IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 74-79
www.iosrjournals.org

Cloud Based Face Detection, Recognition and Analysis

Saurabh Indoria[1], Shubham Chhaparia[2], Vidyadhari Singh[3], Kalindi Awasthi[4]
[1]*(Computer Engineering, Thakur College of Engineering and Technology/ Mumbai University, India)*
[2]*(Computer Engineering, Thakur College Of Engineering And Technology/ Mumbai University, India)*
[3]*(Computer Engineering, Thakur College Of Engineering And Technology/ Mumbai University, India)*

Abstract : *Surveillance devices capture a lot of information but still it requires a human to interpret data. This wastes a lot of potential usage of the valuable data collected. If instead, there is a solution which reduces the human effort required in the process, the efficiency and the utilization of the surveillance system will increase. The main idea behind this is to deploy an application server on AWS cloud which will be connected to a Mobile Application which will be working as a surveillance device. Due to the use of AWS Cloud, the backend costs would be reduced by a significant level. To reduce the development time, face recognition libraries will be used. This system can be used for various applications such as office premises, educational institutions, or other premises.*

Keywords - *AWS, Cloud, Face recognition, Surveillance, Serverless, Server-based.*

I. INTRODUCTION

Security devices have been progressively introduced in different types of organizations and institutional premises. The most widely recognized of all are the reconnaissance gadgets, for example, CCTVs. Various types premises as a rule have them to keep a beware of the exercises of the territories remotely observed by a human operator. This itself presents a state of disappointment as human mistake. People can't be constantly proficient in what they do, and furthermore, they have a restricted extent of work. The worker hours required for expanding the usage of such complex CCTV frameworks bring about an extra weight on the supporter. Thus, in numerous situations, observation gadgets are regularly simply used to record occasions on the off chance that they are utilized as a part of future reference. In general, a surveillance system would consist of thee following components:

1. A number of VGA Night Vision Camera devices.
2. Network Video Recorder (NVR).
3. Ethernet backbone network.
4. Internet routers for remote monitoring and storage (Optional).
5. Monitoring Stations (Optional).

In numerous spots, it is discovered that IP cameras are being utilized which impart through the web to the remote servers and permit remote checking from any piece of the world. Likewise mulling over the expanding web extension in India, we can derive that all reconnaissance frameworks would likely be associated with the web in not so distant future. As of the present situation, the web availability is utilized for enabling the security frameworks to store the information on remote servers and furthermore empowering the remote checking of the frameworks. Be that as it may, since the information is being gathered in such a tremendous amount, security isn't the main viewpoint which could be focused on. Preparing information locally would be a testing errand, yet since it is being sent over the web to remote servers, we can consider different ways which can influence the way the information is used. Considering the way that the observation frameworks are associated with the web, we can go to a deduction that having specific information preparing servers in the cloud can help use the information in a more effective manner. Till date, observation frameworks have been utilizing for unadulterated checking purposes, however we believe that we can extend the extent of these frameworks filling different needs as the information gathered is tremendous and can be used in different ways. Lessening the human work simultaneously and expanding usage is the principle objective behind this undertaking. Utilizing the forces of AWS Cloud and its administrations joined with the reconnaissance frameworks, we go for taking care of genuine issues set up by different prestigious foundations.

II. PROPOSED METHODOLOGY

The main objective of this project is to provide a working proof of concept for the advanced monitoring system. Mobile devices would be used as monitoring devices. Application servers would be deployed on cloud.

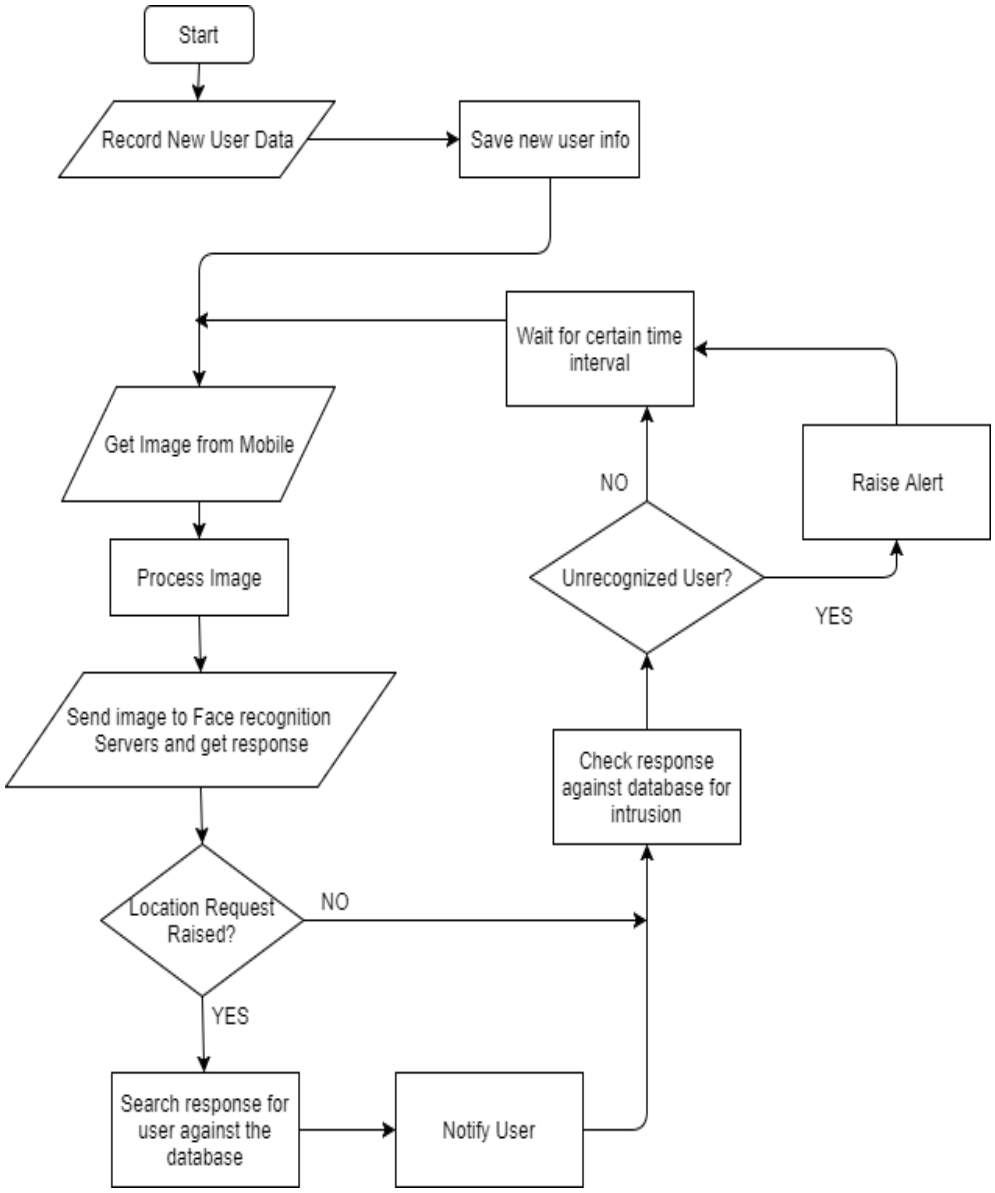

Fig 4. Flowchart

The basic flow of the project would be as such:
Step 1: Mobile device connects to remote servers.
Step 2: At fixed intervals, the device sends an image up to the cloud.
Step 3: These images are run through the face recognition servers.
Step 4: The face ids are retrieved and are checked against the database for intrusion detection.
Step 5: If some room gives a paging request for an individual, the application servers get in touch with all the mobile devices (monitoring devices).
Step 6: A signal is sent to mobile device to send an image of the area its monitoring.
Step 7: All the images are run through face recognition servers and the corresponding face ID is determined by checking the individual against the database.
Step 8: Appropriate alarm is raise and notification is sent.
Step 9: All the activity is logged into the database for analysis purposes.

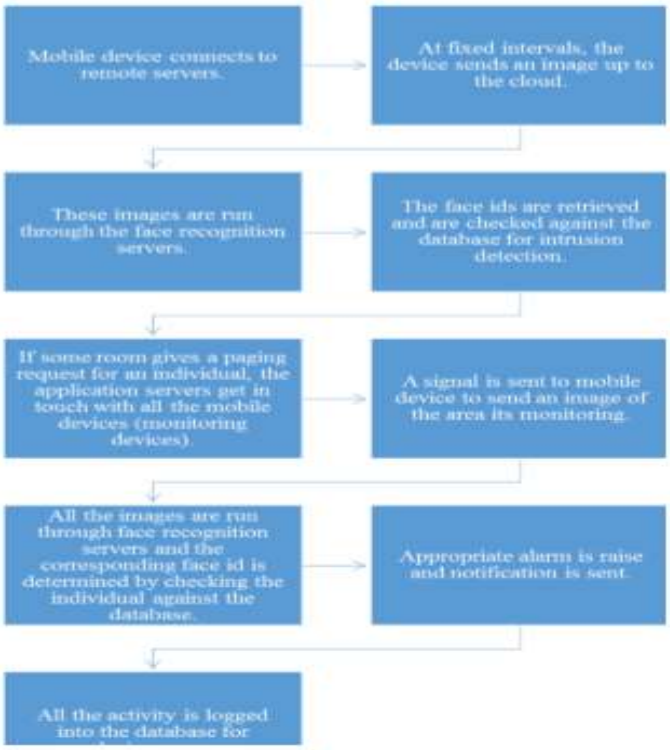

Fig 1. Methodology

III. SYSTEM ARCHITECTURE

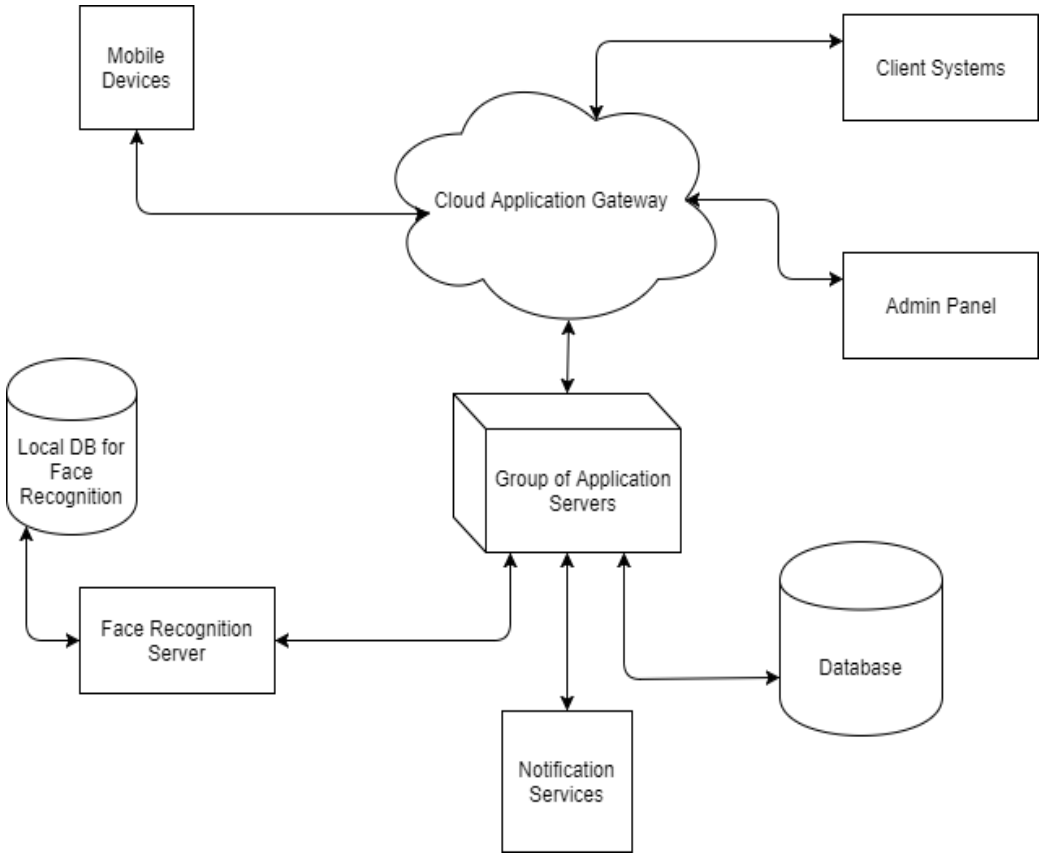

Fig 2. Structural Model

The structural model is described as a general software architecture model. Various modules and their functions are listed below:

1. Mobile Device: It will act as the data collection device, or simply, a CCTV.
2. Client System: This is basically the interface for the alert to be raised from client side to locate a person.
3. Admin Panel: Overall system control and monitoring panel.
4. Cloud application gateway: All the external connections would be through the gateway device.
5. Group of application servers: These will be clusters of instances running to serve the requests and would be under an autoscaling group.
6. Face Recognition Servers: These will be processing the image received from the application server and will return back the response containing the detected and recognized faces.
7. Notification Services: For sending various forms of notifications such as SMS, email, etc.
8. Database: For storing user information, logs, etc.

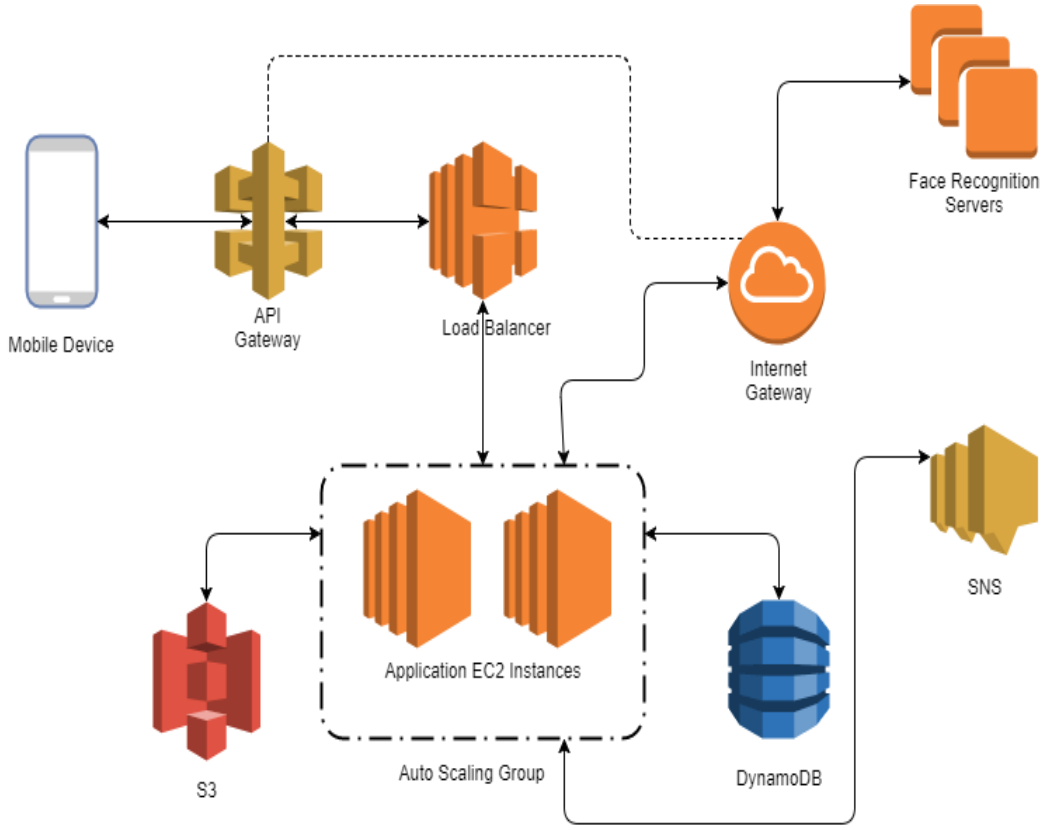

Fig 3. System Architecture

The above is a proposed system architecture using public cloud infrastructure from AWS. Various services are described below:

1. API Gateway: It handles the API requests and routes them to proper application servers. It also manages usage quota, API keys, etc.
2. Load Balancer: It distributes the incoming traffic among the underlying instances using various algorithms.
3. EC2 Instances: Elastic compute cloud instances are basically individual instance of a server, which are used in clusters for load balancing.
4. Auto Scaling Group: This functionality basically monitors the load on the cluster of instances and can be configured to scale up or scale down horizontally or vertically based on various performance metrics.
5. S3: Simple storage service is a key-value store service used to store flat files. This can be used to store images, logs, metadata, etc.
6. DynamoDB: It a fully managed, NoSQL database which concurrently replicates the database in 2 regions, each having 3 availability zones, thus creating 6 redundant copies of the data. It also can be configured to auto scale based on the amount of database traffic being generated. Failover is managed by AWS only.
7. SNS: Simple notification system is used to send SMS, email notifications to users.
8. Internet Gateway: It is used to connect the VPC (Virtual private cloud) to the outside world via internet. ACLs are defined to restrict the type of traffic flow for security purposes.

SCOPE

1. LOCATION TRACKING: DETERMINING THE LOCATION OF INDIVIDUALS IN A HIGH SECURITY PREMISE.
2. Head Count: Determining or approximating the number of individuals present at a given place at a given time.
3. Intrusion Detection: Recognizing unauthorized personnel trying to enter or forcefully entering a secured zone with restricted access and raising appropriate alarm.
4. Authorization: Uninterrupted access using facial recognition for authorization.
5. Management Reports: Generate reports based on certain analysis.

Applications:

1. High Security Premises:
   It can be deployed in high security premises for automated intrusion detection.
2. Business Institutions:
   It can be used to authorize and authenticate access to secured locations without any hindrance.
3. Research Institutions:
   It can be used to track location of important personnel at the time of emergencies.
4. Educational Institution:
   It can be used for attendance management.

IV. DISCUSSION

Since the naive systems are not capable of using the collected data as efficiently as our system, the following will be the advantages and disadvantages of the proposed system.

Advantages:

1) Less human intervention.
2) Reduction in operating costs.
3) Lower chances of human error.
4) Wide scope to expand functionalities.
5) Unlimited capacity.
6) Multiple use cases where the system can be implemented.

Disadvantages:

1) Depends on IP based surveillance infrastructure.
2) Chances of seldom false alarms.
3) Requirement of some level of human assistance, not fully automated.

We also tried to discover the server-based and serverless architectures for this purpose. The findings and observations are explained below:

Serverless: The primary preferred standpoint here is that you don't have to stress over load balancing, auto scaling approaches, and so forth. Serverless architecture utilizes AWS Lambda, which essentially runs a bit of code on request, and you are charged just for the time span the code is run [1][2]. Along these lines, for a less regular application, this advantages as there is no forthright cost or additional servers which costs you money. If there should be an occurrence of substantial scale applications, Lambda is again financially savvy as you can scale up in a flash to any level, without bringing about much cost, as Lambda is generally shoddy. In any case, the drawback is that the whole application must be overseen on stateless demands as sessions, and so forth can't be utilized as a part of Lambda. There are different administrations which we can use in blend to handle this issue, at the same time, it isn't so straight forward to exchange a server-based application to a serverless design, it requires finish upgrade of the whole framework engineering.

Server-Based: Here, you have to deal with the auto scaling arrangements, failovers, stack adjusting, and so forth. There are few administrations which can take the heap off your shoulders, yet at the same time, it requires a great deal of administrative help. The preferred standpoint here is, register escalated applications can be flawlessly keep running on server-based design, and extensive errands can be finished cooperatively by littler cases. In any case, for general application improvement, we have seen that serverless design suits well for versatile applications and is helpful as far as both cost and quality.

V. CONCLUSION

Security is a rising worry for some foundations and just introducing observing gadgets won't help settle the issue totally. Likewise, it is for all intents and purposes infeasible to physically screen every last area constantly. Taking a gander at the expanding pace of web availability development and considering the way that more territories would require reconnaissance in the coming years, we proposed the possibility of a cloud-based application that will utilize confront acknowledgment and will have the capacity to help people in situations like robbery, and so on.

REFERENCES

[1] JINESH VARIA, "ARCHITECTING FOR THE CLOUD: BEST PRACTICES", AMAZON WEB SERVICES WHITE PAPER JAN 2011.

[2] Khan R.Z., Ahmad M.O. (2016) Load Balancing Challenges in Cloud Computing: A Survey. In: Lobiyal D., Mohapatra D., Nagar A., Sahoo M. (eds) Proceedings of the International Conference on Signal, Networks, Computing, and Systems. Lecture Notes in Electrical Engineering, vol 396. Springer, New Delhi

[3] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuriaisingham," Security Issues for Cloud Computing", International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010.

[4] Shang-Hung Lin," An Introduction to Face Recognition Technology", Informing science special issue on multimedia informing technologies-part 2 volume 3 no 1-2000.

[5] Monjur Ahmed and Mohammad Ashraf Hossain," CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.