ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

Cloud Based Secure Access

[1] Chethan Kumar T E, [2]Karthik Venkateswaran
[1][2] L&T Technology Services Ltd.

Abstract **- Secure Access is one of the prime requirements to any personal or public asset. Enabling access to only designated personnel is main requirement. All of the current systems are limited by physical resource to gain access such as Key, Access card or Trusted escort. Cloud Based Secure access apart from solving the physical resource also solves the problem of Access Card/Medium being misused by unauthorized personnel and additional controlled access can be granted or revoked easily by the asset owner.**

Index Terms— Asset Security, Cloud technologies, Camera vision, Face capturing.

I. INTRODUCTION

A. Overview

Asset secure access is a prime requirement across all domains and industry. For example: Hotel, Airport, Residence, Hospital, Industries, and Banking.
Most of the existing secure access systems are statically configured which demand asset owners presence in the vicinity of the asset to manage access (gain or revoke).For instance, the security officer needs to tag the person requesting access with access card, biometrics or similar systems to provide access.

B. Drawbacks

- Asset owner proximity to security system :
  - Configure new users/ revoking existing users
  - Remote management of asset access regulation is not always linked to security access systems (card, biometrics etc.)
- Possibility of unregulated proxy entry using others access card
- Additional hardware required for managing security access such as card readers, biometric readers.

C. Proposed Improvements

- By incorporating Face Recognition as one of the emerging biometric aid
  - Dependency on external hardware is reduced
- Cloud based access control provides flexibility
  - Remote asset access management for user can be made possible with cloud access reducing proxy or unregulated access
- By using existing surveillance cameras the need for specialized hardware for access can be reduced

II. OBJECTIVE

The Objective of the "Cloud Based Secure Access" paper is

- To solve the limitation w.r.t physical resource
- Biometric Integration to cloud (Face Recognition)
- Provide Online
  - Tracking
  - Authorization
  - Access mechanisms for personal and public assets
- Enable Asset owner to
  - Dynamically manage the access privileges without any limitation on the physical resources
  - Monitor and maintain asset access history
- Evolve to a role/privilege based access management

III. PROCEDURE AND METHODOLOGY

Below are set of activities envisaged to create a Cloud based secure access system

1.Create a cloud based secure access frame work
2.Create database for
   a. Asset owner
   b. trusted users needing access
3. Integrate & customize Face capturing & matching Algorithms
4. Provide integrated app/text notification mechanisms to Asset owner
5. Provide framework for Asset Owner to execute remote commands
   a. Allow Access
   b. Deny Access
   c. Allow for limited time

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

IV. CONCEPT DEVELOPMENT

For the Cloud based secure access development following are the essential building blocks and its selection considerations:

A. BUILDING BLOCKS

1) Asset

Asset Area/Physical infrastructure that needs access protection

2) Actors

These are the users of the system:

- Asset Owner:
  - Individual/Group which owns access to the asset
  - Having remote asset access ability to manage remotely the entry/access to the asset
- Users requesting access for an Asset

3) Systems

These are infrastructure such as hardware and software systems providing the ability of secure access management.

More details of the systems are dissected in the next section.

B. SYSTEMS

Systems are the building blocks which has varied set of choices in terms of hardware and software systems. Below sections explains the selection criteria applied and narrowed down set of options.

1)Video Analytics Algorithm:

This is the software that confirms a match from the database of specimen images.

a)Considerations

•Software algorithm to perform face match & recognition
•Ability to configure the match criteria
•Options: OpenCV, OpenBR

b)Selection

•OpenBR[1] provides biometric analysis and configurable algorithms (is a superset of OpenCV functionalities)
•Single API call to confirm face matching (Face Detection, Normalization, Representation, Extraction)

2)Cloud Web Services:

•Services hosted on the cloud to enable asset access management
•Data Base:Managing user registration, revocation of access

a)Consideration

•Cloud framework that is extensible to hybrid, multi-tenant infrastructure
•Simple Web application (frontend + backend) for admin/user role access
•Options: AWS, Google Cloud, Openstack

b) Selection

•Amazon WebServices [3]is most popular IaaS
•Extensible with frameworks such as CloudFront (Content delivery) and Elastic Beanstalk (Web application)
•Cloud web apps ability to be rendered on Asset Owner's smartphones/tablets

3) IOT Enabled Control:

•Embedded controls to allow or deny access to the asset

a)Consideration

•Plug-in the embedded SoC with electro-mechanical access devices
•Off-the shelf internet connectivity
•Options: Arduino, Raspberry, Particle

b)Selection

•Particle Cloud[4] provides necessary REST API control access logic for the on-board Particle core I/O pins

- Less than 20$ for reference board – cheapest WiFi enabled IoT board

V. FINALIZED CONCEPT – ASSEMBLY

Below is the visualization of how actors and finalized system components interact to form a Cloud Based Secure Access.

Figure 1 Finalized Concept Architecture

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

The details of the software implementations are explained in the section Error! Reference source not found. Use case flow of the actors and systems are explained in section VII.

VI. SOFTWARE IMPLEMENTATION

Below provides overview of the software components implemented and its high level functionality:

- Web App (User)
  - HTML Application to capture camera snapshot
  - Upload the image to Server
  - Retrieve the result – Deny/Allow access
- Web App (Admin)
  - Manage Registration of users and their pics
  - View logs of asset requests
  - Allow/Deny strangers
  - Details of Desktop/Android App
  - Web view for asset owner to perform admin actions
  - Web view for user to request access
- Details of Video Analytics
  - Open Biometrics (OpenBR) used to validate the face recognition using 4SF algorithm[2]
- Details of AWS
  - Ubuntu based instance running OpenBR and the PHP Server code
- Details of Particle FW
  - Single Chip IoT Board + WiFi + Relay boards
  - Connectivity through Particle Cloud REST APIs

VII. DEMO USE CASES

A. Use Case 1: Home security system

- Identified family members are registered in the CBSA by the asset owner
- Family member stands in front of POA [Point Of Access]
- CBSA system captures the face of the individual and runs a face match algorithm
- And approves or rejects the access
- Asset Owner is notified through SMS/App Notification

B. Use Case 2: Employee Access to Company

- New employees are registered in the CBSA by the HR/Security officer
- These employees are classified to have access to General work zone and/or Privileged zones.
- Employees of a company stands in front of POA [Point Of Access]
- CBSA system captures the face of the individual and runs a face match algorithm
- And approves or rejects the access depending on the category of zone they have access to.
- SMS/ App Notification/Access of different personnel are logged

VIII. DEPLOYMENT MODELS

This section describes possible deployment models of CBSA system

A. Framework as a service

CBSA can be easily integrated with different options available in the space of Video analytics, Cloud and IoT framework. This can be designed as a plug and play framework, which can be integrated with an existing

- Asset security system that is connected to the network [7],
- Video capturing devices connected to the network
- Face recognition algorithms
- Cloud Home/Industry automation solution[5][6]

B. Product

CBSA can be visualized as a complete end to end product incorporating all the systems with practical considerations refined for the specific domain/industry.

IX. WAY AHEAD

- Analytics across industry/domains
  - Hospitality: Hotel occupancy
  - Medical Facility: In-Patient utilization
- Recommendation engine
  - Asset utilization as applicable to different
  - Consumer Analytics:
    - For Products and Services sectors
    - Loyalty info – offers/discount
  - Identification Possible Repeat Business opportunity

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

- Security
  - Data in transit:
    - Secure communication over HTTPS (Certificate chain of trust between IoT access, Cloud framework and Admin user application)
    - Access control using strong password and user roles (Framework Admin, Asset Owner, User, Stranger)
  - Data at rest:
    - DB and Image security using encrypted user key (specifically required in a multi-tenant cloud like AWS, Google Cloud)

X. CONCLUSION

In this paper, the attempt is to realize advanced secure access system using the face recognition as a primary biometric option. Study and Analysis of all Building blocks involved in Cloud Based Secure Access [Actors, Systems] is incorporated and the procedure for implementing CBSA is detailed. The various sub components involved in system is analysed for various consideration factors and selection is done, however this selection of Subcomponents in the subsystem stage can be further fine-tuned based on the domain involved Finally Uses cases are depicted and Deployment models are identified. Overall be having CBSA implemented and realized there can be a huge benefits that can be realized ad monetized which help in realizing both direct and indirect business benefits CBSA is Applicable for multiple domains as depicted in Figure

Figure 2 CBSA applicability to different domains

REFERENCES

[1] Open BR: http://openbiometrics.org/

[2] Face Recognition Algorithm: http://openbiometrics.org/docs/tutorials/#face-recognition

[3] Application development on AWS: https://aws.amazon.com/developers/getting-started/

[4] Particle Core: https://www.particle.io/

[5] Google Nest https://nest.com/camera/meet-nest-cam/

[6] Comcast Xfinity Home Security Devices: http://www.xfinity.com/home-security/devices.html

[7] Netatmo: https://www.netatmo.com/en-US/product/security/welcome