Regional Forum on Cybersecurity in the Era of Emerging Technologies
&
the Second Meeting of the “Successful Administrative Practices”-2017
Cairo, Egypt 28-29 November 2017

Best Practice In Data Security In The Cloud

Speaker Name

Dr. Eng. Bahaa Hasan

ASC Chairman

Agenda

1. Cloud Security Questions
2. Normal Security Architecture
3. Security Architecture
4. Security Services
5. Security Mechanisms
6. Policies
7. Access Control Layers
8. Authentication Tools
9. Product Diagram

1. Cloud Security Questions

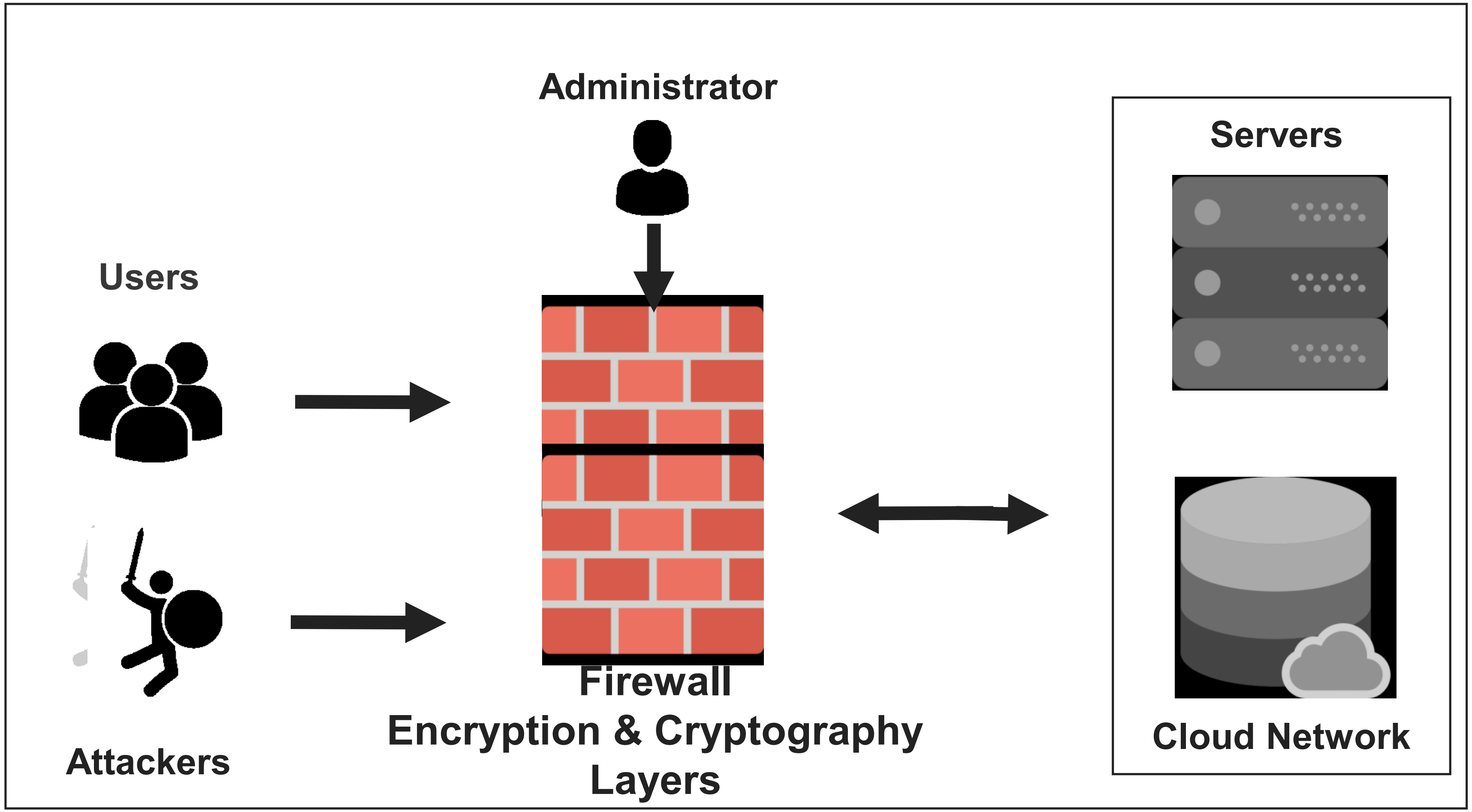
- **RQ-1:** What are the problems ?

- **RQ-2:** What is the security architecture being used to prevent unauthorized users from accessing data within the Cloud?

- **RQ-3**: What are the security services, mechanisms, policies that our proposal present?

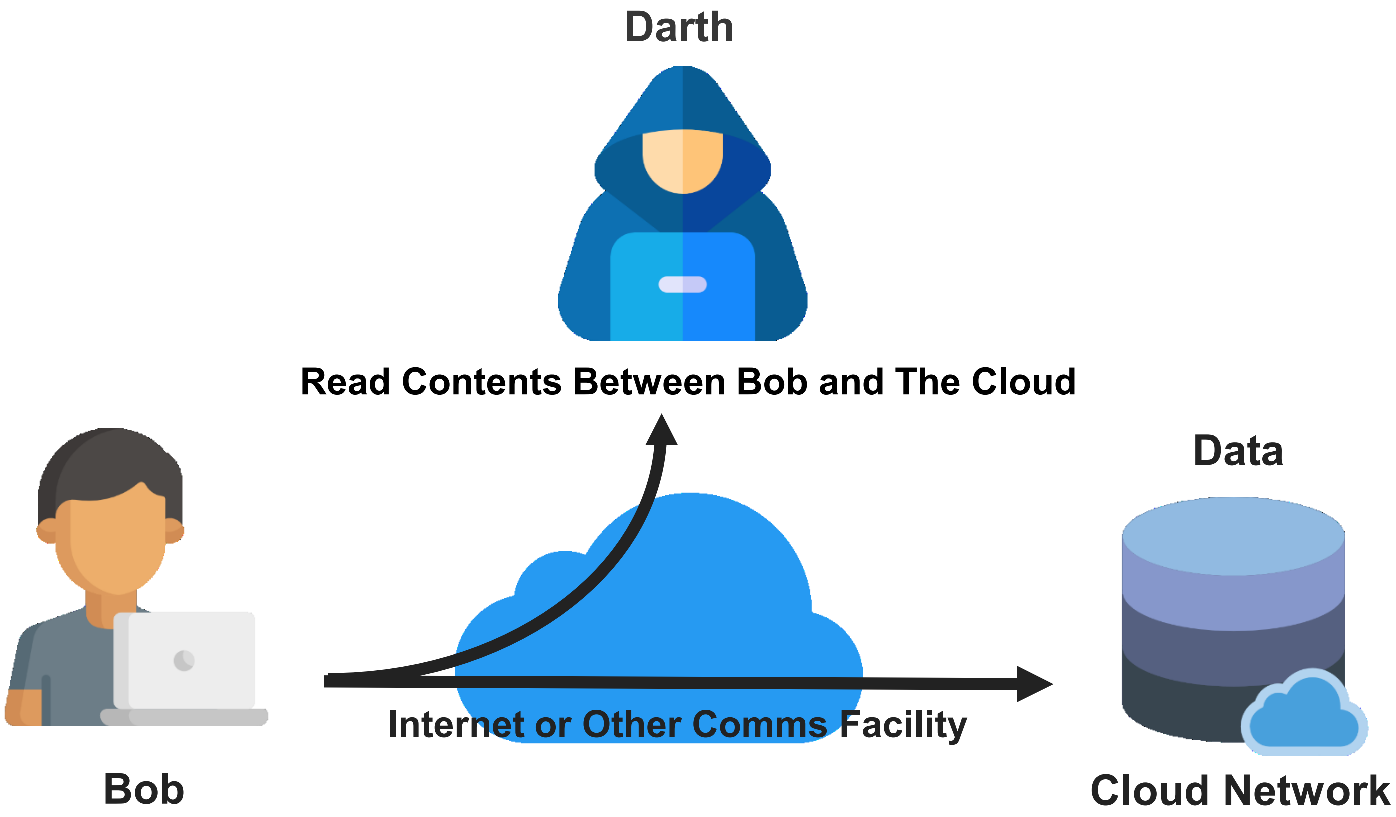
- **RQ-4**: How the proposal works?

2. Normal Security Architecture



What are the problems?

Passive Attacks



Darth

Read Contents Between Bob and The Cloud

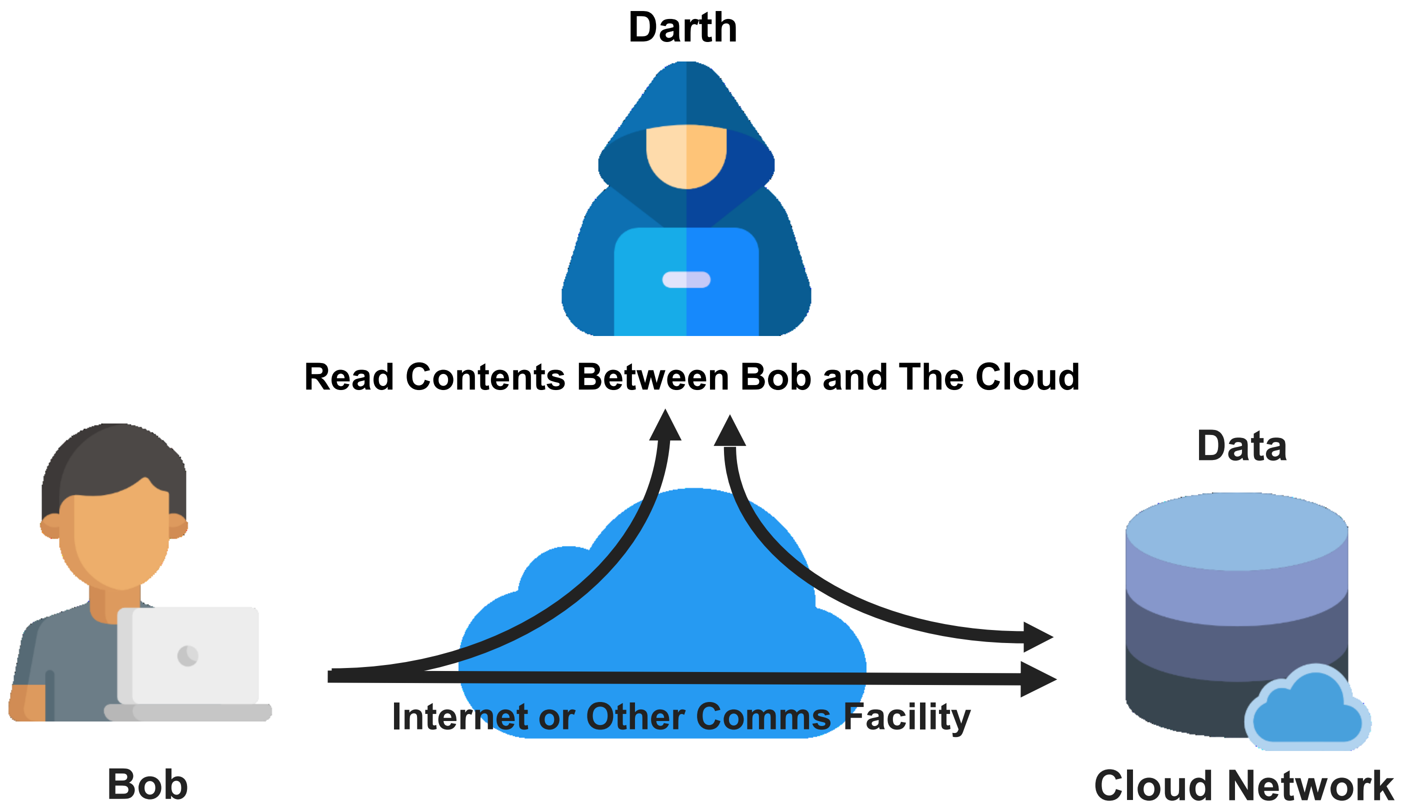
Data

Internet or Other Comms Facility

Bob

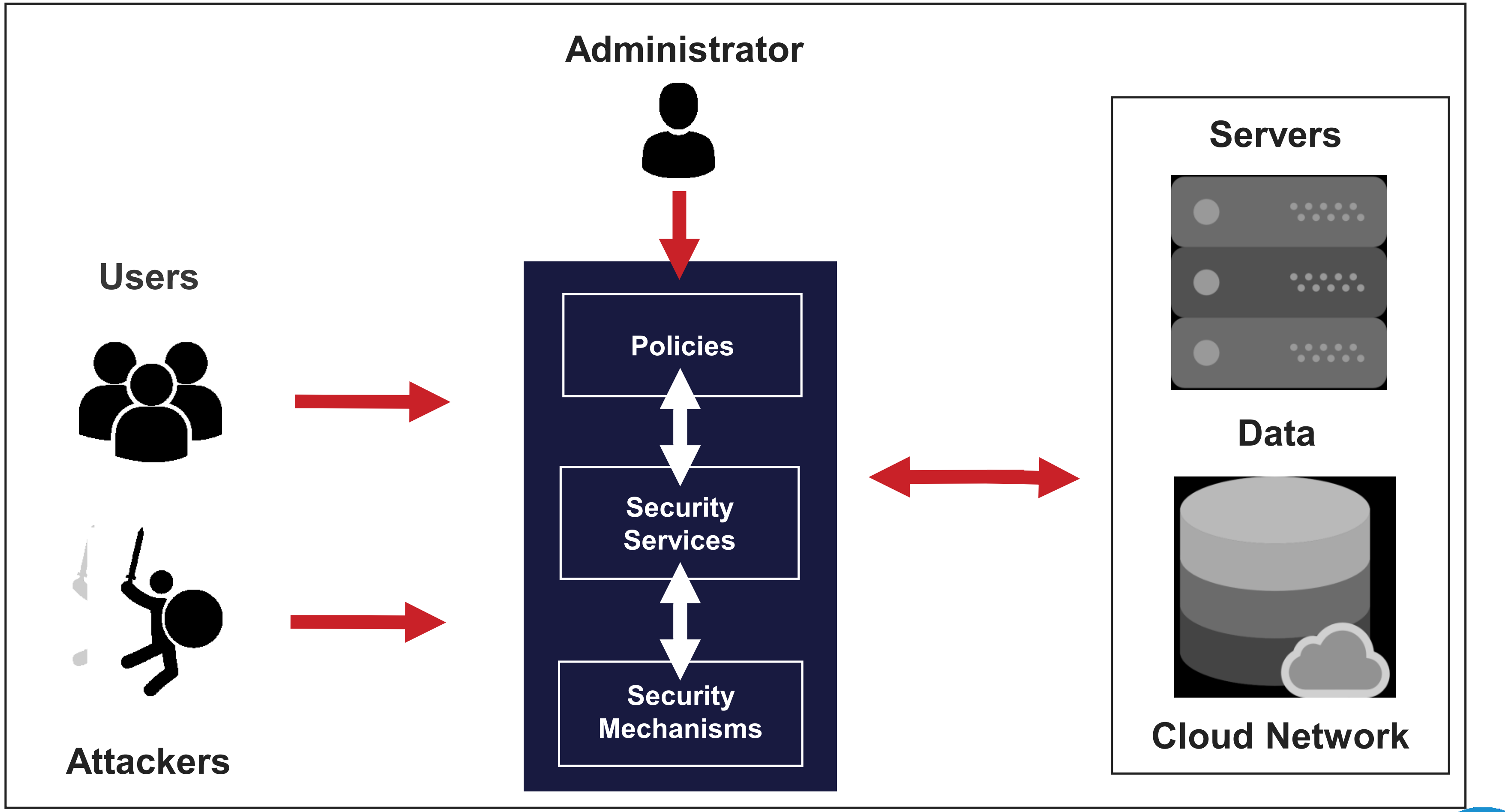
Cloud Network

Active Attacks


Darth
Read Contents Between Bob and The Cloud
Data
Internet or Other Comms Facility
Bob
Cloud Network

Backdoor Attacks For Malicious Activities

3. Security Architecture



4. Security Services

Access Control: prevention of the unauthorized use of a resource.

Data Confidentiality: protection of data from unauthorized disclosure.

Data Integrity: assurance that data received is as sent by an authorized entity.

Non-Repudiation: protection against denial by one of the parties in a communication (Monitoring).

4. Security Services cont.

Authentication: Two factor authentication (OTP – PKI).

Real time monitoring / Logging and auditing: CLI and GUI task monitoring, CLI task log and GUI video log.

- **Session Management:** Block suspicious sessions by administrator (Terminate Session).

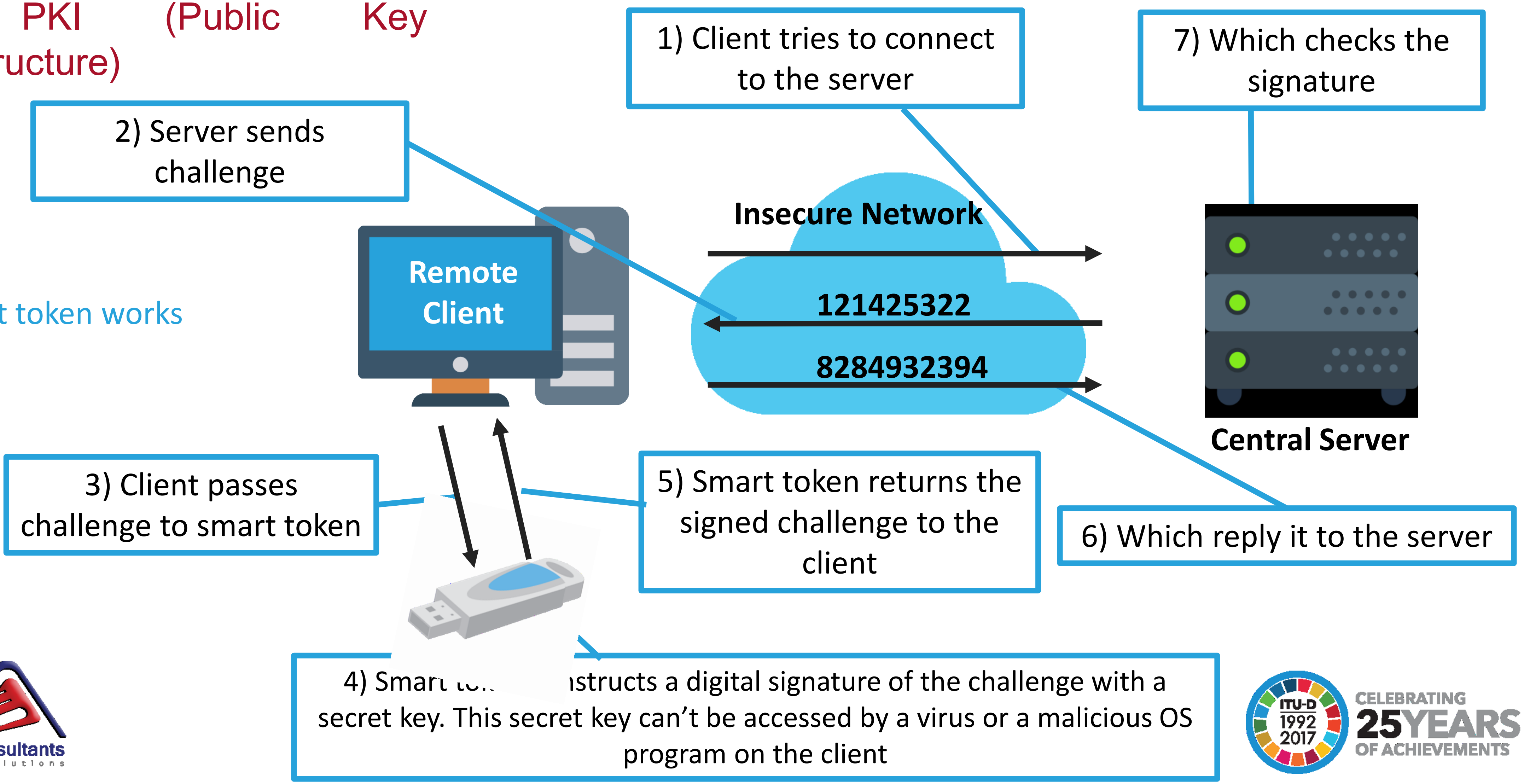
Automatic Vulnerability analysis: Provide guidelines in case of detection vulnerability and Immediate operating vulnerability check.

Manage Account Life cycle: Regulate account life cycle and shared account.

5. Security Mechanisms

5.1 PKI (Public Key Infrastructure)

How smart token works



1) Client tries to connect to the server

2) Server sends challenge

3) Client passes challenge to smart token

4) Smart token constructs a digital signature of the challenge with a secret key. This secret key can’t be accessed by a virus or a malicious OS program on the client

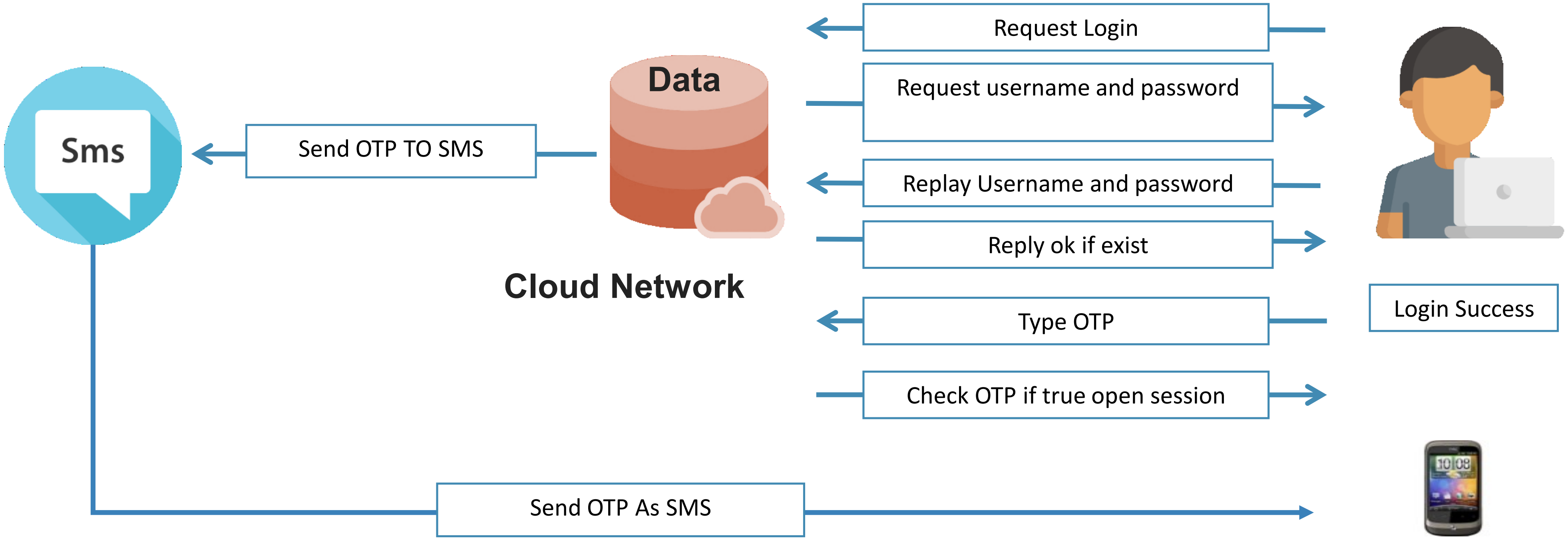
5) Smart token returns the signed challenge to the client

6) Which reply it to the server

7) Which checks the signature

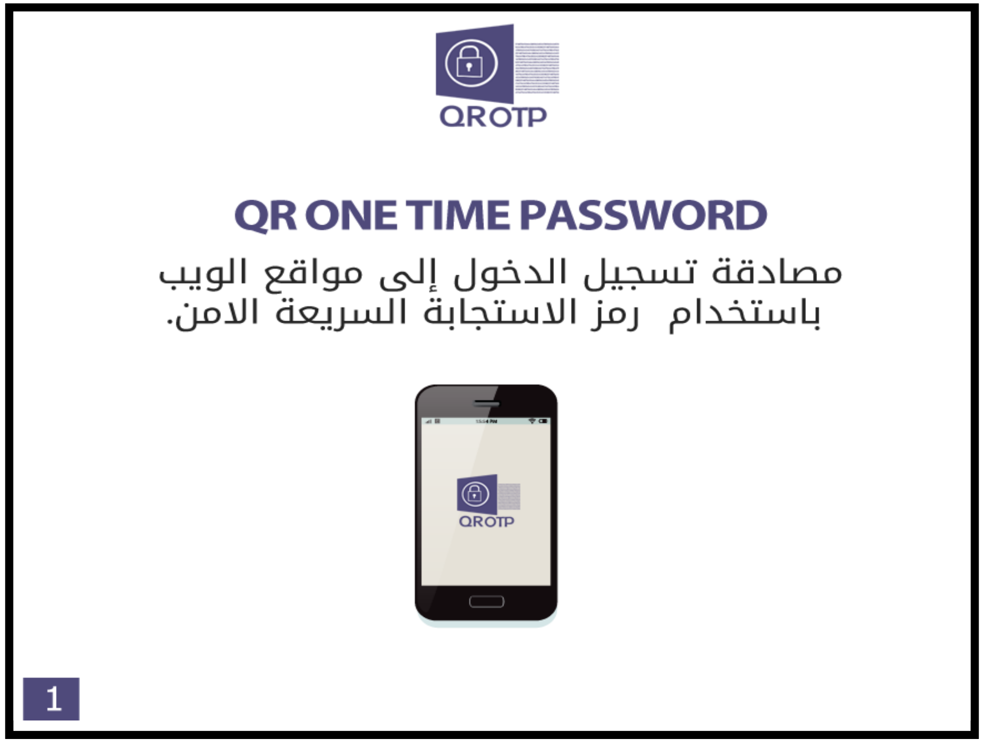
5. Security Mechanisms cont.

5.2 OTP Web Access Control (OTP-WAC)



5. Security Mechanisms

5.2.1 QR One Time Password



QROTP

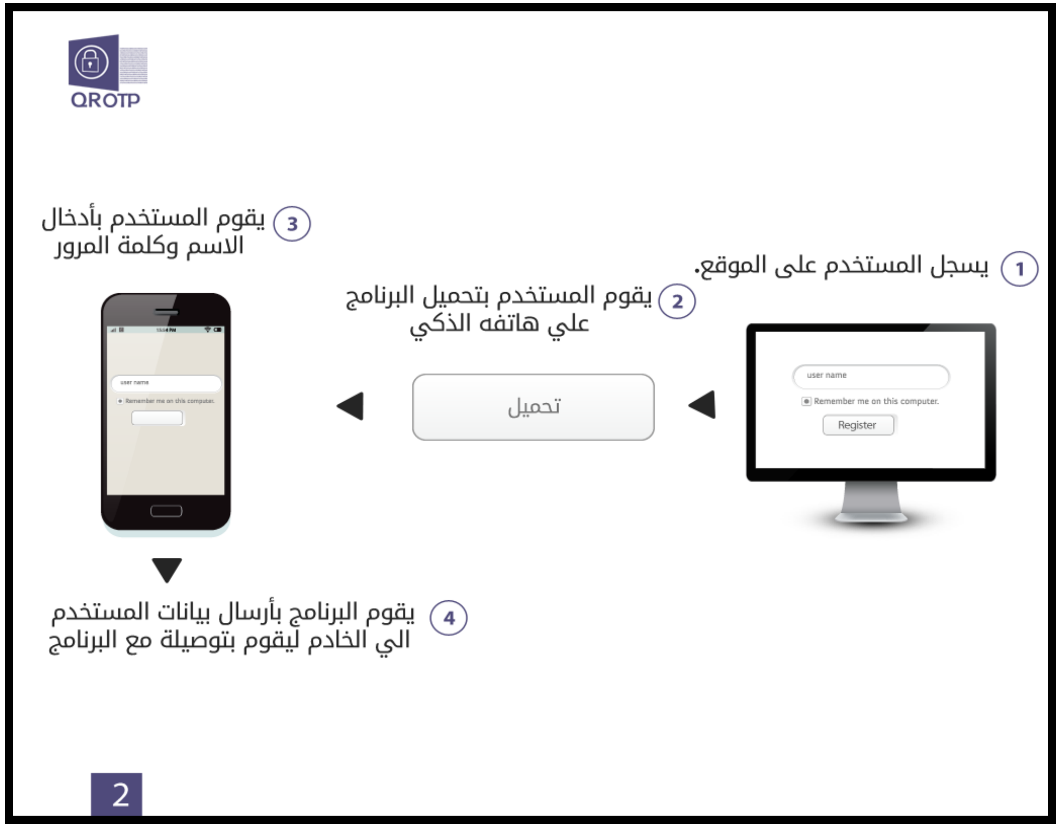
QR ONE TIME PASSWORD

مصادقة تسجيل الدخول إلى مواقع الويب
باستخدام رمز الاستجابة السريعة الامن.

1

5. Security Mechanisms

5.2.1.1 QR One Time Password



1 يسجل المستخدم على الموقع.

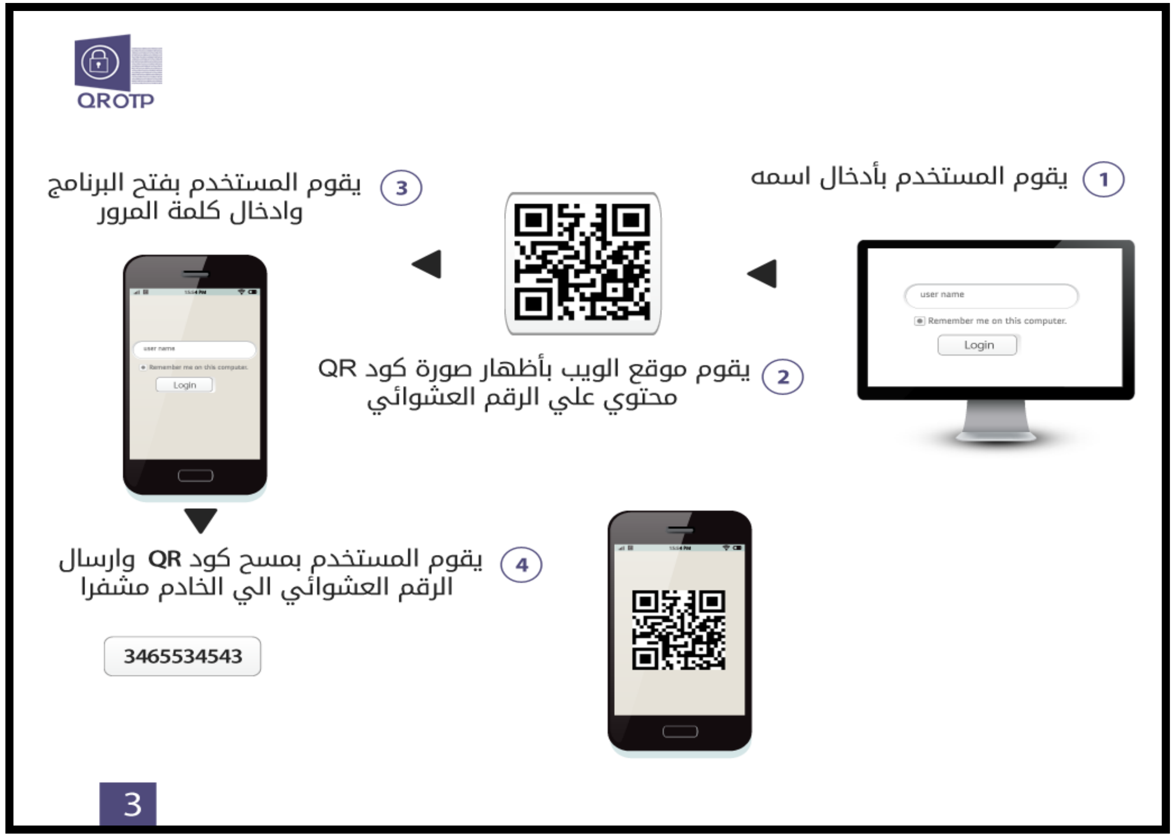
2 يقوم المستخدم بتحميل البرنامج
علي هاتفه الذكي

3 يقوم المستخدم بأدخال
الاسم وكلمة المرور

4 يقوم البرنامج بأرسال بيانات المستخدم
الي الخادم ليقوم بتوصيلة مع البرنامج

5. Security Mechanisms

5.2.1.2 QR One Time Password



1 يقوم المستخدم بأدخال اسمه

2 يقوم موقع الويب بأظهار صورة كود QR
محتوي علي الرقم العشوائي

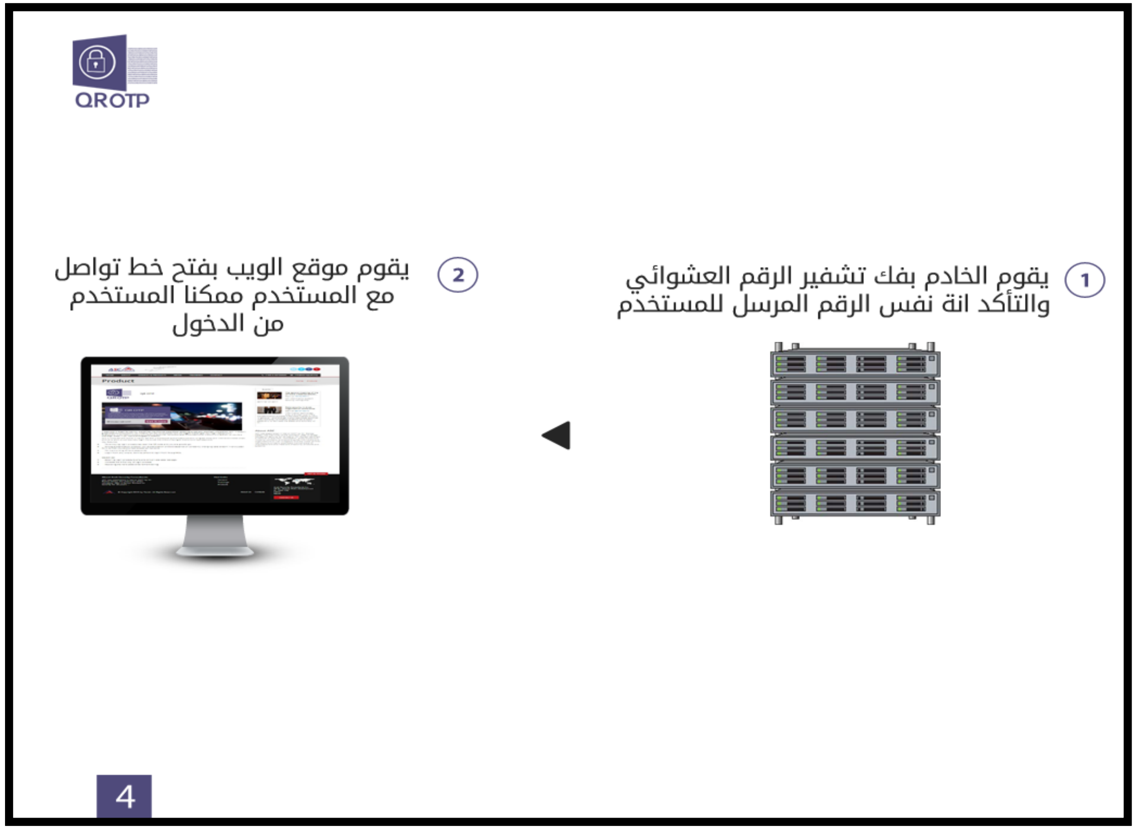
3 يقوم المستخدم بفتح البرنامج
وادخال كلمة المرور

4 يقوم المستخدم بمسح كود QR وارسال
الرقم العشوائي الي الخادم مشفرا

3465534543

5. Security Mechanisms

5.2.1.3 QR One Time Password



1 يقوم الخادم بفك تشفير الرقم العشوائي والتأكد انة نفس الرقم المرسل للمستخدم

2 يقوم موقع الويب بفتح خط تواصل مع المستخدم ممكنا المستخدم من الدخول

6. Policies

- Supports a variety of environments through the application of rule–based policies.

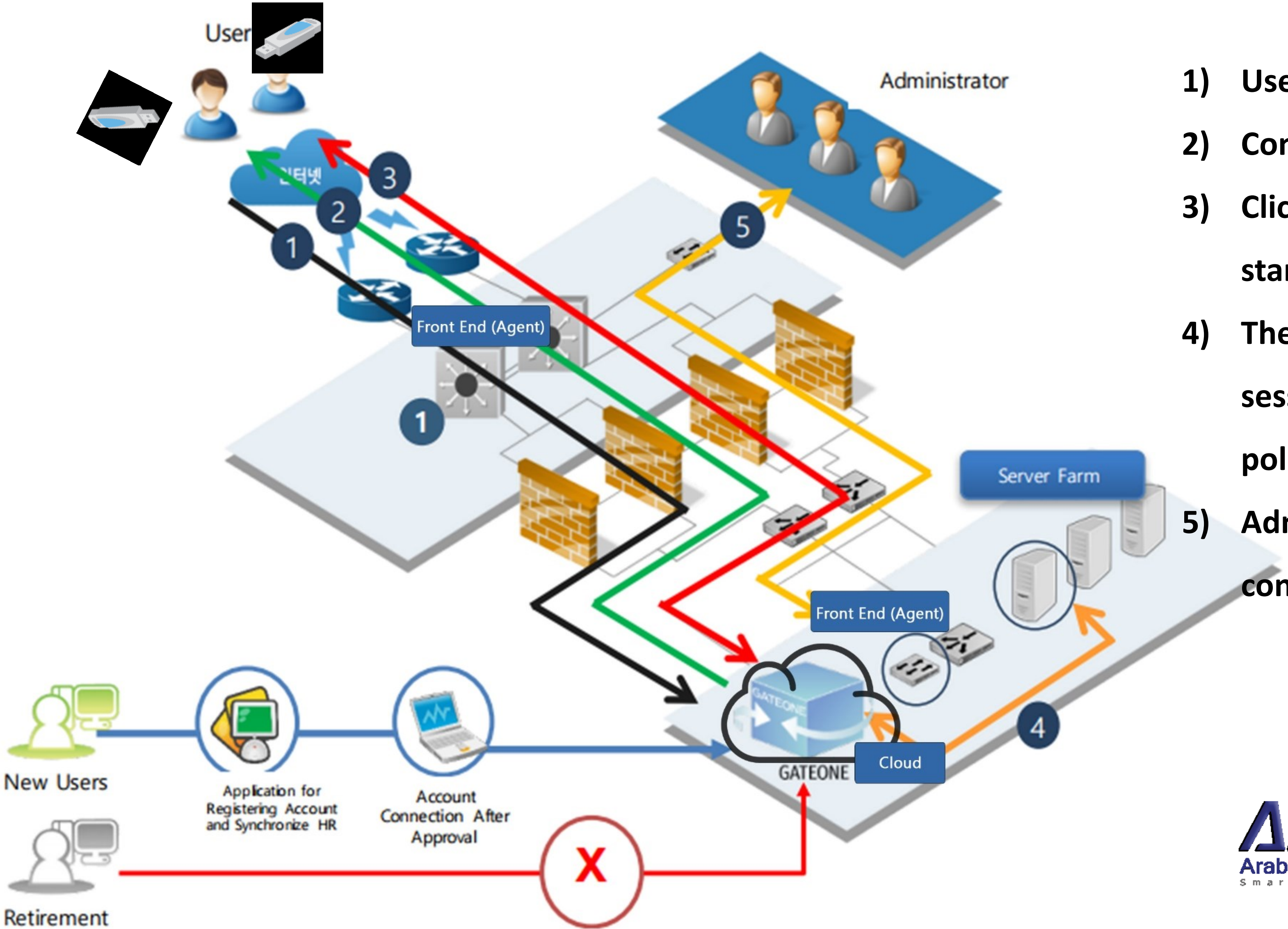
- Admin can set the policy and apply it on users, groups and admins to control commands on client’s needs.

- The policy of our proposal is flexible.

- So the more the policy is specific, the more efficient of the system.

How the solution works?

9. Product Diagram



1) User Logging in on web interface.
2) Connectable list is shown up on user screen.
3) Clicking connectable equipment, user session starts.
4) The proposed system starts recording user sessions and controlling work process upon policy.
5) Administrator performs log auditing, controlling and monitoring.

Any questions?

You can find me at:

Tel : +20-2-22732-620

Fax : +20-2-26701994

Cell: +20-12-314-9864

Website: http://isec.com.eg/

Email : info@isec.com.eg

Thank You