



Mahindra
École Centrale
COLLEGE OF ENGINEERING

INFORMATION SECURITY CLOUD ENVIRONMENT

J GOPALARO

DEC 15, 2015

LEADER ■ ENTREPRENEUR ■ INNOVATOR



WHAT IS CLOUD COMPUTING



A LARGE DATA CENTER ESTABLISHED BY CLOUD PROVIDER
OFFERS SERVICES TO BUSINESS OWNERS

BUSINESS OWNERS USE THEM INSTEAD OF IN HOUSE
INFRASTRUCTURE

SERVICES CAN BE SAAS PAAS IAAS



CLOUD SCENARIO

- APPLICATION DEVELOPED ON VIRTUAL MACHINES USING IDE
- APPLICATION DEPLOYED ON DEMAND
- CLOUD PROVIDERS ASSIGNS PHYSICAL RESOURCES
- PROVIDER GIVES IP ADDRESSES
- OWNER MAPS THEM TO URLS
- END USERS ACCESS APPLN THRO URLS

INFORMATION SECURITY IN



Mahindra
École Centrale
COLLEGE OF ENGINEERING

STAND ALONE SERVER

PHYSICAL

CLIENT/SERVER(NETWORK)

FIREWALLS

INTERNET ACCESS

SECURE PROTOCOLS

CLOUD ENVIRONMENT

?



cloud env vulnerabilities

due to

OUT SOURCED NATURE

RESOURCE POOLING

MULTITENANT MODEL

KEY CHALLENGES

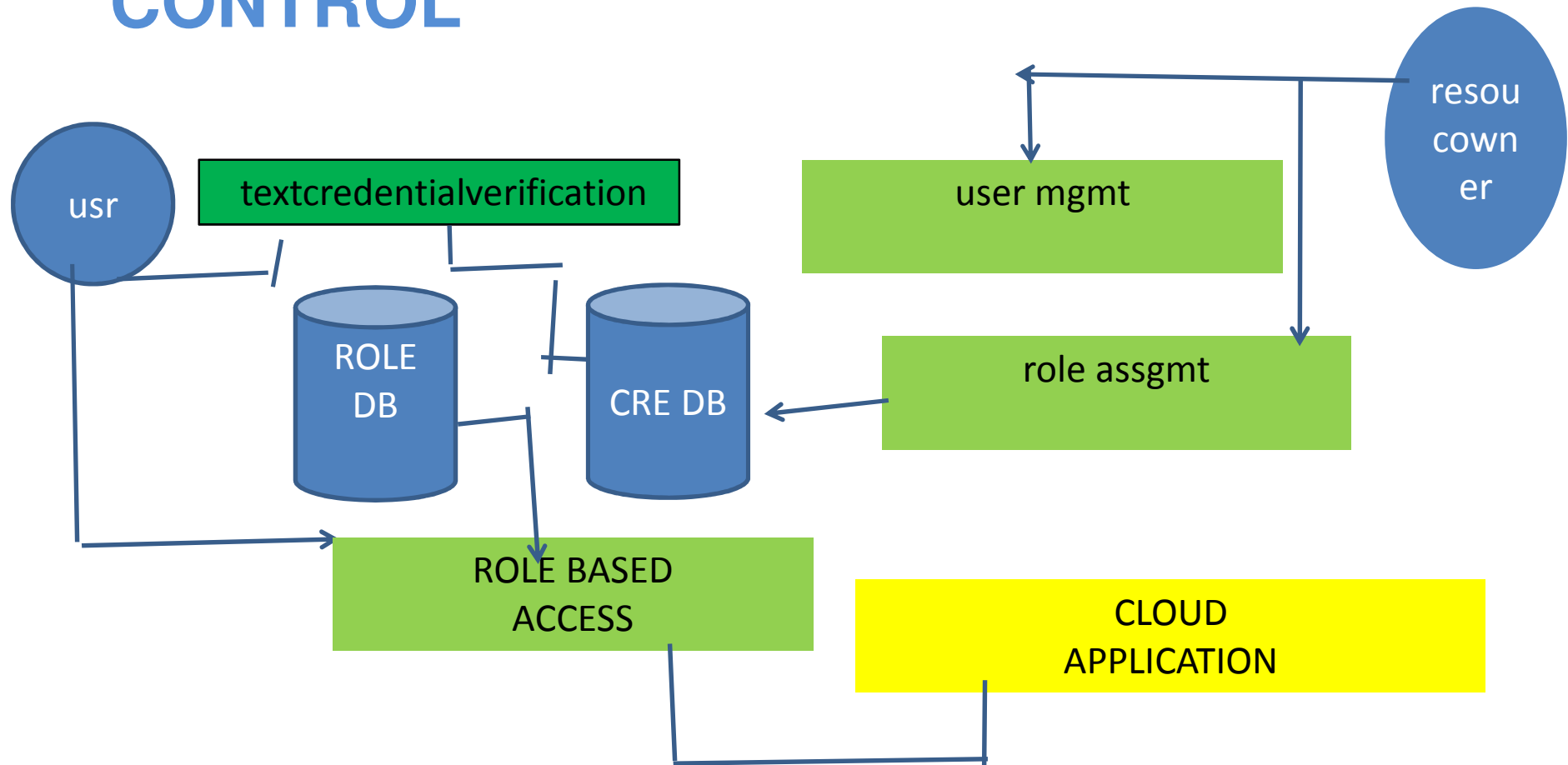
AUTHENTICATION OF USERS
AUTHORISATION OF RESOURCES
SECURITY OF DATA AT REST IN CLOUD
SECURITY OF DATA IN MOTION
TRACEABILITY OF MISUSE

HOW CAN CLOUD PROVIDER ADDRESS
SECURITY CONCERNS OF

BUSINESS OWNER
END USER

IDENTITY&ACCESS MGMT SERVICES

ROLE BASED ACCESS CONTROL



AUTHENTICATION OF USERS

DECIDED BY OWNER PASSWD/SMAETCARD/BIOMETRIC

AUTHENTICATION SERVICE PROVIDED BY CLOUD PROVIDER

USER MGMT PROVIDES FOR CREATING CREDENTIALS DB

ACCESS REQUEST VALIDATED WITH CREDENTIALDB

SOME FEATURES OF AUTHENTICATION SERVICE

SINGLE SIGN ON
SAML TOKEN
KERBEROS
OTP

AUTHORISATION OF RESOURCE ACCESS

ROLE BASED

ROLES CREATED BY USER MGMT

OAuth OPEN PROTOCOL FOR
AUTHORISATION

AUTHORISATION OF RESOURCE ACCESS

NORMALLY OWNER PASSES HIS CREDENTIALS TO USER FOR ENABLING HIM

IN OAUTH CLIENT OBTAINS A TOKEN NOT REQUIRES OWNER CREDENTIALS

A PROTOCOL IS FOLLOWED TO GET A TOKEN

TOKEN IS FOR LIMITED TIME AND USE
UNDER THIS PROTOCOL NO EXCHANGE OF SECRET KEYS
OVER NETWORK

DATA SECURITY

AT REST

THRO ENCRPTION AT
APPLICATION LEVEL
SERVER LEVEL
NETWORK LEVEL
DEVICE LEVEL

IN MOTION

THRO SECURE PROTOCOLS BY CLOUD PROVIDER

KEY MANAGEMENT

CREATION

ROTATION

STORAGE BACKUP

TRACEABILITY&AUDIT



CLOUD PROVIDER KEEPS LOGS OF USAGE
OPEN TO OWNER TO ACCESS LOGS

TRUST OF LOGGING PROCESS
SOME CLOUD PROVIDERS OFFER 3RD PARTY AUDIT



thank you

gopalarao.jammi@mechyd.ac.in

