Is the Project Achieved the Goal of Providing Security to the Instances??

Yes, the project achieved its goal of providing security to the EC2 instances. Here's how:

1. **Private Subnets for EC2 Instances**: The EC2 instances hosting the website are deployed in private subnets (project-subnet-private1-us-east-1a and project-subnet-private2-us-east-1b). These subnets are isolated from direct internet access, ensuring the instances cannot be reached directly from the public internet.
2. **Application Load Balancer (ALB) as the Entry Point**: The ALB, placed in public subnets, acts as the sole public-facing component. It receives external HTTP requests on port 80 and forwards them to the private EC2 instances on port 8000. This setup ensures users interact only with the ALB, not the instances directly.
3. **Security Groups for Controlled Access**:
    - The EC2 instances' security group allows traffic only on **port 22 (SSH)** for management (via the Bastion Host) and **port 8000** for communication with the ALB. This restricts access to only necessary services.
    - The ALB's security group allows only **port 80 (HTTP)** for public access, minimizing exposure to potential attacks.
4. **Bastion Host for Secure Management**: The Bastion Host in the public subnet enables secure SSH access to private EC2 instances using a key pair (key30April.pem). This ensures that administrative access is controlled and secure, as direct SSH from the internet to private instances is not allowed.
5. **NAT Gateways for Outbound Traffic**: Private instances use NAT Gateways in public subnets for outbound internet access (e.g., for updates), ensuring they remain shielded from inbound internet traffic.

By isolating the EC2 instances in private subnets, restricting access through security groups, and routing public traffic through the ALB, the project ensures that the instances are secure and not directly accessible from the internet.