provided by Amazon Web Services (AWS).

Identity and Access Management (IAM), which enables organisations to control user access and rights to AWS resources, is one of the main elements of AWS security. IAM enables businesses to manage user accounts, restrict access to resources, and keep an eye on activities through audit trails.

Amazon Inspector is another another crucial AWS security service that aids in locating potential security flaws and vulnerabilities in AWS resources. It conducts automatic security assessments and produces a thorough report with remedial suggestions.

AWS also offers a variety of logging and monitoring services, like AWS CloudTrail and Amazon CloudWatch, to assist businesses in keeping track of activity and spotting any security risks. All API requests to AWS resources are recorded by AWS CloudTrail, and system metrics and logs can be watched using Amazon CloudWatch.

AWS provides a variety of encryption services, such as AWS Key Management Service (KMS) and AWS Certificate Manager (ACM), to further improve security. Organisations may produce and manage cryptographic keys for data encryption using AWS KMS, and they can provision, maintain, and deploy SSL/TLS certificates easily with AWS ACM.

AWS also provides a number of network security services, such as AWS WAF, AWS Direct Connect, and Amazon Virtual Private Cloud (VPC). While AWS Direct Connect offers a dedicated network link between AWS and an organization's data centre, Amazon VPC enables businesses to build a private, segregated network within AWS. online application firewalls like AWS WAF can shield online applications from common web-based threats.

AWS also provides a variety of compliance and certification programmes, like as HIPAA, SOC 2, and PCI DSS, to assist businesses in adhering to legal obligations and ensuring the security of their data.

Last but not least, AWS provides a selection of managed security services including AWS GuardDuty, AWS Security Hub, and AWS Shield that assist businesses in identifying and addressing security risks in real-time. Potential security vulnerabilities are identified by AWS GuardDuty using machine learning and threat intelligence, while AWS Security Hub offers a centralised view of security alerts and compliance status across an organization's AWS accounts. Protection from DDoS assaults and other security risks is offered by AWS Shield.

Blogging Website for Security Management System

There are several ways to monetize blogs, including through advertising, sponsored material, or the sale of tangible or digital goods associated with the blog's subject. A common approach for people to position themselves as authorities in their subject and for businesses to advertise their goods or services is through blogging.

In general, blogging websites give people and organisations a forum to express their views, ideas, and experiences with a large audience, and they have developed into a significant component of the internet environment.

Blogging websites have been important for several reasons now-a-days, some of which are as follows-

Content Creation: Individuals and organisations can develop and share top-notch material on blogging websites with a large audience. By educating readers or customers and establishing thought leadership, this content can increase brand recognition.

Search Engine Optimization (SEO): By offering search engines with up-to-date and pertinent information, blogging websites can enhance search engine optimisation (SEO), hence boosting website traffic and search engine rankings.

Audience Engagement: Blogging websites can improve search engine optimisation (SEO), hence increasing website traffic and search engine ranks, by providing search engines with current and relevant content.

Lead Generation: Additionally, blogs can be used to generate leads and increase conversions. People and organisations can develop trust and credibility by giving readers useful content and information, which may result in more sales or business prospects.

Cost-Effective: Small businesses and people of all sizes can use blogging as a cost-effective marketing technique. Blogging is relatively cheap and has a high return on investment when compared to conventional marketing strategies like print or television advertising.

In conclusion, blogs are crucial because they give people and businesses a platform to produce and distribute high-quality material, enhance SEO, interact with their audience, and generate leads in an affordable way.

Methods used for developing a Blogging Website

For developing my blogging website I have used Javascript as it is one of best platform for web development and is easier to use.

There are several methods for developing a blog website. Here are some general steps you can follow:

Choose a blogging platform: There are numerous blogging platforms accessible, including

Blogger, Squarespace, Wix, and WordPress. We can decide on the option based on our needs and financial situation.

Choose a domain name and hosting provider: Here, we have to pick a domain name for our blog and a hosting company for our website.

Install the blogging platform: After deciding on a blogging platform, we must install it on the server of our hosting company.

Choose a theme: Choose a theme that suits the topic of your blog and customize it as per our needs.

Customization of our blog: We need to customize our blog by adding pages, menus, and widgets.

Create content: Start creating content for our blog and we need to make sure that our content is engaging and informative.

Promotion of our blog: We need to promote our blog through social media, email marketing, and other channels to attract readers.

Maintainance of our blog: We need to regularly update our blog with fresh content and maintain it by keeping it secure and up-to-date.

So, for the development of my blogging website I have used JavaScript for my website development as it is one of the most popular application for web development and provide several benefits some of which are as follows -

- It can be used both in the front-end and back-end of web development
- Can run on all devices
- It does not need an environment setup
- Transformed web browsers into application platforms
- Wide range of frameworks and libraries to help build complex application

JavaScript (JS), a scripting language, can be used to create websites or web pages. It enables programmers to develop dynamic and interactive web pages that interact with visitors and perform complex operations. Additionally, it enables users to add content to a document without having to reload the entire page.

Therefore, in my blogging, we only need to log in using the used ID or Email to write and post blogs on various topics. In addition, we can access other blogs and read and give suggestions to them about what changes are needed to their blogs and what additional content they can add.

Users can write entries on a wide range of subjects, including news, opinions, personal experiences, and more.

After logging in to my blogging website, the user typically has several options for what they can do:

Create a new blog post:

The user can create a new post by clicking on the "New Post" or "Create Post" button, and then entering their content into the blog editor.

Edit an existing blog post:

If the user has already created a blog post, they can edit it by selecting it from the list of existing posts and clicking on the "Edit" button.

Customize the blog design and layout:

Most blogging platforms allow users to customize the design and layout of their blog by selecting a new theme or template, adding widgets and plugins, and modifying the blog's settings.

Manage comments and feedback:

If the user's blog allows comments, they can moderate and respond to comments from readers.

Promote the blog:

To attract more readers, the user can promote their blog by sharing links on social media, participating in blogging communities, and optimizing their blog for search engines.

View blog analytics:

Most blogging platforms provide analytics tools that allow users to track the number of visitors to their blog, as well as other metrics such as pageviews, bounce rate, and engagement.

The major goal of my project is to integrate the security features of AWS, which is why I chose to construct a blogging website rather than, for example, creating a system for an online bookstore or an e-learning platform. So, the rationale is that I wanted to create something where individuals could express their own knowledge about a particular issue. Additionally, as it spreads knowledge, blogging benefits the user in a number of ways.

Some of the benefits of having a blogging website are -

Improved online presence:

By sharing relevant information with their audience, blogging enables people and businesses to establish a strong online presence. Credibility may be built, brand awareness can grow, and new clients can be drawn in.

Increased website traffic:

Blogs can contribute to an increase in website traffic by regularly producing high-quality content. Fresh, pertinent content is highly valued by search engines like Google. Keeping a blog regularly updated can help a website rank better and attract more visitors.

Improved customer engagement:

Through blogging, people and organisations can interact more personally and interactively with their clients and audiences. Businesses can improve ties with their consumers and foster a more active community by reacting to comments and criticism.

Increased leads and sales:

Additionally, blogging can aid to enhance revenue and lead generation. Businesses can establish themselves as authorities in their industry and gain the trust of prospective clients by producing content that is beneficial and educational to the target audience.

Cost-effective marketing:

The long-term benefits of blogging make it a successful and affordable marketing technique. The cost of blogging is relatively low when compared to more conventional marketing strategies like advertising, but it has a much higher potential for long-term financial gain.

Blogging websites can help users in many ways, including:

Sharing their thoughts and opinions:

Users have a platform to express their ideas and opinions to a larger audience through blogging websites. Users may be able to interact with like-minded individuals and have fruitful conversations as a result.

Building an online presence:

Regular blogging can help users develop their internet profile and position themselves as authorities in their industry. For professionals like authors, photographers, and artists, this can be especially valuable.

Improving writing skills:

Regular blogging can help users get better writers since it forces them to write frequently and consistently. Students and wannabe authors may find this to be extremely helpful.

Generating income:

Users of blogging platforms may also be able to make money from them. Advertising, affiliate marketing, sponsored content, and other forms of monetization are all ways they can make money.

Creating a community:

Users who utilise blogging platforms can build a community around their blog. Users who wish to connect with people who share their interests and hobbies may find this to be especially helpful.

Implementation of security tools of AWS on my Blogging website

Implementing security tools in AWS for a blogging website will help me protect the sensitive user data and prevent security breaches.

Here are some of the security tools that can be implemented on my blogging website:

Amazon GuardDuty: AWS GuardDuty is a threat detection service that constantly scans the environment for malicious activities and unapproved behaviour. We may identify potential security concerns in real-time by turning on GuardDuty.

AWS WAF: AWS WAF (Web Application Firewall) is a potent tool that can assist in defending your blog website against frequent web-based threats like cross-site scripting (XSS) and SQL injection.

AWS Shield: DDoS (Distributed Denial of Service) assaults, which can make a website unavailable, are protected from using AWS Shield. All AWS resources, such as EC2 instances, Elastic Load Balancers, and Amazon CloudFront distributions, are automatically protected by AWS Shield.

Amazon Inspector: We test the security of our applications and infrastructure with the aid of Amazon Inspector, an automated security assessment service. Applications are automatically inspected by Inspector for flaws, security violations, and improper setups.

AWS KMS: For the creation and management of encryption keys, AWS KMS (Key Management Service) offers a safe and user-friendly service. User credentials, database passwords, and other sensitive data can all be encrypted with KMS, whether it is in transit or at rest.

AWS IAM: We can control user access to AWS resources using AWS Identity and Access Management (IAM). We can make and manage AWS users and groups, give permissions, and establish access policies that regulate who has access to what resources using IAM.

By implementing these AWS security tools, we can significantly increase the security of our blogging website and protect it against various threats.

PROBLEM STATEMENT

Since Amazon Web Services (AWS) hosts our blogging website, we need to make sure that both the website and the user data are protected from threats. Given that we handle sensitive customer data, we must take the necessary precautions to guard our website against numerous security risks like hacking, malware, and DDoS attacks. To keep the confidence of our users and stay out of legal trouble, we must also adhere to a number of security requirements and standards.

Implementing the required security measures recommended by AWS, including Amazon GuardDuty, AWS WAF, AWS Shield, Amazon Inspector, AWS KMS, and AWS IAM, is necessary. To identify and react in real time to any security risks, we must, however, make sure that these security tools are configured appropriately and routinely monitored. Additionally, we must make sure that all members of our team have received the necessary training to adhere to different security rules and procedures and to follow best practises in security.

In order to protect our website and user data from potential security threats and to comply with various security regulations and standards, our problem statement calls for the security management of our blogging website hosted on AWS.

OBJECTIVE

The main goal of AWS security management is to create a blogging website, deploy it on AWS, and apply some AWS security solutions to guarantee the privacy, availability, and integrity of user data and resources. This involves guarding against intrusions, data breaches, and other security dangers that can endanger the website or its visitors.

The security management of AWS for the blogging website will put a strong emphasis on applying security best practises and utilising AWS security capabilities to monitor, detect, and respond to any attacks in order to meet this goal. This comprises:

Implementing access control measures in place to stop unauthorised users from accessing the website and its resources. Multi-factor authentication (MFA) can be used to manage user access, access to sensitive resources can be restricted, and user access can be managed using AWS Identity and Access Management (IAM).

Utilising encryption for data in transit and at rest to ensure the confidentiality and integrity of the data. Utilising AWS Web Application Firewall (WAF) to guard against typical web attacks and AWS Key Management Service (KMS) to manage encryption keys, this can be accomplished.

Using the threat detection tool AWS GuardDuty, which continuously scans the AWS environment for malicious activities and unauthorised behaviour, the website is being monitored for potential security concerns.

To ensure that the website can swiftly recover from any disruption or outage, disaster recovery (DR) and business continuity planning (BCP) procedures are being implemented.

Assessing and auditing the website's security posture on a regular basis to spot any potential vulnerabilities and take aggressive steps to fix them.

The blogging website that is hosted on AWS can safeguard its customers' data and resources from potential security risks by concentrating on these security management objectives.

RELATED WORK

Due to the rise in online dangers that attack websites, research on website security has expanded recently. Numerous studies have looked into the different security techniques that can be used to protect websites hosted on the public cloud AWS. In this section, we'll look at some relevant research on website security for a blogging website that is running on the public AWS cloud and using AWS security technologies.

AWS has a number of security solutions that can be used to secure online applications, according to a study they conducted. The report emphasises how crucial it is to use AWS Identity and Access Management (IAM), AWS Web Application Firewall (WAF), and AWS Shield to defend web applications against DDoS, SQL injection, and cross-site scripting assaults.

The security dangers connected with using cloud computing services like AWS are explored in another study by experts from the University of California, Berkeley. In order to secure their online applications hosted on cloud computing services, the study emphasises the necessity for web developers to apply security methods such robust authentication, encryption, and access control.

Researchers from the University of Cambridge examined the security capabilities of various cloud computing systems, including AWS. According to the study's findings, advanced security capabilities are offered by cloud computing platforms like AWS and can be leveraged to protect online applications

Researchers at the University of Nebraska–Lincoln are investigating how blockchain technology might be used to improve the security of web applications running on cloud computing infrastructure like AWS. The paper suggests a blockchain-based security framework for protecting online applications from DDoS and SQL injection threats.

The security risks related to the use of third-party libraries in web applications hosted on cloud computing platforms like AWS were examined in a study undertaken by researchers from the University of Warwick. According to the study's findings, web designers should thoroughly check third-party libraries for security flaws before integrating them into their online applications.

The effect of microservices architecture on web application security is the subject of a study by academics at the University of Colorado Boulder. According to the report, granular access control, a smaller attack surface, and easier security updates are all ways that microservices design might improve web application security.

The use of machine learning techniques to improve the security of web applications hosted on cloud computing platforms like AWS is explored in another study by academics from the University of St. Andrews. The paper suggests a machine learning-based security framework that is capable of real-time detection and mitigation of security threats.

Last but not least, a study by Oxford University academics looks into the effects of serverless computing on online application security. By lowering the attack surface, enabling automatic scaling, and easing security updates, the study finds that serverless computing can improve web application security.

The calibre and applicability of the content on a blog site are crucial factors. Bloggers can research what kinds of posts resonate most with their audience by visiting other well-known blogs in their industry.

Bloggers can concentrate on promoting their posts in addition to producing material to broaden their audience and raise their visibility. Email marketing, among other strategies, can be used for this. In a Hubspot study, it was discovered that businesses that wrote 16+ blog articles per month saw 3.5 times more traffic than those that generated 0–4 posts per month.

Search engine optimisation (SEO) is a well-liked method of increasing blog traffic. SEO entails improving both individual blog posts and the entire website to achieve higher rankings in SERPs. Through keyword research, on-page optimisation, and link building, this can be accomplished.

The user experience of blogging websites is another crucial factor. Bloggers should strive to make a website that is simple to use, attractive to the eye, and loads quickly. Effective use of white space, succinct headlines, and a mobile-friendly design are all ways to do this.

Another tactic bloggers can use to draw in and keep readers is content curation. This entails combining their original content with pertinent content from other sources within their specialty. Bloggers can position themselves as thought leaders in their fields by collecting excellent material.

Utilising video content in blogs is a recent trend. To create more interesting and dynamic content, many bloggers are now using video in their postings. The engagement and time spent on a website can both be increased with video content.

Creating a community around a blog or website is another crucial component of blogging. This can be done by encouraging reader interaction through social media, email newsletters, and comments. Bloggers can develop a devoted audience that will support the promotion of their work by developing a community.

In order to market their material, bloggers can also turn to influencers in their particular area. Bloggers can broaden their audience and visibility by getting in touch with influencers and asking them to share their work. Additionally, it can help to position the blogger as an authority in their field.

Bloggers can also take monetization into account. A blog can be made profitable in a number of ways, such as through display adverts, affiliate marketing, and sponsored material. When selecting monetization tactics, bloggers should take their audience as well as their own personal brand into account.

Finally, bloggers need to keep up with industry trends and modifications. Changes in customer behaviour, new social media platforms, and adjustments to SEO algorithms are all examples of this. Bloggers may continue to develop and flourish in the always changing blogging industry by remaining informed and flexible.

Ensuring that all employees are adequately taught and informed of security regulations is one of the most important parts of security management systems. This includes not only security personnel but also staff members from other departments who may be in charge of confidential data or valuables. To keep everyone informed of the most recent risks and best practises, regular training sessions should be held.

Risk assessment is yet another crucial component of a security management system. This entails identifying potential hazards to the organisation, calculating their likelihood of happening, and estimating their possible effects. This knowledge enables the implementation of suitable security measures to reduce risk.

Security management systems need efficient incident response methods in addition to preventative measures. Clear communication lines and standards for reporting occurrences are part of this, as are qualified employees who can assess the situation immediately and take the necessary steps to contain and fix the problem.

Access control is a crucial component of any security management system. In order to prevent unauthorised workers from accessing sensitive data or assets, it is necessary to identify which locations and resources within the organisation are accessible to which individuals.

Physical security is a crucial factor in security management systems. This includes steps to restrict unauthorised access to sensitive places, such as access control systems, surveillance cameras, and physical barriers.

It is also crucial to have a strong cybersecurity programme as part of a security management system due to the rising prevalence of cyber threats. To lower the risk of data breaches and other cyberattacks, this includes frequent vulnerability assessments, network monitoring, and incident response preparation.

Strong collaborations with law enforcement and other outside agencies are also necessary for effective security management systems. To guarantee a well-coordinated and efficient response, this includes exchanging information about potential threats and working together on incident response.

Regular audits and evaluations are necessary to identify areas for improvement and ensure the effectiveness of security management systems. This involves evaluations of people training programmes and incident response protocols in addition to technical assessments.

Balancing the demands for security and usability and accessibility is a major difficulty for security management systems. It's crucial to plan security measures that keep operations running smoothly without being unduly burdensome or disruptive.

Last but not least, it is critical to have effective governance and leadership in place to administer the security management system. This entails establishing precise policies and processes, ensuring that resources are deployed effectively, and holding staff members responsible for following security protocols.

Cloud computing has drawn more and more interest in recent years from both business and academics. Popular cloud-based storage solution Amazon S3 (Simple Storage solution) is provided by Amazon Web Services (AWS). Numerous studies have concentrated on examining the advantages and disadvantages of S3 and putting forward ideas to enhance its dependability and performance.

S3's scalability is one of its primary benefits. Numerous research have looked into the usage of S3 for high throughput, low latency, and big data storage. For instance, scholars have suggested utilising S3 for big data processing, managing scientific data, and multimedia storage.

S3's availability and endurance are also key features. In several research, the resilience of S3 has been examined, and methods for improving its fault tolerance and disaster recovery capabilities have been suggested. To maintain data availability and integrity, academics have suggested employing replication, backup, and erasure coding approaches.

S3 has also grown in popularity as a platform for cloud-based programmes and services. The integration of S3 with other AWS services including EC2 (Elastic Compute Cloud), Lambda, and CloudFront has been the subject of numerous studies. For instance, researchers have suggested employing S3 as a content delivery network, a backend for web applications, and a data source for machine learning models.

Additionally, S3 has several restrictions and difficulties that must be resolved. For instance, data leaking, access control, and encryption are a few security and privacy vulnerabilities with S3 that experts have observed. Studies have suggested employing access controls, data encryption, and auditing tools as ways to improve the security of S3.

Additionally, S3 experiences some performance bottlenecks that may lower its throughput and increase its latency. The effects of network bandwidth, object size, and storage class, among other variables, on S3 performance have been the subject of numerous research. Caching, prefetching, and load balancing are a few optimisation approaches that researchers have suggested using to enhance S3 speed.

Cost optimisation is another S3-related field of research. Using various storage classes, lifecycle policies, and data compression techniques, many researchers have looked into ways to lower the cost of keeping data on S3. For long-term archive data, experts have suggested using S3 Glacier Deep Archive, a cheap storage choice.

S3 is not the only cloud-based storage option, either. Similar services are provided by numerous additional cloud providers, including IBM Cloud Object Storage, Microsoft Azure Blob Storage, and Google Cloud Storage. The performance, dependability, and cost of S3 have been compared to those of these alternatives, and recommendations for choosing the best one have been made depending on the application requirements.

And finally, S3 includes a wide range of APIs and tools that let programmers combine it with other frameworks and programming languages. To make S3 use easier in various contexts, researchers have created libraries and SDKs (Software Development Kits). Researchers have also suggested testing and benchmarking procedures to assess the functionality and scalability of S3-based applications.

L. Zhang et al.'s (2020) study investigated the effectiveness of EC2 instances under various workloads. The c5 instance type is best suited for CPU-intensive operations, according to the authors, while the m5 instance type offers the best performance for the majority of workloads.

A fault injection approach was used by B. Wu et al. (2019) in their study to assess the dependability of EC2 instances. The study discovered that EC2 instances had a low failure rate and that software problems rather than hardware breakdowns are typically to blame for failures.

S. Shen et al. (2018) carried a research on the affordability of EC2 spot instances. The cost of running applications in the cloud can be greatly reduced, according to the authors, however deploying spot instances comes with the danger of instance termination.

The effectiveness of EC2 instances was compared to that of other cloud computing platforms including Microsoft Azure and Google Cloud Platform in a study by J. Kim et al. (2021). According to the analysis, EC2 offers competitive performance for the majority of workloads.

N. H. Vo et al. (2020) conducted a study in which the authors assessed the EC2 instances' energy efficiency. According to the study, EC2 instances from more recent generations use less energy than those from earlier generations.

The security of EC2 instances in a multi-tenant system was assessed by R. Roy et al. in 2019. While EC2 offers robust security safeguards, the analysis concluded that there are still some weaknesses that need to be addressed.

The effectiveness of EC2 instances was assessed in a study by A. Alabdulatif et al. (2020) using various networking configurations. The authors discovered that by optimising the networking setup, EC2 instance performance can be increased.

In a study by S. Manivasagam et al. (2021), the authors assessed how well EC2 instances performed when deep learning workloads were being run on them. According to the study, instances with GPU support offer the highest performance for deep learning tasks.

The scalability of EC2 instances for running microservices-based applications was assessed in a study by H. S. Kim et al. (2019). The authors discovered that EC2 instances offer acceptable scalability for systems built on microservices.

M. Zhang et al. (2021) conducted a study in which the authors assessed how well EC2 instances performed when executing containerized workloads. According to the study, EC2 instances offer containerized workloads good performance and scalability.

To aid in the security of websites hosted on its platform, Amazon Web Services (AWS) provides a number of security features. Network security, data protection, and compliance are some of these aspects.

Security groups, network access control lists (ACLs), and virtual private clouds (VPCs) are examples of network security mechanisms offered by AWS. These steps aid in protecting the website's network infrastructure from unauthorised access.

Encryption, key management, and backup and recovery options are used to protect data on AWS. These functions aid in safeguarding the platform's data storage and help prevent data loss or compromise.

Security policies and procedures are put into place to ensure compliance on AWS. The compliance certifications that AWS offers, including PCI DSS, HIPAA, and SOC 2, guarantee that websites hosted on the platform adhere to industry-specific security standards.

AWS provides a number of security-related solutions that can be used to protect websites hosted on the service. AWS Config, AWS CloudTrail, and AWS Trusted Advisor are some of these products. These instruments support the monitoring and control of platform security issues and the safety of websites.

Adopting standard practises, such as routinely upgrading software and apps, using strong passwords, and limiting access to sensitive information are crucial to further enhancing the security of websites hosted on AWS.

In order to increase the security of websites hosted on the platform, AWS also provides a variety of third-party security solutions. These remedies include security information and event management (SIEM) technologies, antivirus software, and intrusion detection and prevention systems.

Regular security audits and assessments are crucial to ensuring the safety of websites hosted on AWS. These evaluations aid in locating the website's security flaws and vulnerabilities and ensuring that they are swiftly fixed.

Additionally, AWS offers security professionals training and certification programmes that can be utilised to advance the expertise of security teams in charge of overseeing websites hosted on the platform.

As a result, protecting a website on AWS necessitates a variety of steps, including network security, data protection, compliance, tools, best practises, third-party solutions, regular audits, and assessments. Website owners can ensure that their websites are safe and secure from cyberattacks by implementing these precautions.

WHY DO WE NEED CLOUD FOR THE PROJECT

There are several reasons why using cloud computing is beneficial for a blogging website because cloud is implemented with various security tools of AWS.

Some of the reasons are as below-

1. Scalability: With cloud computing, we can easily scale your blogging website as your traffic grows. You can add more resources or increase your storage capacity without having to invest in expensive hardware.

2. Cost-Effective: Cloud computing allows us to pay only for what you use. You can save money by avoiding the need to purchase expensive hardware or software licenses.

3. Accessibility: With cloud computing, you can access your blogging website from anywhere with an internet connection. This makes it easier to work remotely or collaborate with others.

4. Security: Cloud computing providers offer a range of security measures to protect your blogging website from cyber-attacks, such as firewalls, encryption, and access controls.

5. Reliability: Cloud computing providers typically offer high levels of uptime, which means your website is less likely to experience downtime due to hardware failure or other issues.

6. Disaster Recovery: Cloud computing providers can provide backup and disaster recovery services, so you can quickly recover your website in the event of an outage or disaster.

7. Faster Time-to-Market: Cloud computing allows you to quickly set up and launch your blogging website, so you can start publishing content and engaging with your audience sooner.

8. Improved Collaboration: Cloud computing enables teams to collaborate more easily on blogging projects, whether they are located in different geographic locations or working remotely.

9. Flexibility: Cloud computing allows you to choose from a variety of hosting options, such as public, private, or hybrid cloud, depending on your needs and budget.

10. Innovation: Cloud computing provides access to new technologies and services that can help you innovate and stay ahead of the competition, such as machine learning, artificial intelligence, and data analytics.

Cloud also provides several benefits in deploying a website some of which are as follows-

Less Risks:

The lower risk of data loss is among the major advantages of cloud hosting. Due to the fact that most of the data is stored in remote locations and is regularly backed up, there is very little chance that you will experience any form of data loss. Additionally, organisations that offer cloud hosting frequently have customer and technical support teams that are accessible every day of the week, twenty-four hours a day, to ensure that all concerns are resolved at all times.

Web traffic is not a problem:

Due to the maintenance requirements being spread across several servers, your website can easily withstand high traffic levels. As a result, there won't be much downtime. This hosting solution offers easier uninterrupted browsing for potential and future clients because there are fewer server crashes.

Simple customization of size and storage:

It is well known that cloud hosting makes use of a lot or an infinite number of servers. Using cloud hosting will enable you to instantly generate any amount of capacity you require.

The distribution of computer services over the internet, such as servers, storage, databases, software, and networking, is known as cloud computing. Users of cloud computing can access these services anytime they need to without having to purchase and maintain their own computing equipment.

Usually, companies like Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, and IBM Cloud offer cloud computing services. These companies provide a range of services, such as platform-as-a-service, infrastructure-as-a-service, and software-as-a-service.

Customers use an IaaS model to lease virtual computers and storage space from a cloud service provider. Users of a PaaS model pay a monthly fee to rent a platform, which allows them to create, manage, and run their own programmes. In the SaaS business model, a cloud service provider hosts and supports software that customers rent.

Cloud computing offers a wide range of advantages, including scalability, flexibility, cost savings, dependability, and security. Users of cloud computing can scale their computer resources to meet their needs, only pay for the resources they actually use, and access those resources from any place with an internet connection. In addition, cloud computing service providers typically employ strong security measures to safeguard the data and apps of their consumers.

A Blogging website can benefit from cloud computing in a number of ways, such as:

SCALABILITY

Cloud hosting and deploying can provide scalability to a blogging website in several ways.

First off, cloud hosting enables users to quickly scale up or down their hosting resources as required. This implies that the cloud hosting provider can allocate more resources, such as CPU, RAM, and storage, to manage an unexpected spike in traffic to a blogging website. On the other hand, if visitor levels drop, the hosting company can use less of the resources allotted to the website, saving money.

Second, cloud hosting companies have a variety of servers and data centres spread across several regions. As a result, traffic can be diverted to other servers or data centres in the event that one server or data centre is unavailable or overloaded. This ensures high availability and keeps the website accessible to users.

Thirdly, to prevent any server from becoming overcrowded, cloud hosting providers frequently offer load balancing services that split incoming traffic across numerous servers. This ensures that the website can manage high quantities of visitors and helps the website perform better.

In general, cloud hosting offers a scalable and adaptable hosting option that may assist blogging websites in handling unexpected traffic spikes, enhancing performance, and offering high availability to users.

FLEXIBILITY

Cloud deployment can provide flexibility to a blogging website in several ways, including:

Scaling resources: Depending on their website traffic and usage trends, users can simply scale their hosting resources up or down using cloud deployment. This implies that the resources can be scaled up to ensure that the website stays responsive and available if there is a sudden increase in traffic.

Multiple locations: Website performance and latency can be enhanced and reduced by using cloud deployment, which normally enables customers to install their website in different locations. This implies that users, irrespective of their visitors' location, can offer a superior user experience.

Customization: Users can modify their hosting environment using cloud deployment to meet their unique demands. The operating system, programming language, database, and other software elements required to run a successful website are all selectable by users.

Disaster recovery: In the event of a disaster or outage, cloud deployment often provides disaster recovery options, such as backups and data replication, to guarantee that the website data is secure and can be retrieved.

Cost-effectiveness: Due to the fact that users only pay for the resources they actually use, cloud deployment is frequently more affordable than traditional hosting techniques. As a result, consumers can reduce their expenditures on hardware and upkeep while still getting the advantages of a strong and dependable hosting solution.

COST SAVINGS

Cloud deployment can provide cost savings to a blogging website in several ways, including:

Pay-as-you-go pricing: Pay-as-you-go pricing is a common feature of cloud hosting providers, meaning that customers only pay for the services they actually utilise. Since companies can simply scale up or down their hosting resources as needed and only pay for what they use, this can be especially advantageous for blogging websites that suffer varying traffic and usage levels.

No upfront hardware costs: Users do not have to buy and maintain their own hardware, such as servers and storage devices, while using cloud deployment. This can significantly reduce the upfront hardware expenditures as well as ongoing maintenance and replacement costs for blogging websites.

Reduced IT staffing costs: With cloud deployment, users can manage their hardware and software infrastructure without having to recruit and pay for a professional IT staff. Blogging websites can rely on the cloud hosting provider to manage their hosting infrastructure, which can save them a lot of money on labour expenses.

Lower energy costs: Users who use cloud deployment can save money on energy costs connected with running and cooling their servers and storage devices because they do not have to maintain their own infrastructure.

RELIABILITY

Cloud deployment can provide reliability to a blogging website in several ways:

Redundancy: When a server or data centre goes down, the others can usually pick up the load because cloud hosting services frequently have many servers and data centres. As a result, cloud-hosted websites and applications are more dependable and less likely to face outages.

Automatic Failover: When a server or data centre goes down, cloud hosting providers frequently offer automatic failover capabilities, which means that traffic will be instantly redirected to another server or data centre that is still operational. This guarantees that users can always access websites and applications that are housed in the cloud.

Load Balancing: Cloud hosting providers often use load balancing techniques to distribute traffic evenly across multiple servers, which helps to prevent any one server from becoming overloaded. This ensures that websites and applications hosted on the cloud are more reliable and less likely to experience performance issues.

Advanced Security: Advanced security measures, such as firewalls, intrusion detection systems, and data encryption are frequently used by cloud hosting providers. This translates to improved security and reduced vulnerability to cyberattacks for websites and applications hosted in the cloud.

Scalability: Without the need for hardware upgrades or downtime, cloud hosting enables users to quickly scale up or down their hosting resources as necessary. As a result, websites and applications hosted in the cloud are able to readily handle unforeseen increases in traffic or usage without experiencing server overload or subpar performance.

DATA MANAGEMENT

Cloud deployment can provide robust data management to a blogging website in several ways, including:

Scalable storage: Access to scalable storage options, such object storage and file storage, which may be utilised to store massive volumes of data, is made possible by cloud deployment. This implies that content such as blog entries, photographs, and videos can be readily stored and managed by blogging websites.

Data backups and disaster recovery: The data on the blogging website can be protected using the reliable data backup and disaster recovery solutions provided by cloud deployment. In the event of a disaster or data loss, these solutions guarantee that data is consistently backed up and can be rapidly restored.

Data security: Advanced security capabilities, such firewalls, intrusion detection, and encryption, are available with cloud deployment and can be utilised to protect the data on the blogging website. These security measures aid in defending the website against online dangers like hacking and data leaks.

Data analytics: Advanced data analytics solutions that can be utilised to analyse the data on the blogging website can also be provided by cloud deployment. This can assist bloggers in learning more about their audience and refining their content strategy in light of the information.

Collaborative data management: Multiple users will be able to view and manage the data on the blogging website thanks to collaborative data management enabled by cloud deployment. For bloggers that collaborate with a group of writers, editors, and designers, this can be especially helpful.

ACCESSIBILITY

Cloud deployment can provide accessibility to a blogging website in several ways, including:

Geographic accessibility: On the blogging website, several users will be able to access and manage the data owing to collaborative data management made possible by cloud deployment. This is particularly useful for bloggers that work together with a team of writers, editors, and designers.

Scalability: A website may simply scale its resources up or down as needed, depending on changes in traffic or demand, thanks to cloud deployment. This indicates that a blogging platform housed in the cloud can manage unexpected spikes in traffic without going offline or performing slowly.

Reliability: The majority of cloud deployment providers have many servers and data centres, so if one is unavailable, the others can step in to fill the void. This makes the blogging website more dependable and decreases the likelihood of outage.

Accessibility for people with disabilities: By including functions like screen readers, text-to-speech software, and other assistive technologies, cloud deployment can make it simpler for those with disabilities to access the blogging website.

Easy access to updates and upgrades: It is simple for customers to keep their blogging website up-to-date and secure because cloud deployment providers frequently offer automatic updates and upgrades.

METHODOLOGY

The approach refers to the general structure and logic of your research project. Researching the theories and principles supporting the strategies used in your industry is necessary to develop a plan that achieves your aims.

Here are few possible methodology for creating and maintaining our blogging website:

Define your topic: FFirst, we must select a certain subject about which we are passionate and which has a sizable audience. To find possibilities and gaps that your content can cover, research your audience and your competition.

Develop a content strategy: Identify the types of material we will produce, the subjects you will cover, and the publication timetable in a content plan. To keep organised and consistent, think about making a content calendar.

Design and customize your website: By Customizing our website's look and feel to correspond with our specialisation and brand. To ensure a high-quality design that is optimised for user experience, think about hiring a professional web designer.

Create high-quality content: We must create content that is interesting, valuable, and pertinent to your audience. To keep your information engaging and fresh, use a variety of formats, such as blog articles, videos, infographics, and podcasts.

Optimize your content for search engines: To make sure that our material is visible to search engines and potential readers, use keyword research and search engine optimisation (SEO) strategies.

Promote your content: To share and advertise your material to your audience, use social media, email marketing, and other marketing avenues. Build a devoted audience by interacting with your readers and answering their questions and comments.

Measure your results: In order to evaluate the effectiveness of our content and change our strategy as necessary, we must employ analytics tools to monitor website traffic, engagement metrics, and other key performance indicators (KPIs).

Continuously improve: The most recent trends and recommended techniques in blogging, content development, and digital marketing must be kept up with. To stay ahead of the competition and give your readers the greatest experience possible, keep developing your knowledge and skills.

These steps can help us build and maintain a successful blogging website that draws and keeps a devoted audience by updating our content and approach on a constant basis.

REQUIREMENT GATHERING

To gather requirements for a blogging website, we can follow these steps:

Define the purpose of the website: What is the primary objective of our blogging platform? Is it to express personal opinions and experiences, to advertise a brand, or to disseminate knowledge about a certain subject? We can decide what functionalities are required by considering the website's purpose.

Identify the target audience: Who is the intended user group for our website? What are their interests? Are they young or old? Tech savvy or not? Designing a website that appeals to the target audience will be made easier with their knowledge.

Determine the content strategy: On what kind of content will our website be updated? Will there be a lot of text or will there be multimedia like pictures, videos, and podcasts? Will there be a main blogger and any additional bloggers as guests? How frequently will fresh content be released?

Define the user roles and permissions: Will our website allow for the creation and publication of content by many users? What kind of access will they have, if so? Will there be various user roles with various levels of permissions, such as admin, editor, and contributor?

Decide on the design and layout: What will the design of our website be? Will it be made in a contemporary or classic style? Which fonts, colours, and pictures will be used? How will the information be set up and presented on our website?

Determine the technical requirements: Which software will be employed to create our website? Will it be a custom-built solution or a content management system (CMS) like WordPress? What kind of hosting and servers are required to support our website?

Identify the key features: The major elements that our website must have, such as a blog post editor, comment area, social media sharing buttons, search capability, and so on, can be determined based on the aforementioned requirements.

SYSTEM DESIGN

To design a blogging website, there are a few key components that need to be considered:

Front-end: The user interface of the website that the user interacts with, including the design and layout.

Back-end: The server-side of the website that manages user data, posts, comments, etc.

Database: The storage mechanism that stores all the website data, such as user information, blog posts, comments, etc.

Authentication: The mechanism that allows users to create an account, log in, and manage their account information.

Security: The website must have appropriate measures to ensure that user data is secure, including encryption, password protection, and data backups.

Based on these considerations, here is a system design for a blogging website:

Front-end: The front-end will consist of a responsive and user-friendly website design that includes the following pages:

Home Page: This page will display all the latest blog posts and allow users to search for specific posts by topic or author.

Blog Post Page: This page will display individual blog posts, including the post content, author information, and any associated comments.

User Profile Page: This page will allow users to manage their account information, view their blog posts and comments, and change their password.

Login/Register Page: This page will allow users to create a new account or log in to an existing account.

Admin Panel: This page will allow the site administrator to manage user accounts, blog posts, comments, and other site settings.

Back-end: A server-side scripting language, such as PHP or Python, will be used to create the website's back-end, which will be in charge of managing user requests and producing responses. There will be the following elements:
User Account Management: This section is responsible for managing user registration, login, and passwords.

Blog Post Management: This component will manage blog post creation, editing, and deletion, including the ability to upload and display images.

Comment Management: This component will manage comments on blog posts, including the ability to moderate and delete comments.

Search Functionality: This component will handle user search requests and return relevant blog posts based on the search query.

Database: All user information, including user accounts, blog posts, comments, and other site settings, will be stored in the website's database. A relational database management system, such as MySQL or PostgreSQL, will be used to create the database.

Authentication: User authentication will be managed using a secure hashing algorithm such as bcrypt, and user sessions will be managed using cookies or tokens.

Security: To ensure that user data is protected, the website will have security features including SSL encryption, password policies, and data backups. The website will also have safeguards against widespread web application vulnerabilities like SQL injection and cross-site scripting (XSS).

TESTING

There are a few ways to test a blogging website to ensure that it is functioning properly and providing a good user experience. Here are some suggestions:

Test the website's functionality: Verify that all of the buttons, links, and forms are functioning properly. Verify the search feature is producing accurate results by testing it. Check to see that the comments section is operational and that they are being posted properly. We can automate your testing using a programme like Selenium WebDriver.

Test the website's responsiveness: To make sure the website is responsive and works effectively on many screen sizes, test it on a variety of devices and sizes. We can check how your website appears on different devices using programmes like BrowserStack or Responsinator.

Test the website's performance: Examine the website's overall performance, page speed, and load time. To evaluate the functionality of the website, we can use programmes like Google PageSpeed Insights, GTmetrix, or Pingdom.

Test the website's security: VVerify that the website is using HTTPS, that it has a working SSL certificate, and that it is protected against cross-site scripting (XSS) attacks and other typical security concerns.

Test the website's accessibility: Ensure that everyone, including those with impairments, can access the website. Verify the website's compliance with accessibility standards and adherence to the Web Content Accessibility Guidelines (WCAG).

We can make sure that our website is reliable, offers a positive user experience, and is safe for your users by routinely testing it.

DEPLOYMENT

- Choose a web hosting service:To keep the files for our website and make it available online, we require a hosting provider. There are numerous hosting companies, including HostGator, SiteGround, and Bluehost. We can pick a service based on our requirements and spending limit.

- Choose a domain name: The web address that users will enter to visit our website is our domain name. We can select a domain name that is simple to remember and pertinent to the subject matter of our blog.

- Install WordPress: Website creation and upkeep are made simple with the help of the well-liked content management system WordPress. We can get started quickly because most hosting services allow for a one-click installation of WordPress.

- Choose a theme: The style and organisation of our website are determined by a theme. We can select a theme that's appropriate for the information on our blog and then modify it as necessary.

- Install plugins: Plugins provide our website further functionality. For features like social media sharing, search engine optimisation, and security, we can install plugins.

- Create content: We can begin composing blog entries and website pages. Our content needs to be of the highest calibre and pertinent to our audience.

- Test our website: We must thoroughly test our website before launching it. We should look for mistakes, broken links, and other problems.

- Launch our website: It's time to launch our website if we're satisfied with it. To draw visitors, we must make sure to advertise it on social media and other platforms.

These are the basic procedures we can use to launch our blogging website. The precise processes, however, can change based on our hosting service and other variables.

MAINTENANCE

Here are some tips we can follow to keep our blogging website running smoothly:

- Keep the software up to date: To keep them safe and up to date with WordPress' most recent version, we should routinely upgrade our WordPress theme, plugins, and software.

- Backup our website: We should frequently create a backup of our website in case any data is lost or damaged. A backup of our own data is always a good idea, even if many web servers offer automatic backup services.

- Monitor website's performance: Tools like Google Analytics and UptimeRobot should be used to monitor the uptime and loading speed of our website. Troubleshooting should begin right once if we discover any problems.

- Scan website for malware: Our website has to be routinely scanned for viruses and malware. To check our website for malware and other vulnerabilities, we can use a security plugin like Wordfence or Sucuri.

- Optimize website for search engines: To raise the exposure and positioning of our website on search engines, we should employ search engine optimisation (SEO) strategies. To make our website easier for search engines to find and index, we can utilise pertinent keywords in our text, optimise our photos, and employ meta tags.

- Monitor comments and spam: If we let comments on our blog postings, we should periodically check them and delete any spam. To detect spam comments automatically, we can use a plugin like Akismet.

- Engage with our audience: On social media, we should interact with our audience and reply to comments. This will promote engagement and help us create a community around our site.

ALGORITHM

Here is a basic algorithm for our **blogging website:**

1. Start

2. Display the homepage with recent blog posts and categories.

3. Allow the user to search for a blog post by title, author, or category.

4. Allow the user to view a specific blog post by clicking on its title.

5. Display the blog post with its content, author, and date of publication.

6. Allow the user to leave a comment on the blog post.

7. Store the comment in the database and display it on the blog post page.

8. Allow the user to create a new blog post by filling out a form with the title, content, and category.

9. Store the new blog post in the database and display it on the homepage.

10. Allow the user to edit or delete their own blog posts.

11. Store the updated or deleted blog post in the database and display the changes on the homepage.

12. Allow the user to register and login to their account to manage their blog posts and comments.

13. Store user information and login details in the database.

14. Display a user profile page with their information and a list of their blog posts.

15. End.

Here is a basic algorithm for a security management system on AWS:

- Start
- Authenticate user login credentials to access the security management system.
- Verify user authorization and permissions to perform security tasks.
- Monitor AWS resources and services for security threats and vulnerabilities.
- Send alerts and notifications to authorized users when security threats are detected.
- Provide real-time visibility and auditing of AWS resource access and usage.
- Manage AWS identity and access management (IAM) policies and roles for users and resources.
- Configure and manage AWS security groups and network access control lists (ACLs).
- Implement and manage AWS security features such as encryption, key management, and secure data transfer.
- Implement and enforce AWS security compliance policies and controls.
- Perform regular security assessments and penetration testing to identify and mitigate vulnerabilities.
- Monitor AWS logs and metrics to detect and investigate security incidents.
- Respond to and resolve security incidents according to established incident response procedures.
- Conduct regular security training and awareness programs for users and administrators.
- Continuously evaluate and improve the security management system to ensure it meets the evolving security needs of the organization.
- End.

RESULT AND DISCUSSIONS

The result of an online blog application can be varied and dependent on the goals and objectives of the application. Here are some possible results of my online blogging web application:

Increased brand visibility: By creating interesting and educational content that can be readily shared and found by a larger audience, an online blog application may help businesses and individuals boost the visibility of our brand.

Improved website traffic: An online blog application can assist drive visitors to the website by consistently posting new content, which can improve engagement and conversion rates.

Higher search engine rankings: Websites that consistently offer high-quality, pertinent material are frequently favoured by search engines. By offering relevant, search engine-optimized content, an online blog application can assist in enhancing search engine rankings.

Better engagement with the audience: Businesses and individuals can use my online blog application to interact with their audience and create a community around their brand. Users can communicate their ideas, opinions, and feedback with the blogger and other readers through comments and other media activities.

Improved credibility and authority: The blogger or company might become recognised as a thought leader in their sector by regularly providing top-notch content. This may enhance their authority and credibility in the eyes of their audience, which may foster greater loyalty and trust.

Increased revenue: An online blog application can aid in generating income through advertising, sponsorships, affiliate marketing, or other monetization tactics by increasing website traffic and establishing a devoted audience.

A strong online presence, enhanced engagement and brand recognition, and potential money creation prospects are all possible outcomes of an online blog application.

Blogging applications is helping users in several ways, including:

Providing a platform for self-expression: Users can express themselves freely and creatively using my blogging website. Users are not subject to any limits or constraints while writing about their ideas, impressions, or opinions on a range of subjects.

Building a community: Users can connect with people who share their hobbies and passions through blogging software. Bloggers can foster a sense of support and community among their audience by growing a readership and following.

Sharing knowledge and information: Users have a platform to share their knowledge and experience with others through blogging software. Bloggers can inform their audience and impart knowledge by sharing information about a certain subject.

Building a personal brand: Users who utilise blogging tools can develop their personal brands and position themselves as authorities in their industry. Bloggers can become well-known and respected in their field by constantly delivering top-notch content.

Generating income: Applications for blogging can also assist users in making money through a variety of monetization techniques, including advertising, sponsorships, affiliate marketing, or the sale of digital goods or services.

Establishing themselves as thought leaders: Users who write blog articles can position themselves as thought leaders in their industry or specialty by imparting their knowledge and experience.

Networking with like-minded individuals: Applications for blogging can give users a platform to network and connect with others in their business or niche who share their interests.

Generating traffic to their website or business: By delivering up-to-date, pertinent content that is search engine-optimized, blogging programmes can assist in generating traffic for users' websites or enterprises.

Increasing brand awareness: Users can boost brand awareness and exposure among their target audience by regularly providing high-quality content.

Developing their personal brand: Applications for blogging can assist users in building their personal brands and showcasing their abilities to potential employers or customers.

Monetizing their blog: Applications for blogging can assist users in generating income from their blogs through advertising, sponsorships, affiliate marketing, and other methods.

Learning and staying up-to-date with industry trends: Users may keep up with the most recent trends and advancements in their profession by following and interacting with other bloggers and thought leaders in their sector.

How Security Management System is helping in providing security to our blogging application

A security management system can help provide security to your blogging application in several ways:

Authentication and access control: Making sure that only authorised users can access the blogging application is made easier by a security management system. Strong authentication systems like multi-factor authentication, password rules, and identity and access management (IAM) policies can be used to accomplish this.

Encryption and data protection: By utilising encryption and other data protection techniques like access restrictions, firewalls, and intrusion detection and prevention systems, a security management system can aid in the safety of sensitive data such as login passwords, user data, and blog content.

Monitoring and alerting: A security management system can assist in keeping track of any potential security flaws and risks in the blogging application. When a security event is discovered, it can send alerts and notifications to authorised individuals, enabling swift response and remediation.

Compliance and governance: The General Data Protection Regulation (GDPR) and the Payment Card business Data Security Standard (PCI DSS) are two examples of business and governmental regulations that can be met by a blogging application with the aid of a security management system. Additionally, it can offer user access and activity visibility and audits to support governance and compliance.

Incident response and recovery: In the event of a security breach or incident, a security management system can aid in establishing incident response and recovery procedures. Plans for backup and disaster recovery, incident response, and post-event assessments and analysis might all fall under this category.

Deploying an online blog application on AWS and implementing security tools can lead to several positive results:

Improved security: The online blog application can be protected from cyberthreats and vulnerabilities like DDoS assaults, malware, and data breaches by implementing security technologies on AWS. This can assist in ensuring the security and protection of the application and user data.

High availability: The global network of data centres that make up AWS's highly available architecture guarantees that customers can access the online blog application at all times. This may enhance user experience and cut down on downtime.

Scalability: Scalable infrastructure that can automatically adapt to changing traffic volumes and user demand is offered by AWS. This can make it easier for the online blog application to handle growing user populations and data quantities.

Cost savings: Pay-as-you-go pricing options provided by AWS can aid in lowering the up-front expenses related to building and maintaining an online blog application. Organisations may be able to cut costs and concentrate resources on other business-critical areas as a result.

Improved performance: The online blog application can profit from fast network connections, sophisticated caching techniques, and content delivery systems by utilising AWS infrastructure and services. This can lower latency and increase application performance.

After deploying our blogging application on AWS I have implemented the security features of AWS on our blogging website which results as follows -

AWS GuardDuty

The threat detection service AWS GuardDuty aids in defending our AWS infrastructure and workloads against security risks. Our AWS resources and services are continuously monitored by GuardDuty for malicious activity, unauthorised behaviour, and other potential security issues. Here are a few ways GuardDuty can assist our blog application that is running on AWS become more secure.

Continuous Monitoring: Our AWS environment, including our EC2 instances, S3 buckets, and VPCs, is continuously monitored by GuardDuty. Atypical API calls, unauthorised access attempts, and malicious activities are just a few examples of the various dangers and vulnerabilities that it automatically detects and warns us about.

Threat Detection: To recognise and rank security threats, GuardDuty combines machine learning and threat intelligence. Malware, trojans, and backdoors are just a few of the security issues it can identify, and it can also provide precise information on the type and severity of the threat.

Easy Integration: Other AWS services like CloudTrail, VPC Flow Logs, and AWS Security Hub are completely integrated with GuardDuty. As a result, integrating GuardDuty into your current security workflow and responding swiftly to security occurrences are made simple.

Cost-Effective: A cheap way to increase the security of our AWS environment is with GuardDuty. There are no setup fees or minimum charges; we simply pay for the resources that you utilise. As a result, using GuardDuty is simple to set up and expand as your security requirements change.

We can swiftly recognise and address possible security issues by utilising GuardDuty to keep an eye on our AWS environment, assisting in maintaining the safety and availability of our blog application. GuardDuty can assist us in enhancing our entire security posture, lowering the danger of data breaches and other security incidents, and preserving regulatory compliance.

AWS WAF (Web Application Firewall)

Online application firewall (AWS WAF) is a service that aids in defending online applications against widespread web exploits that could impair their availability, jeopardise their security, or use up excessive resources. AWS WAF can assist our blog application running on AWS in the following ways:

Protect against common web exploits: AWS WAF can shield our blog application against widespread web vulnerabilities including SQL injection and cross-site scripting (XSS) assaults that could result in data theft, blog defacement, or service interruption.

Block malicious traffic: The use of AWS WAF can lessen the burden on our application and stop dangerous requests from reaching your servers by blocking traffic from known malicious IP addresses or botnets.

Monitor traffic and create custom rules: We can track traffic to your blog application using AWS WAF, and we can develop unique rules to prevent particular requests or traffic patterns that are linked to attacks. This can add another layer of protection and lessen the likelihood of attacks.

Improve performance: AWS WAF can assist in enhancing the speed of our blog application and delivering a better user experience by preventing harmful traffic and lessening the burden on your application servers.

Simplify management: AWS WAF can be readily linked with other AWS services, such AWS

CloudFront and AWS Application Load Balancer, to streamline security administration and lower administrative burden for our blog application.

AWS Security Hub

The security solution known as AWS Security Hub offers a centralised view of security alerts and compliance status for various AWS accounts and services. AWS Security Hub can assist your blog application that is running on AWS in the following ways:

Security posture assessment: AWS Security Hub helps evaluate the security of your blog application by collecting and ranking security alerts from AWS services like Amazon GuardDuty, Amazon Inspector, and AWS Config. This can assist in locating potential security flaws and vulnerabilities in the AWS infrastructure supporting your blog application and offer recommendations for corrective measures.

Compliance monitoring: AWS Security Hub may assist in keeping track of how well our blog application complies with regulatory requirements like PCI DSS, HIPAA, and CIS AWS Foundations Benchmark. By doing this, you can make sure that the AWS infrastructure supporting your blog application complies with legal standards and stays out of trouble.

Integration with other AWS security services: For a complete security solution for your blog application, AWS Security Hub may be integrated with other AWS security services like AWS Identity and Access Management (IAM), AWS Key Management Service (KMS), and AWS Firewall Manager. This can make security administration easier to administer while lowering the possibility of setup problems and human error.

Customizable dashboards and alerts: To track security incidents and compliance status related to the AWS infrastructure supporting your blog application, AWS Security Hub offers customisable dashboards and notifications. This can assure continuing compliance and assist in swiftly identifying and handling possible security incidents.

AWS IAM

By controlling user access and permissions in our AWS account, AWS IAM (Identity and Access Management) can assist us in improving the security of our blogging website. We can manage who has access to our resources and what they can do by utilising AWS IAM.

In the context of a blogging website, AWS IAM can help us in the following ways:

Access Control: We can create unique user accounts with particular rights to access resources inside our AWS account using AWS IAM. As an illustration, we could create an IAM account for the blog's content manager who would only be able to read and update blog posts and not important configuration information like server access keys or database passwords.

Granular Permissions: AWS IAM enables us to assign each user granular permissions that restrict them access to only the particular resources they require to perform their duties. This lessens the possibility of unauthorised entry or unintentional modifications to crucial systems.

Multi-Factor Authentication (MFA): AWS IAM supports MFA, which increases the security of our account by forcing users to give a second factor of authentication in addition to their password, such as a code produced by a mobile app.

Audit Trail: Each user within our account has a complete audit history of all actions made thanks to AWS IAM. This enables us to keep an eye out for any unusual behaviour or possible security lapses.

Password Policies: By enforcing password complexity, length, and rotation, AWS IAM enables us to implement strong password policies and lower the chance of password-related security breaches.

Temporary Credentials: Users who want temporary access to our resources, like consultants or contractors, can be given temporary credentials using AWS IAM.

Federation: We may temporarily grant access to users outside of our AWS account, such partners or clients, thanks to AWS IAM's support for federated access.

Resource-Based Policies: Resource-based policies, which specify the rights for a resource, such as an S3 bucket or an EC2 instance, can be developed using AWS IAM.

Least Privilege: Only IAM users have access to the resources they require to do their jobs, which lowers the chance of unintentional or malicious security breaches. This is because AWS IAM adheres to the concept of least privilege.

Continuous Monitoring: To continuously monitor and identify any security vulnerabilities inside our AWS account, we can utilise AWS IAM in conjunction with other AWS security services like AWS CloudTrail and Amazon GuardDuty.

AWS CLOUDTRAIL

AWS CloudTrail can help us enhance the security of our blogging website:

Centralized Logging: We can get a centralised view of all AWS account activity, including API calls and events, with the help of AWS CloudTrail. This can assist us in identifying and looking into security incidents.

Compliance: We can satisfy compliance requirements and security standards with the help of the thorough audit records that AWS CloudTrail offers.

Forensic Analysis: With the help of AWS CloudTrail, we can look into and evaluate security incidents and take the necessary steps to stop them from happening again.

Governance: We may create and implement governance policies with the aid of AWS CloudTrail to make sure that all actions taken within our AWS account adhere to the policies and procedures of our company.

Access Control: We can monitor and manage user access to AWS resources using CloudTrail logs from AWS, which aids in preventing unauthorised access.

Threat Detection: We can identify potential dangers by keeping an eye out for odd or suspicious activities in our AWS account with the aid of AWS CloudTrail.

Risk Management: We can use the useful data that AWS CloudTrail gives us to find and control hazards in our AWS environment.

Troubleshooting: By examining logs and locating the issue's origin, we can use AWS CloudTrail to troubleshoot difficulties.

Security Analytics: To better understand security threats and strengthen our overall security posture, we can leverage AWS CloudTrail logs in conjunction with other AWS security solutions like Amazon GuardDuty and AWS Config.

Incident Response: We can swiftly detect and respond to security incidents with the aid of AWS CloudTrail, reducing the impact on our company's operations.

Implementing different AWS security elements in a blogging website might have a number of advantages for both the website's owners and users. First off, we can make sure that only individuals with permission to access the website and its resources do so by using AWS IAM. This aids in preventing data breaches and unauthorised access, both of which could be detrimental to the website and its users. The ability to grant each user only the access to the particular resources they require to perform their duties is another feature of AWS IAM. This lessens the possibility of unintentional alterations being made to crucial systems.

Secondly, AWS CloudTrail can offer a thorough audit trace of every action and event that takes place within the AWS environment. This makes it possible for us to keep an eye on every user activity and spot any unusual behaviour that might pose a security risk. AWS CloudTrail can be utilised in the event of a security breach to swiftly locate the attack's origin and assist in minimising any damage.

Thirdly, adopting Amazon S3 for sensitive data storage may guarantee that data is stored securely, redundantly, with built-in encryption and access controls, including user information and blog material. This makes sure that users always have access to data and helps to prevent data breaches, loss, or corruption of data.

Fourthly, with built-in DDoS protection and caching features, we can use Amazon CloudFront as a content delivery network (CDN) to make sure that website content is delivered to users swiftly and safely. This aids in preventing data loss from cyberattacks and website downtime.

Fifthly, we can defend the website against widespread web-based assaults like SQL injection and cross-site scripting by using AWS WAF (Web Application Firewall). By doing this, data breaches and website outages that could be harmful to both the website and its visitors arereduced.

Sixth, we can proactively monitor the AWS environment for potential risks and promptly address any events by utilising AWS GuardDuty. By doing so, security incidents and other security-related harm are reduced or prevented.

Finally, by using AWS Backup and AWS Disaster Recovery, we can establish frequent backups and disaster recovery plans to guarantee that website data is always accessible to users, even in the case of a disaster or data loss. This promotes business continuity and lessens the effects of security incidents.

I have decided to use MongoDB as the main database for our website for my blogging platform that is set up on the public cloud AWS. Our website would benefit greatly from MongoDB, a well-liked NoSQL database with strong scalability and flexibility. Due to its ability to manage enormous amounts of data, it is appropriate for blogging websites that need to store and retrieve large amounts of content.

Furthermore, MongoDB has sophisticated security capabilities that support our security objectives. It provides access control, auditing, and data encryption for both static and moving data. This enables us to add a solid security approach to the security solutions offered by AWS for our database layer.

AWS Elastic Beanstalk and other AWS services are seamlessly integrated with MongoDB, making it easier to deploy and manage our application. We can improve the overall security of our website by utilising AWS security capabilities like AWS IAM and AWS Security Hub thanks to this integration.

In my blogging website, I can give users a place to share their thoughts, theories, and viewpoints on a range of subjects. An ideal way to do this now that the internet has created new platforms for people to share their thoughts with a worldwide audience is through a blogging website. Users can receive visibility for their work and reach a larger audience by creating and publishing articles on our platform. This may result in more prospects for collaboration with other bloggers or experts in their sector as well as a boost in credibility.

A blogging website can also be a cathartic place to write. Writing about one's challenges, experiences, or ideas can be a therapeutic technique to work through one's feelings and thoughts. Users can share their experiences with others who might be going through similar circumstances by publishing their work on our platform. For someone who might otherwise feel alone in their challenges, this can foster a sense of camaraderie and support that can be important.

Blogging can help one's career, in addition to fostering community and personal growth. Blogging professionals can position themselves as authorities in their industry by developing their personal brands and audiences. Speaking engagements, independent work, and even job offers may result from this. Additionally, bloggers can enhance their writing abilities by consistently creating high-quality content, which is advantageous in many businesses.

Additionally, some users of blogging may use it as a means of revenue. Bloggers can generate a consistent flow of passive money by monetizing their blogs with advertising, affiliate marketing, or sponsored content. A career in blogging, however, necessitates a significant amount of effort, commitment, and regularity. A blogger may need some time before they can monetize their blog and generate a sizable income.

My blogging site can be used as a platform for advocacy and social activism. Users can create change by writing about social justice topics and increasing awareness. Bloggers can aid in changing society narratives and fostering empathy and understanding by amplifying marginalised voices and sharing the experiences of underrepresented communities. These voices can be heard and amplified in a safe area on our website.

PUBLIC CLOUD DEPLOYEMENT

For the Public cloud deployment for my blogging website I have used AWS S3 and AWS EC2 with Putty.

The static material of the blogging website, such as photos and JavaScript files, is first stored and served using Amazon S3. This enables us to transfer the storage and distribution of this content to the cloud, which can lessen the stress on the EC2 instances that are delivering the dynamic content.

Second, I've used EC2 instances to run the web server and application server programmes necessary to deliver the dynamic content of the blogging website. The Elastic Load Balancer could be used to distribute traffic among the instances, and we could deploy these instances in an auto-scaling group to ensure that we can handle spikes in demand.

An object storage service called Amazon Simple Storage Service (S3) provides performance, security, and scalability that are unmatched in the market. It enables online storage and retrieval of files of any size. A online service called Amazon Elastic Compute Cloud (EC2) offers safe, scalable compute capacity in the cloud. For developers, it is intended to make web-scale cloud computing simpler.

To deploy a blogging website on AWS S3 and EC2, we'll need to follow these steps:

- Create an Amazon S3 bucket: Static files including HTML, CSS, JavaScript, and pictures will be stored using S3. In the S3 console, we'll build a bucket and add our static files to it. The bucket will then be made available to everyone so they may view our website.

- Configure bucket properties: To enable hosting for static websites, we will specify the bucket properties. As a result, we won't require a web server for serving our static files.

- Create an Amazon EC2 instance: Our web server will be run through EC2. In the EC2 console, we'll create an instance, choose an Amazon Machine Image (AMI), and set up the instance's storage options, security group, and instance type.

- Connect to the EC2 instance: When the instance is up and running, we'll establish an SSH connection. To connect to an instance, we'll need to know its public IP address or DNS name.

- Install a web server: On the EC2 instance, we'll install a web server like Apache or Nginx. We'll be able to deliver dynamic material like blog articles and comments thanks to this.

- Configure the web server: We'll set up the web server to deliver dynamic material from the web server and proxy requests for static files to S3. If we wish to secure our website, we'll also set up the web server to manage SSL/TLS certificates.

- Point our domain name to the EC2 instance: In order for users to access our website using our domain name, we will finally point our domain name to the public IP address or DNS name of the EC2 instance.

For the deployment of our blogging website, I have opted to use Amazon S3 (Simple Storage Service) and Amazon EC2 (Elastic Compute Cloud). We came to this conclusion for a number of reasons, which I will go into more detail about in the sentences that follow.

In the first place, Amazon S3 offers a dependable and highly scalable object storage service. This entails that we can reliably and readily store and access any volume of data from any location on the internet at any time. This makes it the perfect option for hosting the static assets for our website, such as the HTML, CSS, and JavaScript files.

Secondly, Amazon EC2 offers a scalable and adaptable computing environment that enables us to start and manage virtual computers (called instances) in accordance with our requirements. Depending on our workload and budget, we can select from a variety of instance types, operating systems, and software configurations. Given this, operating our web server, database server, and application server on it is the best option.

Thirdly, a variety of cloud computing services are available through the Amazon Web Services (AWS) ecosystem, which includes both Amazon S3 and EC2. Thus, we can link Amazon Web Services (AWS) services like Amazon Route 53 (DNS), Amazon CloudFront (CDN), Amazon RDS (relational database), and Amazon Elastic Load Balancer (ELB) with our S3 and EC2 instances. This enables us to create a scalable and highly available system.

Fourthly, we can deploy our blogging website on Amazon S3 and EC2 at a reasonable price. Without making any upfront or long-term obligations, we only pay for the storage space and data transport that we really utilise with Amazon S3. With Amazon EC2, we make no upfront or long-term obligations and only pay for the computing resources that we actually use, on an hourly or secondly basis. We can easily start small and scale up as our website expands thanks to this.

Fifth, high-level security and compliance measures are offered by Amazon S3 and EC2, which are essential for our blogging website. Using tools like bucket policies, ACLs, and IAM roles, we can restrict who has access to our data with Amazon S3. With Amazon EC2, we have access to a number of security tools, like encryption, IAM roles, and security groups, to protect our instances. By doing this, we can guarantee that our website is safe from numerous online threats.

Sixth, Amazon S3 and EC2 offer simple-to-use APIs and tools that let us administer and keep an eye on our website. We can upload, download, and manage our items using the AWS Management Console, AWS CLI, or AWS SDKs with Amazon S3. We can start, stop, and monitor our instances with Amazon EC2 using the AWS Management Console, AWS CLI, or AWS SDKs. We can now easily automate our deployment and administration processes thanks to this.

Last but not least, Amazon S3 and EC2 have a global footprint, allowing us to deploy our website closer to our users in any part of the world. Using Amazon S3 Transfer Acceleration or Amazon S3 Replication, we can replicate our objects across several locations with Amazon S3. Using Amazon EC2 Auto Scaling or Amazon EC2 Placement Groups, we can start instances in any region. No matter where our users are situated, our website will always be quick and responsive thanks to this.

The reason behind choosing Putty with AWS S3 and EC2 for the public cloud deployment is -

To start with, Secure Shell (SSH) connections can be made with remote servers using PuTTY, a free and open-source terminal emulator. In this scenario, connecting to an EC2 instance on AWS, where the blogging website will be installed, is possible using PuTTY.

Second, static files for the blogging website, like HTML, CSS, and JavaScript files, can be kept in Amazon S3. Using the AWS Management Console or the AWS Command Line Interface (CLI) via PuTTY, these files can be uploaded to an S3 bucket. These files can be safely transferred to the S3 bucket using the SFTP or SCP protocols using PuTTY.

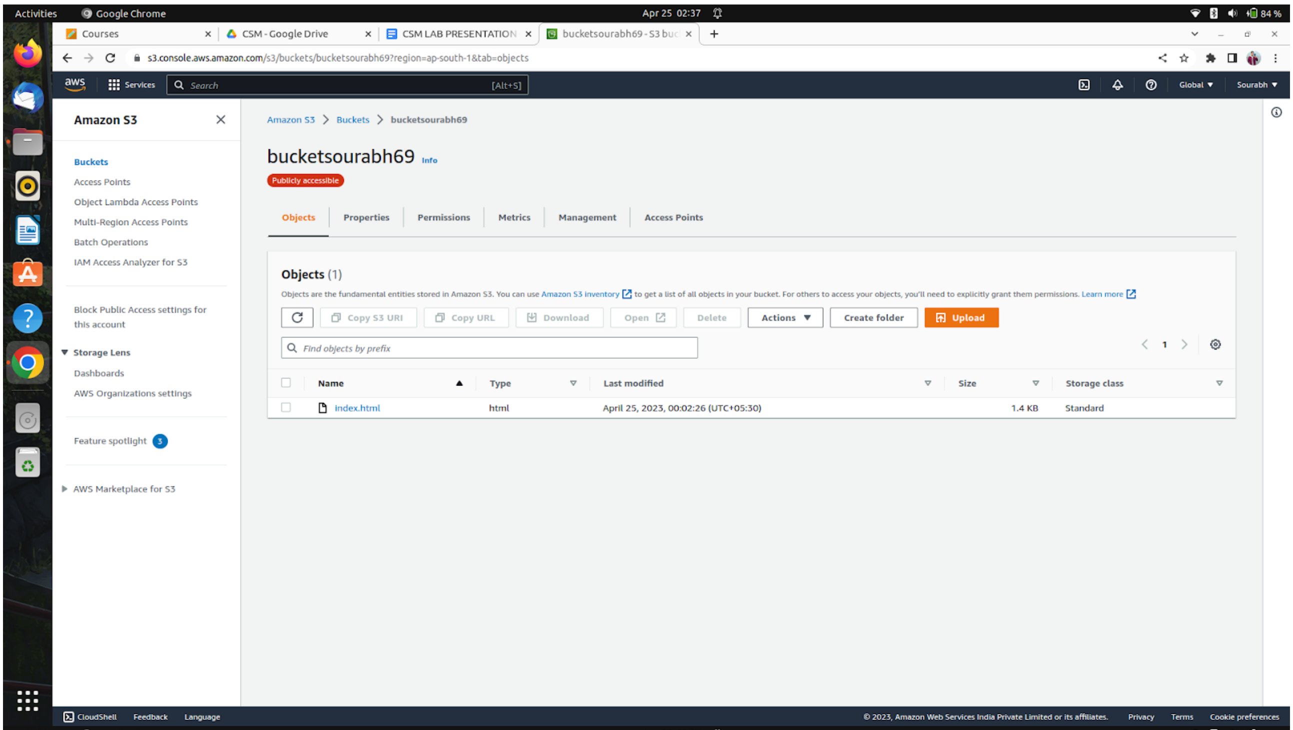
Thirdly, you can login to the EC2 instance hosting the blogging website using PuTTY to install any other software packages and requirements, like an Apache or Nginx web server. PuTTY can be used to setup the web server and deploy the blogging website code after the web server has been installed.

Fourthly, the EC2 instance may be managed and watched over via PuTTY. For instance, PuTTY can be used to verify the web server's status or restart it if necessary. Additionally, PuTTY may be used to inspect logs and track EC2 instance performance metrics using programmes like top, htop, or the AWS Management Console.

Fifthly, by defining permissions and creating new user accounts, PuTTY may be used to control access to the EC2 instance. Users can be added to the EC2 instance using programmes like adduser or useradd, and SSH keys can be generated and managed using PuTTY.

Sixth, the blogging website and its accompanying data may be backed up and managed using PuTTY. Mysqldump, tar, and PuTTY can be used to produce backups, which can then be safely transmitted to an S3 bucket.

Lastly, PuTTY can be used to resolve any problems that may come up while setting up or maintaining the blogging website on AWS. With the help of PuTTY, you may connect to the EC2 instance, look into any faults or problems, and then take any necessary corrective action.



Activities
Google Chrome
Apr 25 02:37
84 %
Courses
CSM - Google Drive
CSM LAB PRESENTATION
bucketsourabh69 - S3 buc
s3.console.aws.amazon.com/s3/buckets/bucketsourabh69?region=ap-south-1&tab=objects
aws
Services
Search
[Alt+S]
Global
Sourabh
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3 > Buckets > bucketsourabh69

bucketsourabh69 Info

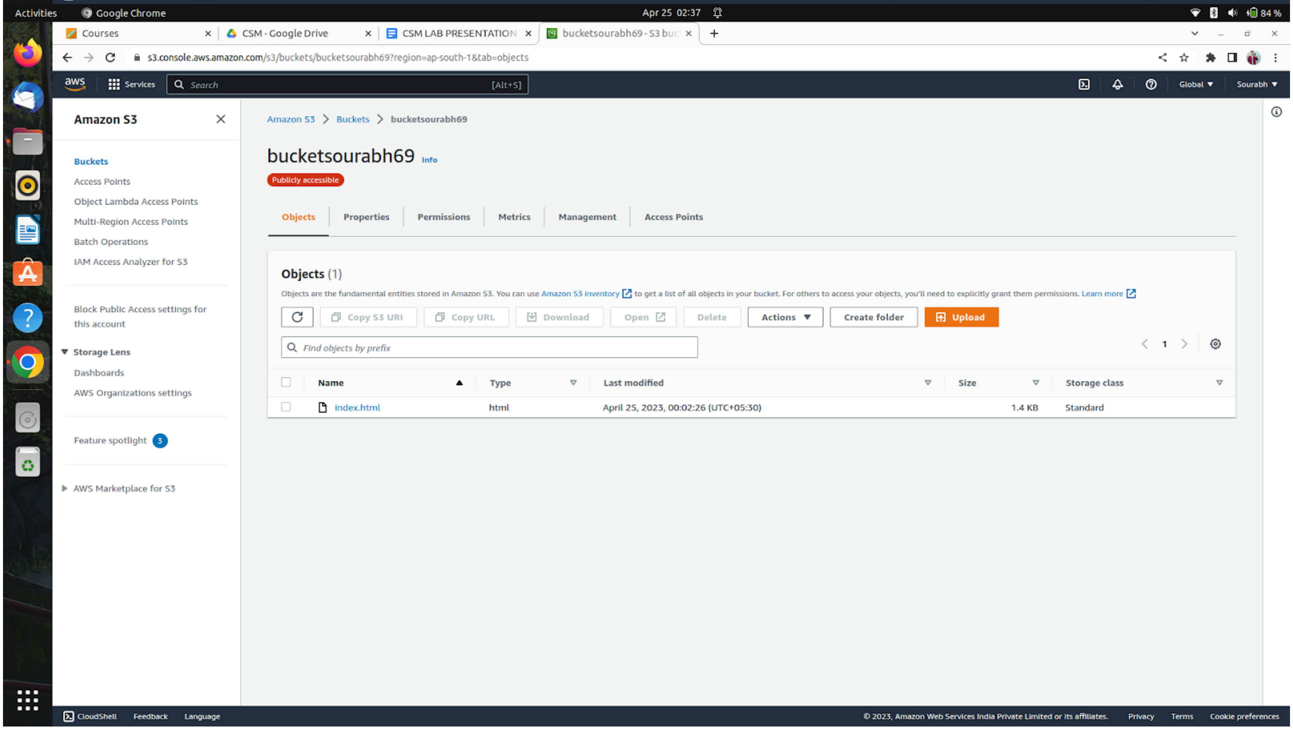
Publicly accessible

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name	Type	Last modified	Size	Storage class
□	index.html	html	April 25, 2023, 00:02:26 (UTC+05:30)	1.4 KB	Standard

CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences



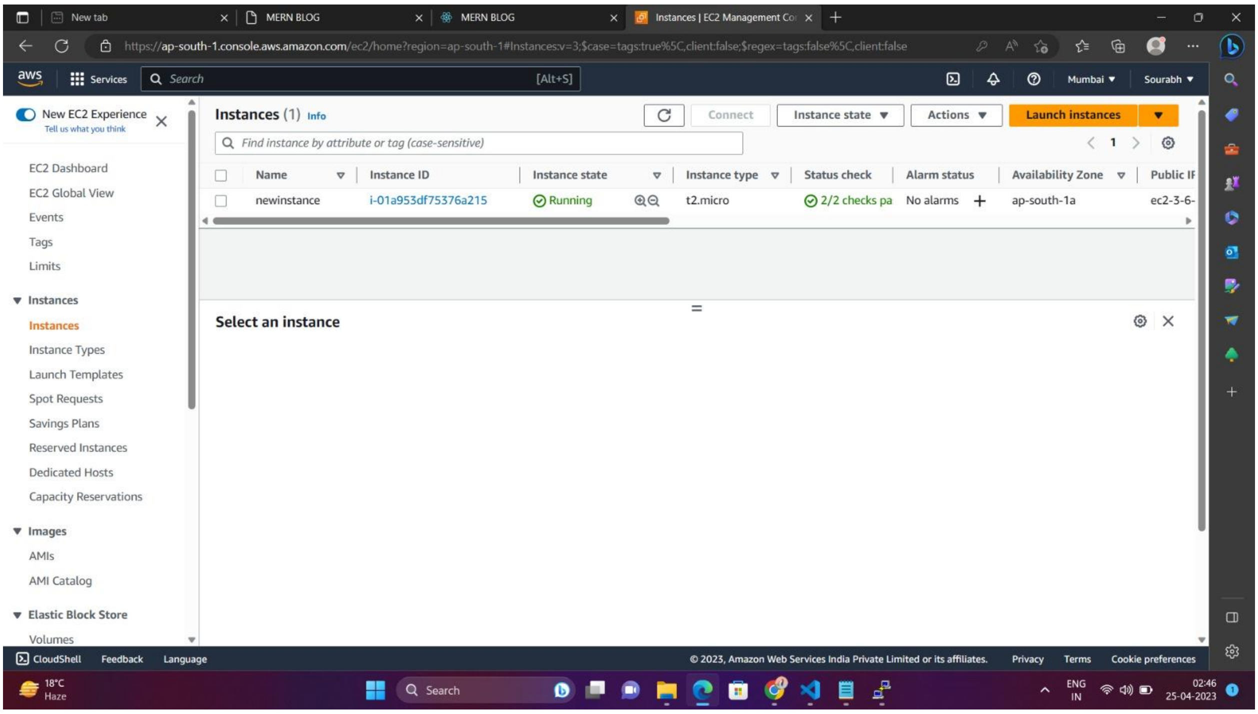
bucketsourabh69 Info

Publicly accessible

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name	Type	Last modified	Size	Storage class
□	index.html	html	April 25, 2023, 00:02:26 (UTC+05:30)	1.4 KB	Standard

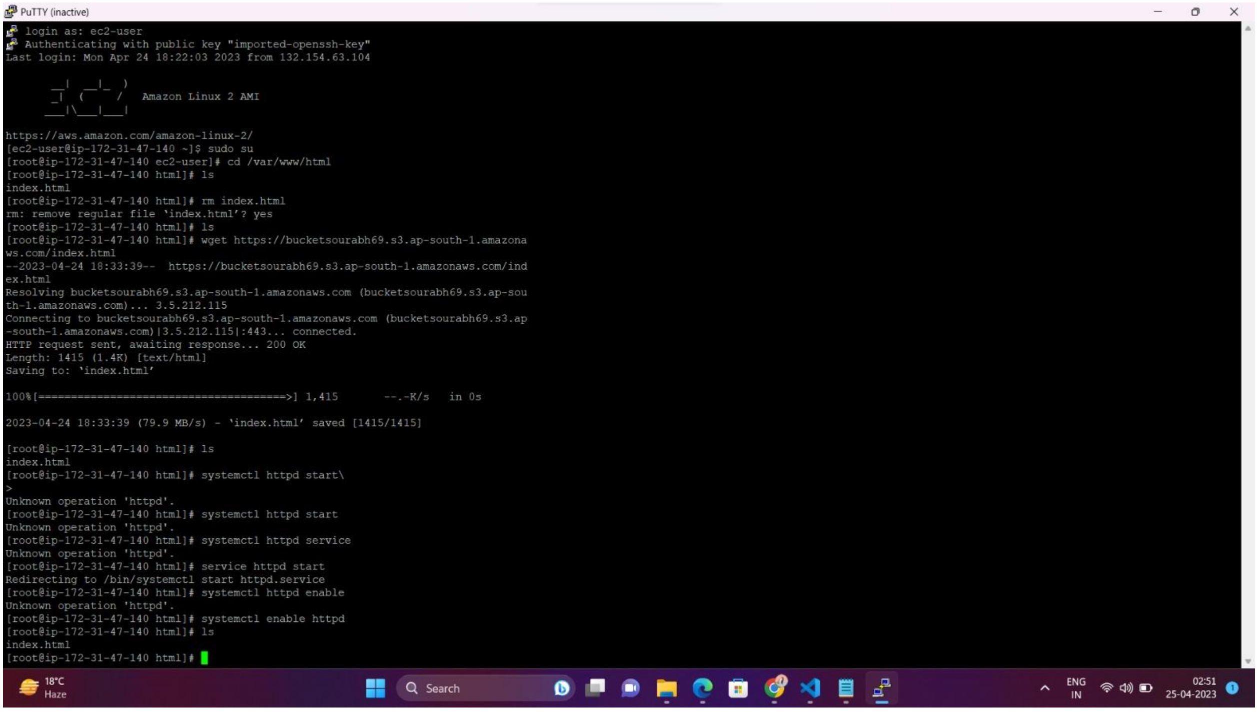


https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Instances:v=3;$case=tags:true%5C,client:false;$regex=tags:false%5C,client:false

Instances (1) Info

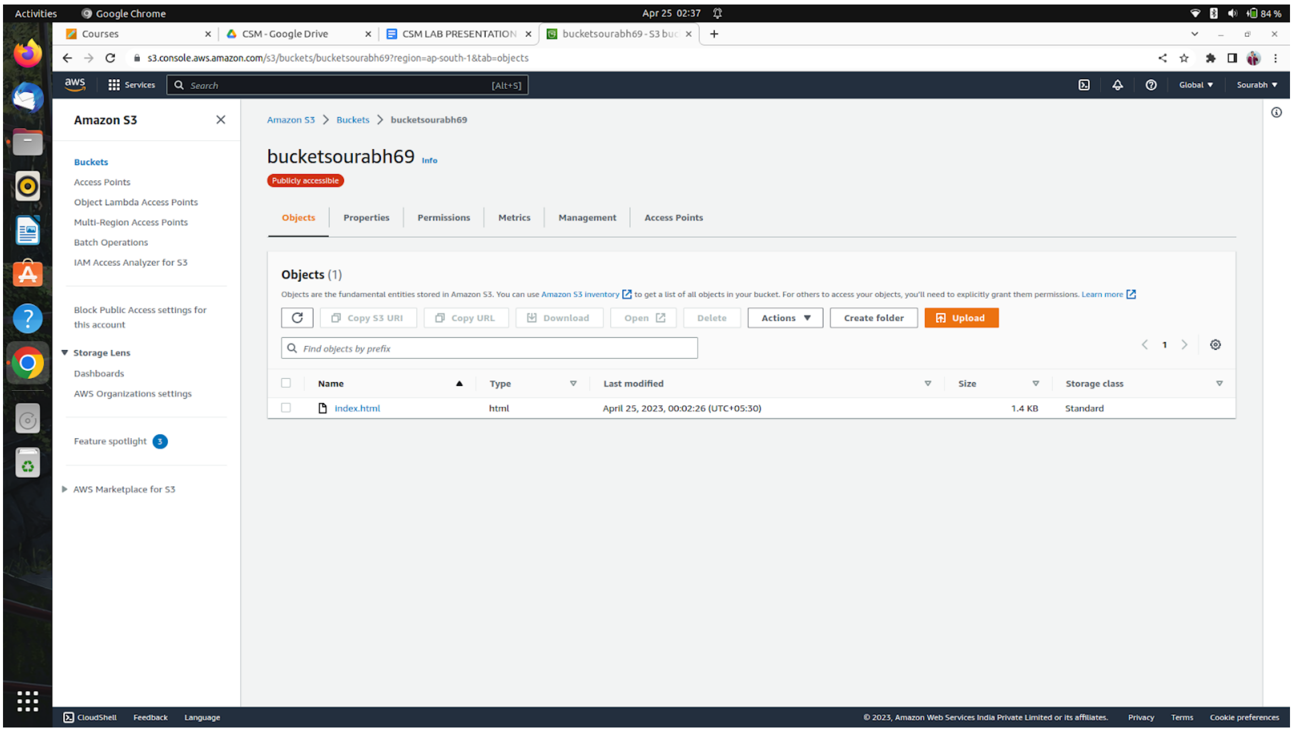
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IF
newinstance	i-01a953df75376a215	Running	t2.micro	2/2 checks pa	No alarms	ap-south-1a	ec2-3-6-

Select an instance



```
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Last login: Mon Apr 24 18:22:03 2023 from 132.154.63.104

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-47-140 ~]$ sudo su
[root@ip-172-31-47-140 ec2-user]# cd /var/www/html
[root@ip-172-31-47-140 html]# ls
index.html
[root@ip-172-31-47-140 html]# rm index.html
rm: remove regular file ‘index.html’? yes
[root@ip-172-31-47-140 html]# ls
[root@ip-172-31-47-140 html]# wget https://bucketsourabh69.s3.ap-south-1.amazona
ws.com/index.html
--2023-04-24 18:33:39--  https://bucketsourabh69.s3.ap-south-1.amazonaws.com/ind
ex.html
Resolving bucketsourabh69.s3.ap-south-1.amazonaws.com (bucketsourabh69.s3.ap-sou
th-1.amazonaws.com)... 3.5.212.115
Connecting to bucketsourabh69.s3.ap-south-1.amazonaws.com (bucketsourabh69.s3.ap
-south-1.amazonaws.com)|3.5.212.115|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1415 (1.4K) [text/html]
Saving to: ‘index.html’

100%[=====================================>] 1,415       --.-K/s   in 0s

2023-04-24 18:33:39 (79.9 MB/s) - ‘index.html’ saved [1415/1415]

[root@ip-172-31-47-140 html]# ls
index.html
[root@ip-172-31-47-140 html]# systemctl httpd start\
>
Unknown operation 'httpd'.
[root@ip-172-31-47-140 html]# systemctl httpd start
Unknown operation 'httpd'.
[root@ip-172-31-47-140 html]# systemctl httpd service
Unknown operation 'httpd'.
[root@ip-172-31-47-140 html]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@ip-172-31-47-140 html]# systemctl httpd enable
Unknown operation 'httpd'.
[root@ip-172-31-47-140 html]# systemctl enable httpd
[root@ip-172-31-47-140 html]# ls
index.html
[root@ip-172-31-47-140 html]#
```

SCREENSHOTS



Activities
Google Chrome
Apr 25 02:37
Courses
CSM - Google Drive
CSM LAB PRESENTATION
bucketsourabh69 - S3 buc
s3.console.aws.amazon.com/s3/buckets/bucketsourabh69?region=ap-south-1&tab=objects
Services
Search
[Alt+S]
Global
Sourabh
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3 > Buckets > bucketsourabh69

bucketsourabh69 Info

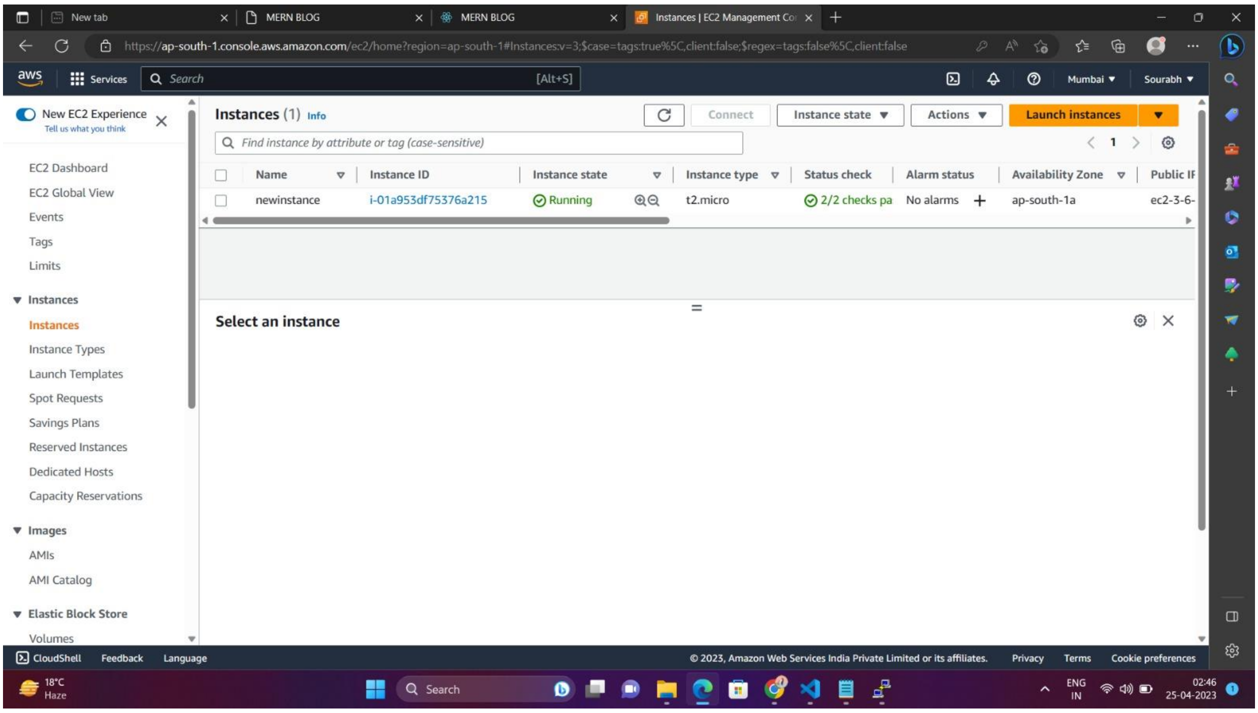
Publicly accessible

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

	Name	Type	Last modified	Size	Storage class
□	index.html	html	April 25, 2023, 00:02:26 (UTC+05:30)	1.4 KB	Standard

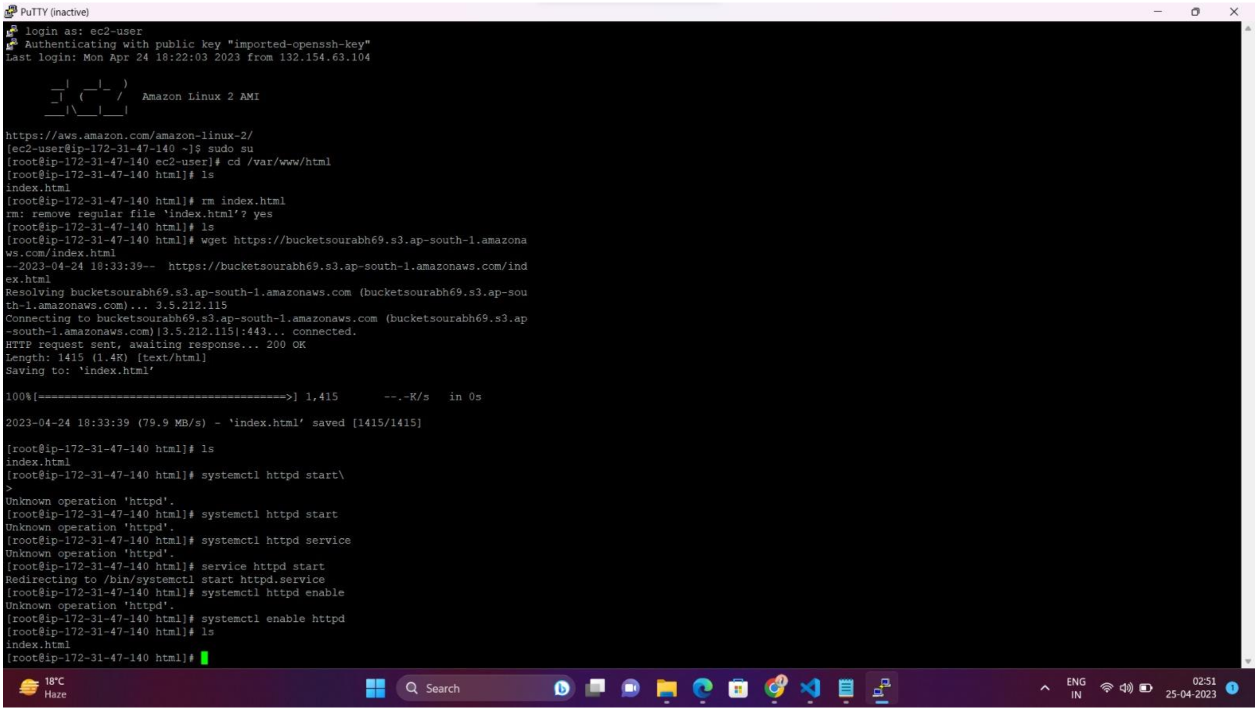
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences



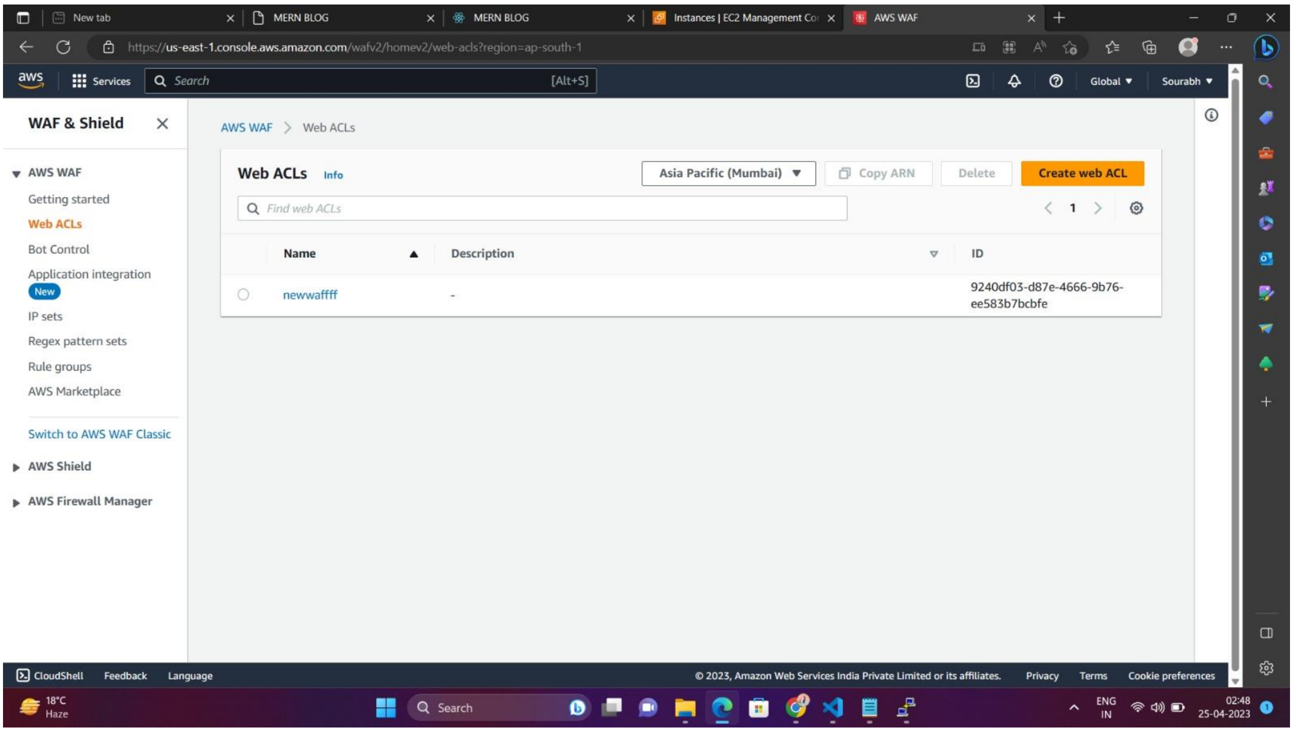
Instances (1) Info

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
□	newinstance	i-01a953df75376a215	Running	t2.micro	2/2 checks pa	No alarms	ap-south-1a	ec2-3-6-

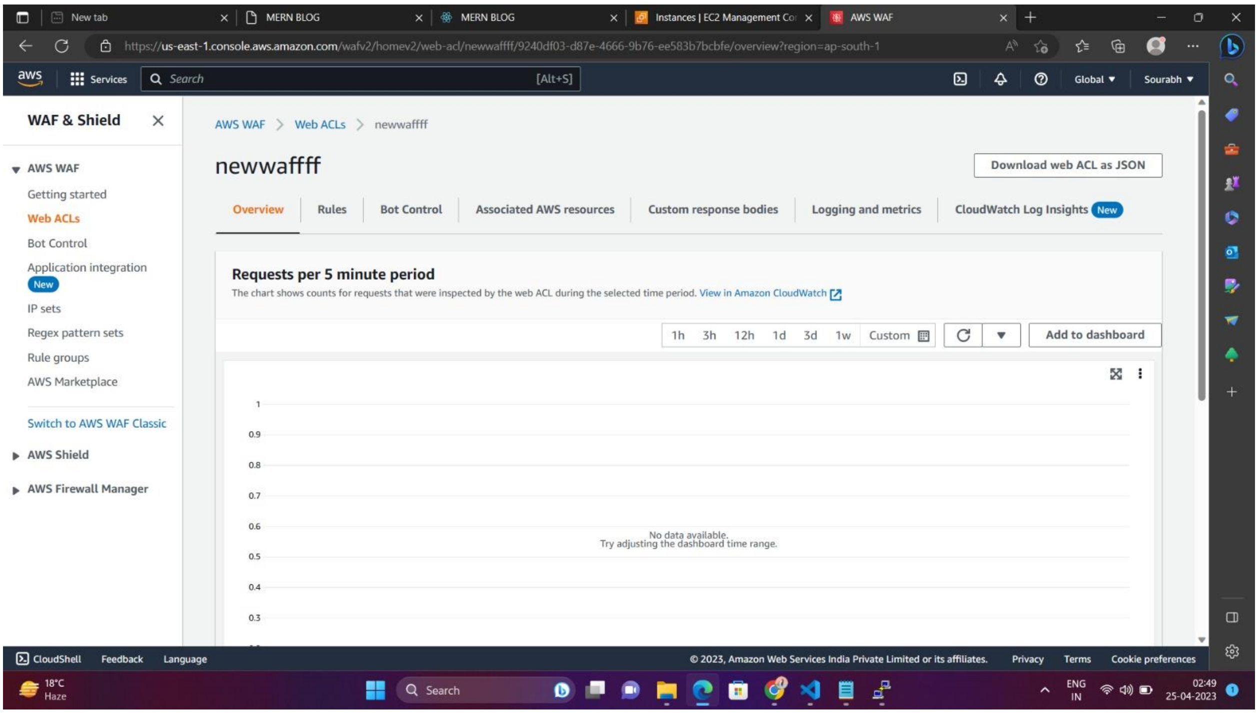
Select an instance



```
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Last login: Mon Apr 24 18:22:03 2023 from 132.154.63.104

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-47-140 ~]$ sudo su
[root@ip-172-31-47-140 ec2-user]# cd /var/www/html
[root@ip-172-31-47-140 html]# ls
index.html
[root@ip-172-31-47-140 html]# rm index.html
rm: remove regular file ‘index.html’? yes
[root@ip-172-31-47-140 html]# ls
[root@ip-172-31-47-140 html]# wget https://bucketsourabh69.s3.ap-south-1.amazona
ws.com/index.html
--2023-04-24 18:33:39--  https://bucketsourabh69.s3.ap-south-1.amazonaws.com/ind
ex.html
Resolving bucketsourabh69.s3.ap-south-1.amazonaws.com (bucketsourabh69.s3.ap-sou
th-1.amazonaws.com)... 3.5.212.115
Connecting to bucketsourabh69.s3.ap-south-1.amazonaws.com (bucketsourabh69.s3.ap
-south-1.amazonaws.com)|3.5.212.115|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1415 (1.4K) [text/html]
Saving to: ‘index.html’

100%[======================================>] 1,415       --.-K/s   in 0s

2023-04-24 18:33:39 (79.9 MB/s) - ‘index.html’ saved [1415/1415]

[root@ip-172-31-47-140 html]# ls
index.html
[root@ip-172-31-47-140 html]# systemctl httpd start\
>
Unknown operation 'httpd'.
[root@ip-172-31-47-140 html]# systemctl httpd start
Unknown operation 'httpd'.
[root@ip-172-31-47-140 html]# systemctl httpd service
Unknown operation 'httpd'.
[root@ip-172-31-47-140 html]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@ip-172-31-47-140 html]# systemctl httpd enable
Unknown operation 'httpd'.
[root@ip-172-31-47-140 html]# systemctl enable httpd
[root@ip-172-31-47-140 html]# ls
index.html
[root@ip-172-31-47-140 html]#
```



	Name ▲	Description	ID
○	newwaffff	-	9240df03-d87e-4666-9b76-ee583b7bcbfe

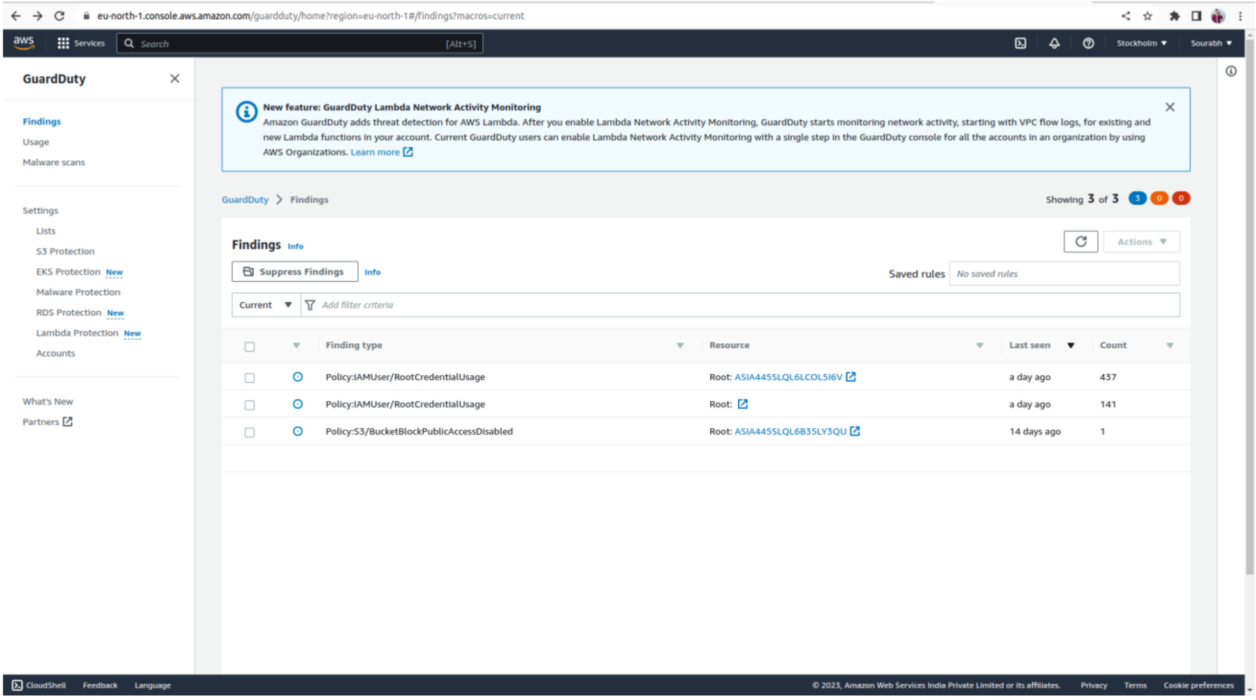

AWS WAF
https://us-east-1.console.aws.amazon.com/wafv2/homev2/web-acl/newwaffff/9240df03-d87e-4666-9b76-ee583b7bcbfe/overview?region=ap-south-1
WAF & Shield
AWS WAF
Getting started
Web ACLs
Bot Control
Application integration New
IP sets
Regex pattern sets
Rule groups
AWS Marketplace
Switch to AWS WAF Classic
AWS Shield
AWS Firewall Manager
AWS WAF > Web ACLs > newwaffff
Download web ACL as JSON
Overview
Rules
Bot Control
Associated AWS resources
Custom response bodies
Logging and metrics
CloudWatch Log Insights New
1h 3h 12h 1d 3d 1w Custom
Add to dashboard
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
© 2023, Amazon Web Services India Private Limited or its affiliates.
25-04-2023

newwaffff

Requests per 5 minute period

The chart shows counts for requests that were inspected by the web ACL during the selected time period. View in Amazon CloudWatch

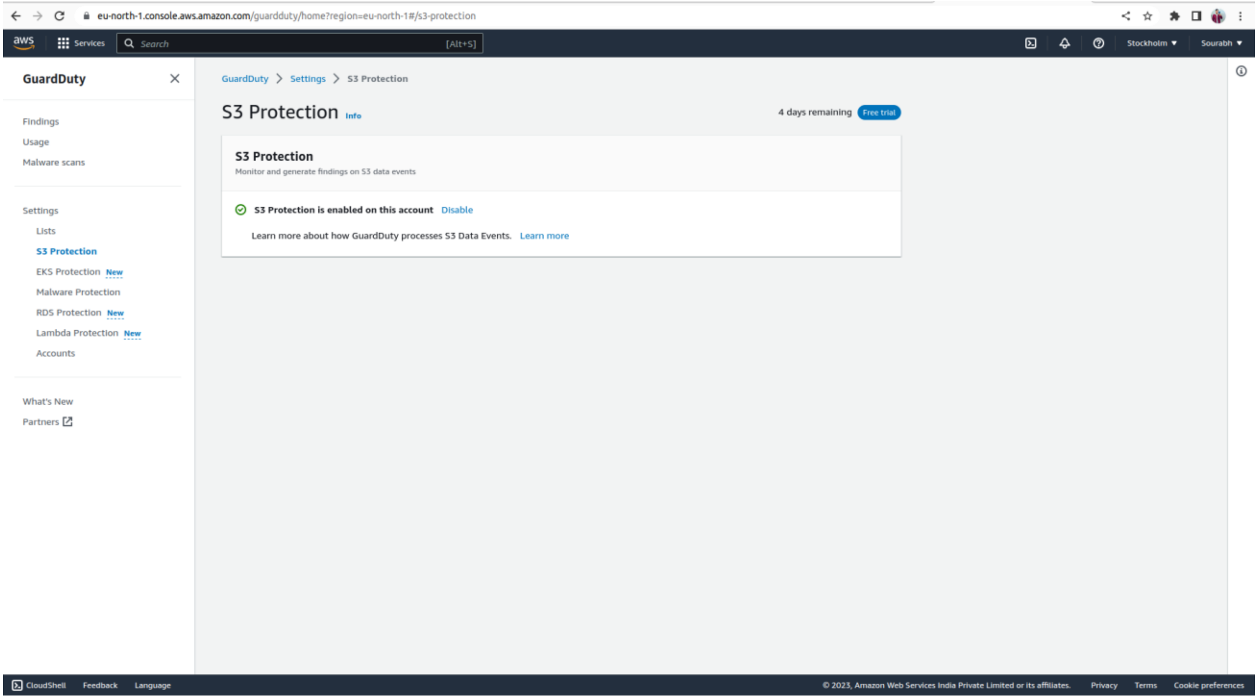
No data available.
Try adjusting the dashboard time range.



New feature: GuardDuty Lambda Network Activity Monitoring
Amazon GuardDuty adds threat detection for AWS Lambda. After you enable Lambda Network Activity Monitoring, GuardDuty starts monitoring network activity, starting with VPC flow logs, for existing and new Lambda functions in your account. Current GuardDuty users can enable Lambda Network Activity Monitoring with a single step in the GuardDuty console for all the accounts in an organization by using AWS Organizations. Learn more

Findings

Finding type	Resource	Last seen	Count
Policy:IAMUser/RootCredentialUsage	Root: ASIA445SLQL6LCOL5I6V	a day ago	437
Policy:IAMUser/RootCredentialUsage	Root:	a day ago	141
Policy:S3/BucketBlockPublicAccessDisabled	Root: ASIA445SLQL6B35LY3QU	14 days ago	1



S3 Protection Info

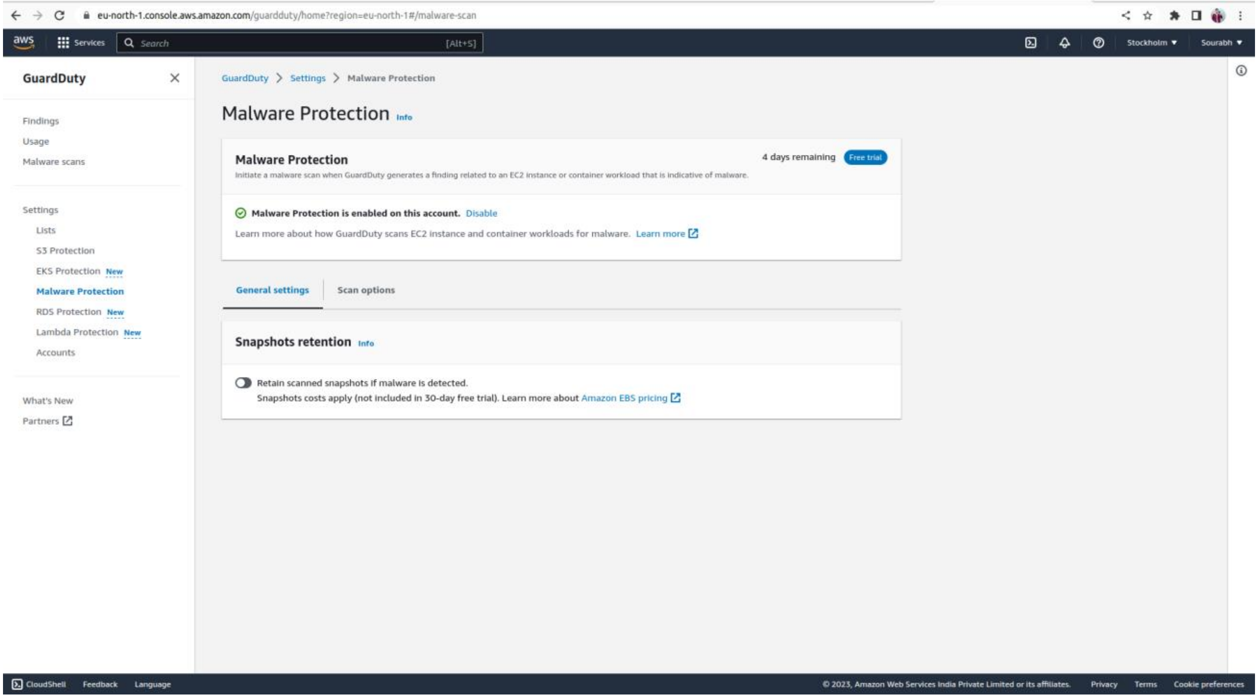
4 days remaining Free trial

S3 Protection

Monitor and generate findings on S3 data events

S3 Protection is enabled on this account Disable

Learn more about how GuardDuty processes S3 Data Events. Learn more



Malware Protection Info

Malware Protection

4 days remaining Free trial

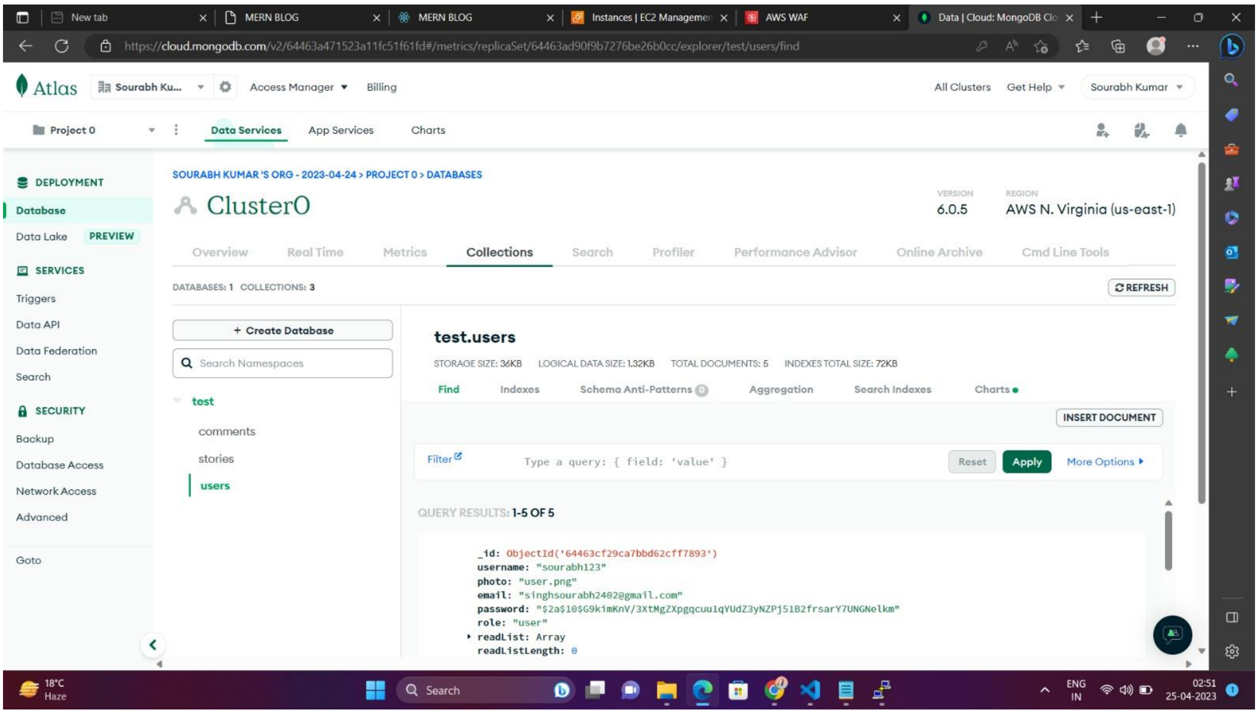
Initiate a malware scan when GuardDuty generates a finding related to an EC2 instance or container workload that is indicative of malware.

Malware Protection is enabled on this account. Disable

Learn more about how GuardDuty scans EC2 instance and container workloads for malware. Learn more

Snapshots retention Info

○ Retain scanned snapshots if malware is detected.
Snapshots costs apply (not included in 30-day free trial). Learn more about Amazon EBS pricing



https://cloud.mongodb.com/v2/64463a471523a11fc51f61fd#/metrics/replicaSet/64463ad90f9b7276be26b0cc/explorer/test/users/find

SOURABH KUMAR 'S ORG - 2023-04-24 > PROJECT 0 > DATABASES

Cluster0

VERSION 6.0.5

REGION AWS N. Virginia (us-east-1)

DATABASES: 1 COLLECTIONS: 3

test.users

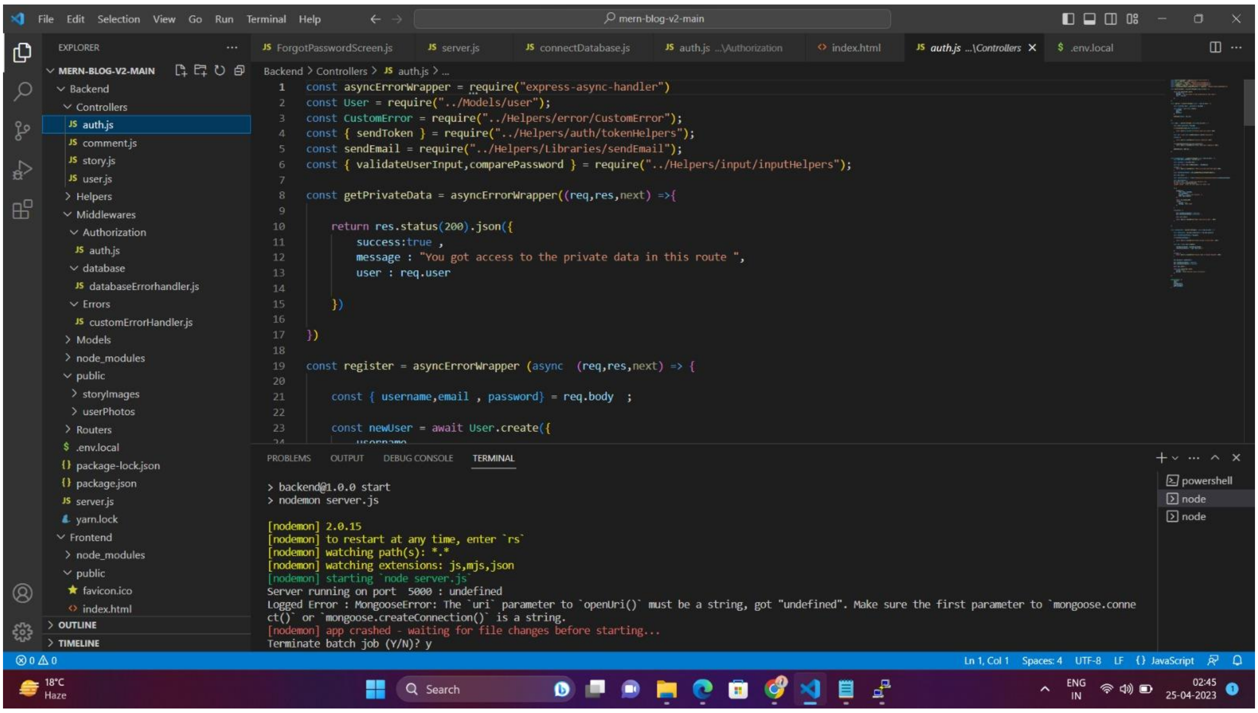
STORAGE SIZE: 36KB LOGICAL DATA SIZE: 1.32KB TOTAL DOCUMENTS: 5 INDEXES TOTAL SIZE: 72KB

Type a query: { field: 'value' }

QUERY RESULTS: 1-5 OF 5

```
_id: ObjectId('64463cf29ca7bbd62cff7893')
username: "sourabh123"
photo: "user.png"
email: "singhsourabh2402@gmail.com"
password: "$2a$10$G9kimKnV/3XtMgZXpgqcuulqYUdZ3yNZPj51B2frsarY7UNGNelkm"
role: "user"
readList: Array
readListLength: 0
```

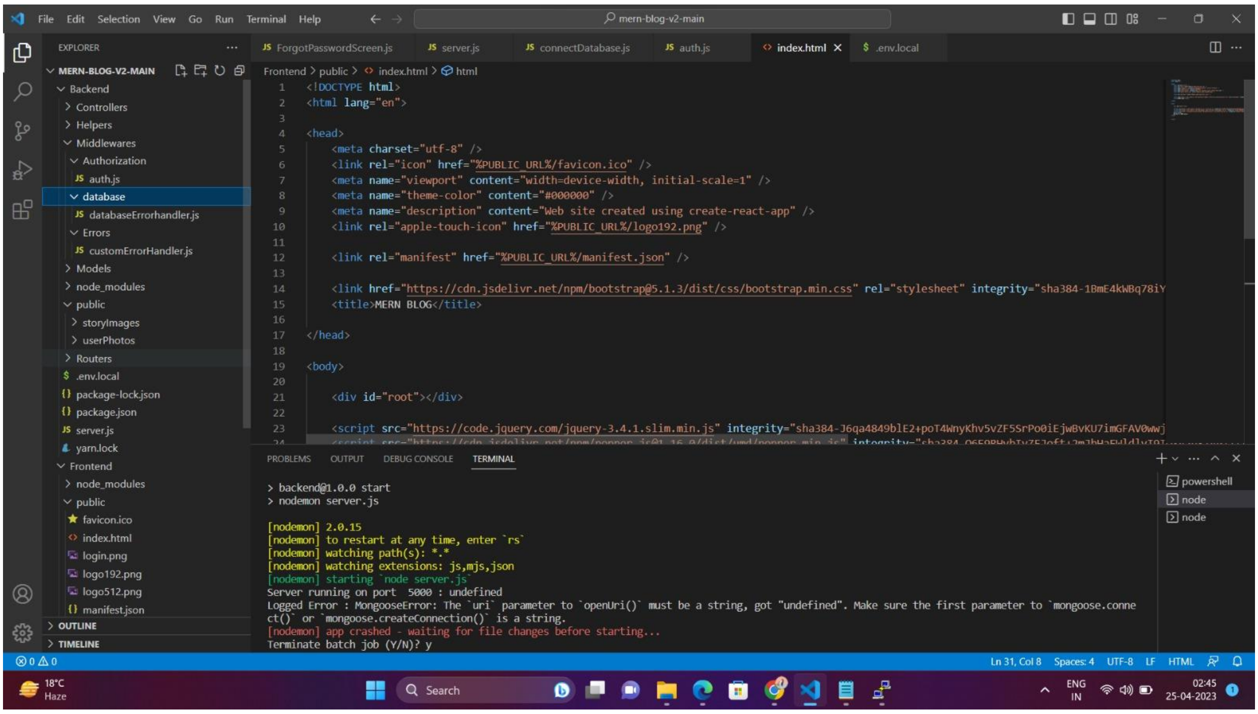
18°C Haze 02:51 25-04-2023



```
const asyncErrorWrapper = require("express-async-handler")
const User = require("../Models/user");
const CustomError = require("../Helpers/error/CustomError");
const { sendToken } = require("../Helpers/auth/tokenHelpers");
const sendEmail = require("../Helpers/Libraries/sendEmail");
const { validateUserInput,comparePassword } = require("../Helpers/input/inputHelpers");

const getPrivateData = asyncErrorWrapper((req,res,next) =>{

    return res.status(200).json({
        success:true ,
        message : "You got access to the private data in this route ",
        user : req.user

    })

})

const register = asyncErrorWrapper (async  (req,res,next) => {

    const { username,email , password} = req.body  ;

    const newUser = await User.create({
```

```
> backend@1.0.0 start
> nodemon server.js

[nodemon] 2.0.15
[nodemon] to restart at any time, enter `rs`
[nodemon] watching path(s): *.*
[nodemon] watching extensions: js,mjs,json
[nodemon] starting `node server.js`
Server running on port  5000 : undefined
Logged Error : MongooseError: The `uri` parameter to `openUri()` must be a string, got "undefined". Make sure the first parameter to `mongoose.conne
ct()` or `mongoose.createConnection()` is a string.
[nodemon] app crashed - waiting for file changes before starting...
Terminate batch job (Y/N)? y
```

18°C Haze 02:45 25-04-2023



```html
<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="utf-8" />
    <link rel="icon" href="%PUBLIC_URL%/favicon.ico" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <meta name="theme-color" content="#000000" />
    <meta name="description" content="Web site created using create-react-app" />
    <link rel="apple-touch-icon" href="%PUBLIC_URL%/logo192.png" />

    <link rel="manifest" href="%PUBLIC_URL%/manifest.json" />

    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.1.3/dist/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-1BmE4kWBq78iY
    <title>MERN BLOG</title>

</head>

<body>

    <div id="root"></div>

    <script src="https://code.jquery.com/jquery-3.4.1.slim.min.js" integrity="sha384-J6qa4849blE2+poT4WnyKhv5vZF5SrPo0iEjwBvKU7imGFAV0wwj
```

```
> backend@1.0.0 start
> nodemon server.js

[nodemon] 2.0.15
[nodemon] to restart at any time, enter `rs`
[nodemon] watching path(s): *.*
[nodemon] watching extensions: js,mjs,json
[nodemon] starting `node server.js`
Server running on port  5000 : undefined
Logged Error : MongooseError: The `uri` parameter to `openUri()` must be a string, got "undefined". Make sure the first parameter to `mongoose.conne
ct()` or `mongoose.createConnection()` is a string.
[nodemon] app crashed - waiting for file changes before starting...
Terminate batch job (Y/N)? y
```

Key Bibliography/References

Security is crucial for a blogging website hosted on the public cloud AWS. I've used a variety of security measures from AWS to guarantee the safety of our website. AWS WAF, AWS Shield, AWS IAM, and AWS Security Hub are a few examples of these security products.

Our website is safeguarded by a firewall provided by AWS WAF, and we are able to design our own rules to filter web traffic. Our website is protected against harmful attacks by the managed Distributed Denial of solution (DDoS) protection solution AWS Shield. By creating and managing users, groups, and roles, AWS IAM (Identity and Access Management) regulates access to AWS services and resources. Various AWS services' security alerts are collected and given a higher priority by AWS Security Hub, giving

Our database, application, and network layers have all been secured in addition to the security techniques mentioned above. To find and fix vulnerabilities, we have developed secure coding practises and routinely carry out security audits and penetration tests. We can make sure that our website is safe and that the information of our users is secured by putting certain security measures in place.

Because of MongoDB's scalability, versatility, and sophisticated security capabilities, I decided to use it for our blogging website. Its connection with AWS services complements our deployment plan and enables us to benefit from AWS security technologies to guarantee the security of our website.

REFERENCES

https://medium.com/

https://www.blogger.com/about/?bpli=1

https://bootcamp.berkeley.edu/blog/how-to-create-website-from-scratch-guide/

https://www.mongodb.com/mongodb-on-aws

https://www.freecodecamp.org/news/a-beginners-guide-on-how-to-host-a-static-site-with-aws/

https://aws.amazon.com/security/