

Platform Security Practices Demonstrated With Oracle Cloud

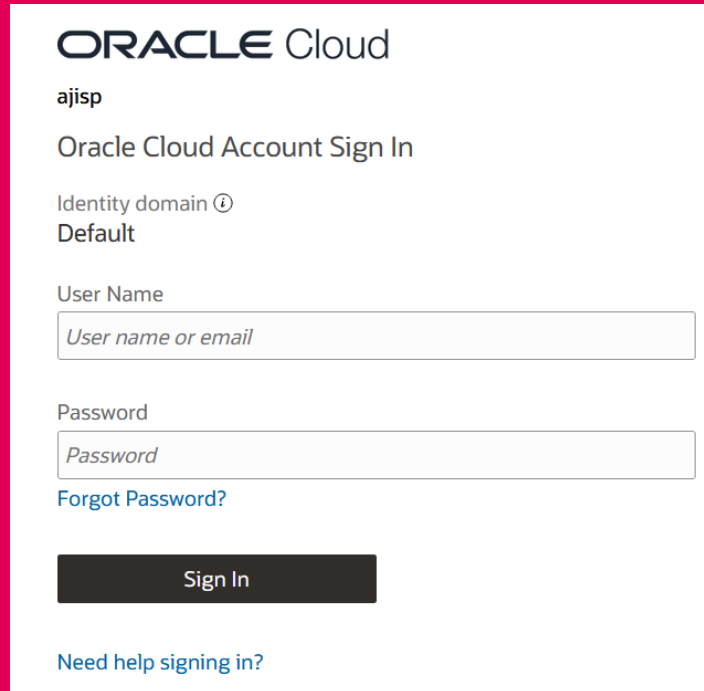
- Kristina Cormier, COSC, Okanagan College
- Ajitesh Parihar, COSC, Okanagan College

Oracle Cloud Platform

The logo for Oracle Cloud Infrastructure is centered on a white rectangular background. It features the word "ORACLE" in a bold, red, sans-serif font with a registered trademark symbol (®) to its upper right. Below "ORACLE" is the text "Cloud Infrastructure" in a black, sans-serif font.

ORACLE®
Cloud Infrastructure

Platform Security Layer 1: Password Authentication



ORACLE Cloud

ajisp

Oracle Cloud Account Sign In

Identity domain ⓘ
Default

User Name

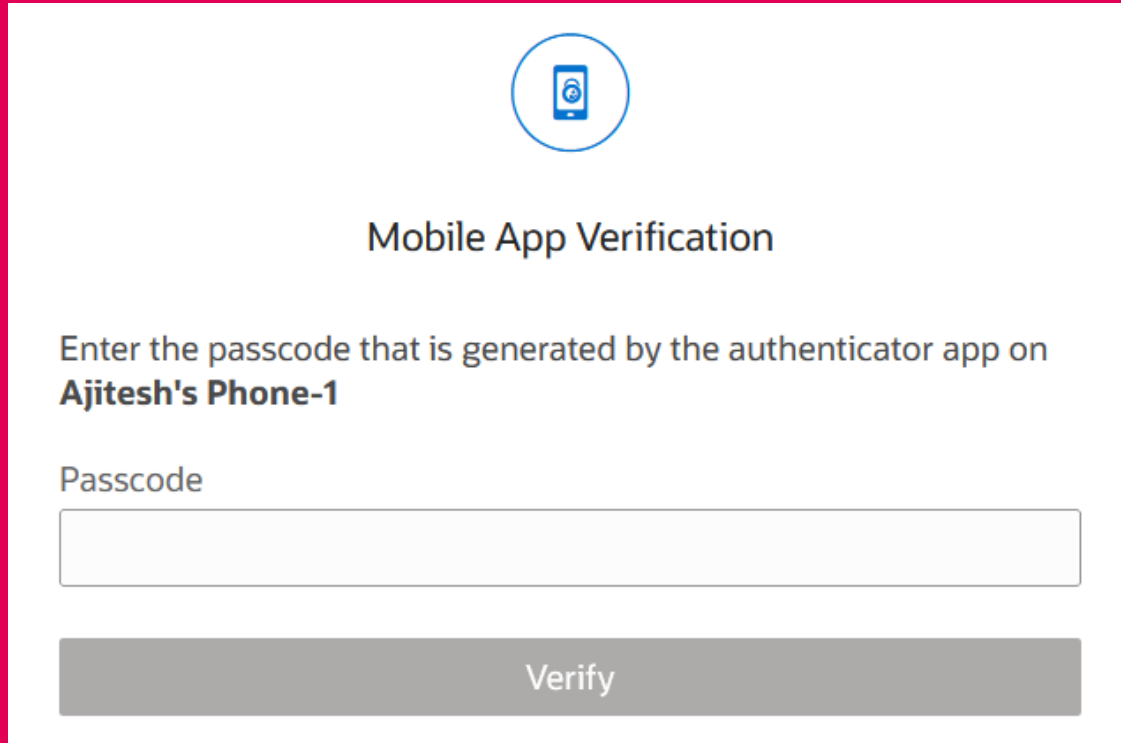
Password

[Forgot Password?](#)

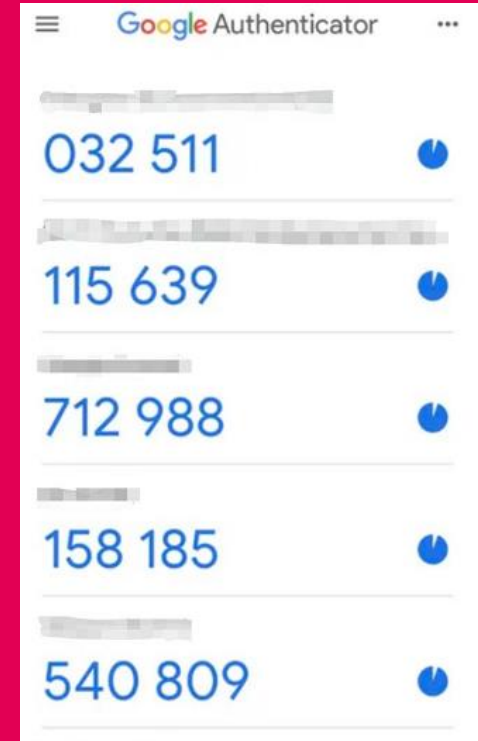
Sign In

[Need help signing in?](#)

Platform Security Layer 2: Multi-Factor Authentication



A screenshot of a mobile application verification screen. At the top center is a blue circular icon containing a smartphone. Below the icon, the text "Mobile App Verification" is displayed. Underneath, a message reads "Enter the passcode that is generated by the authenticator app on **Ajitesh's Phone-1**". A text input field labeled "Passcode" is provided for the user to enter the code. At the bottom of the screen is a large grey button with the text "Verify".



Creating a Virtual Machine on Oracle Cloud

Create compute instance

Create an instance to deploy and run applications, or save as a reusable Terraform stack for creating an instance with Resource Manager.

Name

Create in compartment

Placement

[Edit](#)

Availability domain: AD-1 Always Free-eligible **Capacity type:** On-demand capacity

Fault domain: Let Oracle choose the best fault domain

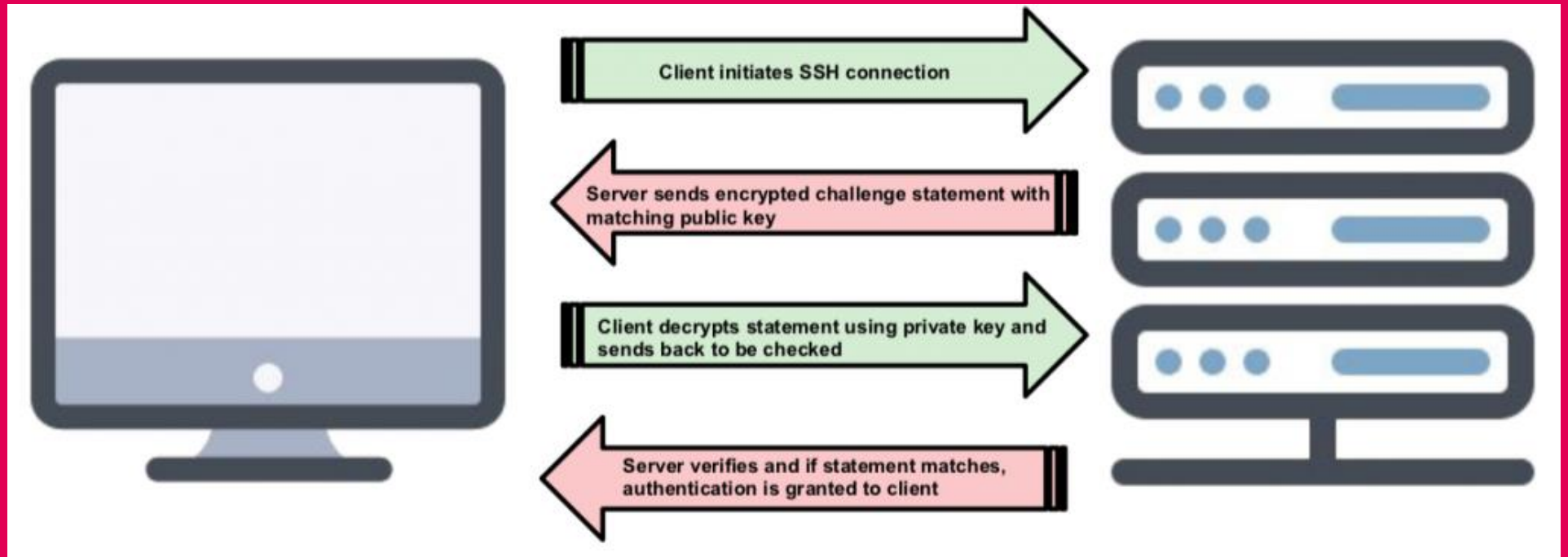
Security

[Edit](#)

Shielded instance: Disabled

[Cancel](#)

SSH Key pair: Asymmetric Encryption

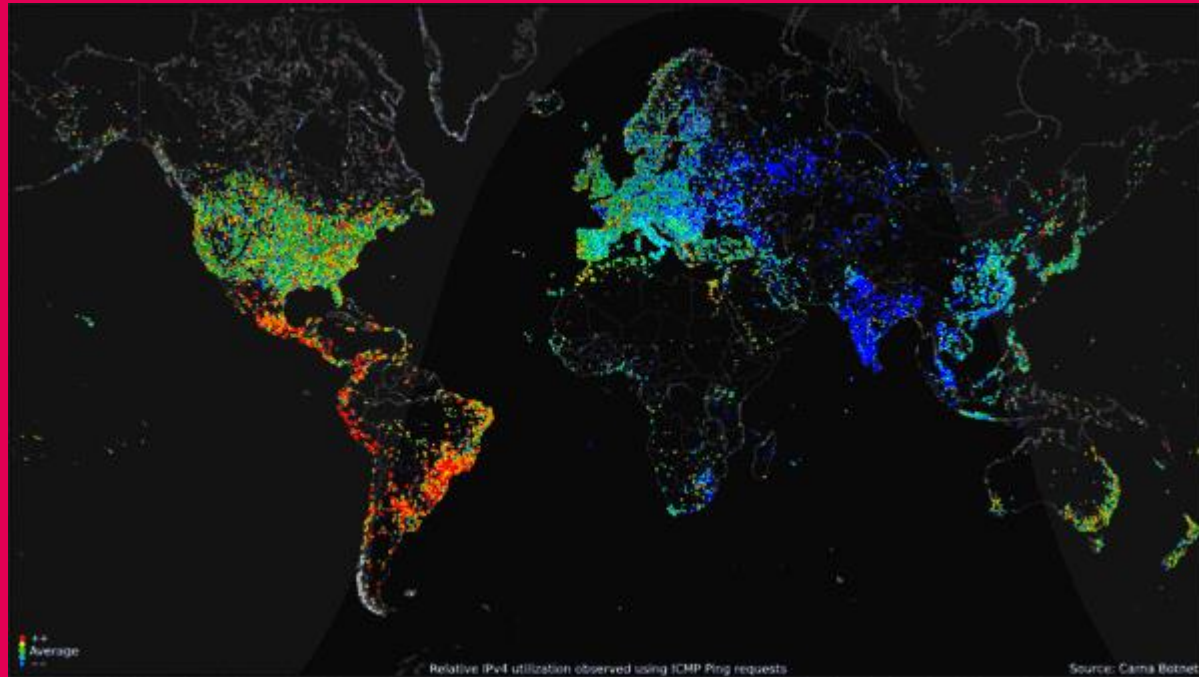


Source: <https://runcloud.io/blog/ssh-public-key-authentication>

Platform Security Layer 3: Accessing VM using private key

```
ubuntu@big-instance: ~  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
  
Try the new cross-platform PowerShell https://aka.ms/pscore6  
  
PS C:\Users\Mannzup> ssh -i C:\Users\Mannzup\OneDrive\Desktop\Work\VPC\ssh-key-2024-01-25.key ubuntu@204.216.109.200  
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-1027-oracle x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/pro  
  
System information as of Wed Aug 7 08:27:19 UTC 2024  
  
System load: 0.0      Processes:            117  
Usage of /:   21.9% of 44.96GB  Users logged in:    0  
Memory usage: 63%      IPv4 address for ens3: 10.0.0.249  
Swap usage:  0%  
  
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s  
  just raised the bar for easy, resilient and secure K8s cluster deployment.  
  
  https://ubuntu.com/engage/secure-kubernetes-at-the-edge  
  
Expanded Security Maintenance for Applications is not enabled.  
  
0 updates can be applied immediately.  
  
2 additional security updates can be applied with ESM Apps.  
Learn more about enabling ESM Apps service at https://ubuntu.com/esm  
  
Last login: Wed Aug 7 03:31:22 2024 from 24.71.238.18  
ubuntu@big-instance:~$
```

Drawbacks of not using SSH key for VM authentication: Bruteforce Botnets



Source: https://en.wikipedia.org/wiki/File:Carnabotnet_geovideo_lowres.gif

Authorization Control: sudo

```
ubuntu@big-instance: ~
SUDO(8) BSD System Manager's Manual SUDO(8)
NAME
  sudo, sudoedit - execute a command as another user
SYNOPSIS
  sudo -h | -K | -k | -V
  sudo -v [-ABknS] [-g group] [-h host] [-p prompt] [-u user]
  sudo -l [-ABknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
  sudo [-ABbEHnPS] [-C num] [-D directory] [-g group] [-h host] [-p prompt] [-R directory] [-r role] [-t type] [-T timeout] [-u user]
  [VAR=value] [-i | -s] [command]
  sudoedit [-ABknS] [-C num] [-D directory] [-g group] [-h host] [-p prompt] [-R directory] [-r role] [-t type] [-T timeout] [-u user]
  file ...
DESCRIPTION
  sudo allows a permitted user to execute a command as the superuser or another user, as specified by the security policy. The invoking user's real (not effective) user-ID is used to determine the user name with which to query the security policy.

  sudo supports a plugin architecture for security policies, auditing, and input/output logging. Third parties can develop and distribute their own plugins to work seamlessly with the sudo front-end. The default security policy is sudoers, which is configured via the file /etc/sudoers, or via LDAP. See the Plugins section for more information.

  The security policy determines what privileges, if any, a user has to run sudo. The policy may require that users authenticate themselves with a password or another authentication mechanism. If authentication is required, sudo will exit if the user's password is not entered within a configurable time limit. This limit is policy-specific; the default password prompt timeout for the sudoers security policy is 0 minutes.

  Security policies may support credential caching to allow the user to run sudo again for a period of time without requiring authentication. By default, the sudoers policy caches credentials on a per-terminal basis for 15 minutes. See the timestamp_type and timestamp_timeout options in sudoers(5) for more information. By running sudo with the -v option, a user can update the cached credentials without running a command.
```

Thank you!

Any Question?