Scientific Journal Impact Factor (SJIF) : 3.518

International Journal of Modern Trends in Engineering and Research

ISSN (ONLINE) : 2349 - 9745

ISSN (PRINT) : 2393 - 8161

CLOUD BASED OUTSOURCED PATTERN MATCHING INFRASTRUCTURE FOR FACE RECOGNITION AND CURRENCY NOTE VALIDATION

Shreyas Kamath M G[1], Apeksha J[2] , Bhavana S Dixit[3], Vinay G R[4]and Vatsala B R[5]

[1,2,3,4]*Student, Department of Computer Science and Engg, NIE, Mysuru.*

[5]*Assistant professor, Department of Computer Science and Engg, NIE, Mysuru.*

Abstract— In applications that involve matching patterns like face recognition, fingerprint identification, conventionally, the algorithms used will process the input (like faces) and then the processed data used to match against a database. The notable characteristic of this model is the coupling of data processing and data matching within a single device/machine. With the advent of internet, web technologies and most revolutionarily that of IoT, there is a need for decoupling the various stages, phases and segments of data production, processing and acting. Following the same need for decoupling, this projects aims at developing a model in which pattern matching can be outsourced and using APIs, its services can be utilised by multiple entities independent of location, platform and underlying protocol stack. As the problem statement, this project attempts to provide a matching engine for the purpose of face recognition and fake currency detection. As a secondary feature, whenever a fake currency is detected, the location of the service request will be logged on the server to enable analytics on circulation of and also the origin of face currencies.

Keywords—Pattern matching, Cloud, Face Recognition, Currency validation.

I. INTRODUCTION

This project is aimed at building a cloud based pattern matching infrastructures that uses secure and scalable methods algorithms to detect whether the data points extracted and sent belong to a genuine currency note. The engine is useful in detecting fake notes in circulation and can be accessed by a smartphone application providing useful tool for a common user. It also provides face recognition and fingerprint matching services that can be accessed in similar ways. The intention behind developing such an engine is to modularize the entire process of pattern matching where feature extraction and matching happens together locally into independent modules that can interact using APIs. The project also makes use of custom made algorithms that would be best suited for the said mode of independent operation.

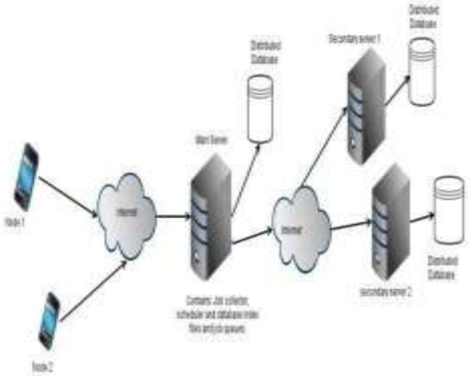

Fig 1 Architecture and Work flow

II. LITERARY SURVEY

Paper [1] focuses on the principle involved in the project viz the concept of Outsourced Pattern Matching. The various challenges, stages, obstacles involved in outsourced pattern matching is talked upon here and the comparison between native and outsourced models is also given. This paper proved to be a great source of information in this relatively new concepts. The paper [2] establishes the concerns with techniques used in public use of cloud resources where the identity management becomes very important. The paper [3] provides insights on the techniques used in fake currency note detection using image processing. The several stages like size normalization, gray scale conversion, image segmentation and background elimination are described in detail and are applicable for the project.

III. PROPOSED METHOD

The proposed system consists of a secure multi tier client-server architecture. There are several operations and events that occur at each tier and the capabilities and roles of each party involved differs from tier to tier. The operations classified as per tier are:
3.1 Tier 0-1 operations
3.2 Tier 1-2 operations

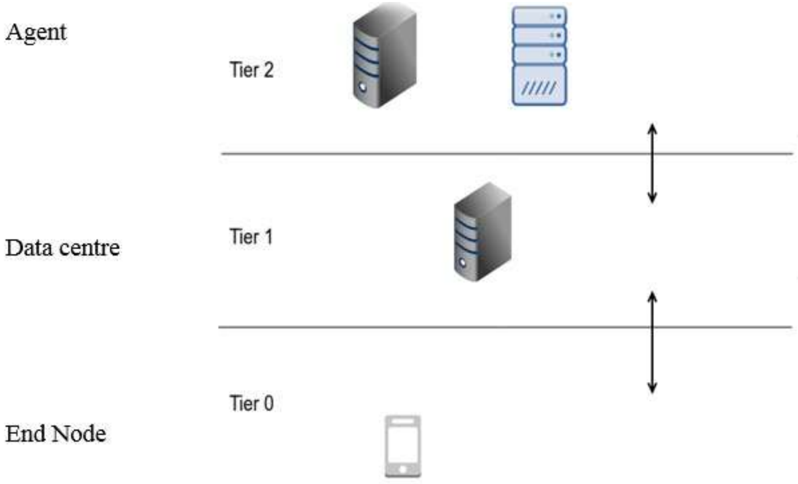

Fig 2 Tier Arrangement

3.1 Tier 0-1 operations

It is important to first identify the population of tier 0 and tier 1 before the tasks can be understood. The tier 0 is the unsecure zone, comprising of all the nodes that would like to avail the services of the infrastructure at varied levels of QoS and also comprises of all malicious nodes that have negative intents. Tier 1 comprises of agent servers which are maintained by the application that cater to requests the tier 0 devices and maintain logs of all transactions. Note that tier 1 devices only take requests from tier 0 devices and do not service it.
Due to the risks involved wrt security, the operations that are undertaken at this tier are:
3.1.1 Handshaking.
3.1.2 Logging.
3.1.3 Service request and acknowledgement.

3.1.1 Handshaking:

This is the mutual identification and acknowledgement of the two parties involved in communication where synchronization procedures might take place in case of time dependant systems.

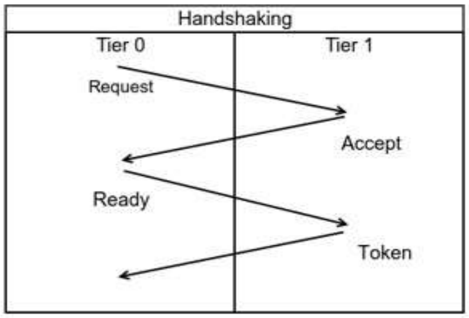

Fig 3 Handshaking between tier 0 and tier 1 devices.

The application infrastructure operates in two levels of QoS. Basic and Premium. In basic, there is no end-to-end encryption as this requires complex key management procedures. In premium level, at the initial registration stage, the key exchange takes place and the user node is given full security guarantee.

3.1.2 Logging

At the end of the handshaking operation, a unique token generated by the agent server is sent to the end node and the transaction is logged in both the end node and the agent server. This is for maintenance and review purpose. The unique token generated is never the same for any two transactions as it is generating by taking in both the time stamp at the time of the server request and a pseudo random number which is dynamically generated by the agent server.

3.1.3 Service request and acknowledgement

After the handshaking is done, the end node which has data to be sent to the matching engine on the application infrastructure specifies the *data type* using an agreed upon mapping between data types and numbers. Then, the data itself follows the ‘data type’ and these pieces of information are relayed onto the agent server. The agent server, upon receipt of these pieces of information, now has a formal *request* and acknowledges the request receipt. The results obtained at the end of matching process is then returned back to the end node from which the request originated.

3.2 Tier 1-2 operations

The parties involved here are the agent server and the tier 2 servers which actually store all thedatabase and the matching scripts that take the feature data sent by the end nodes. This is the zone which has to be secured the most from several types of attacks. Keeping this in mind, the agent servers are not given write access to this tier and only the application DBAs can add, modify or delete data on this tier.

The operations that take place here are:
3.2.1Data reconfiguration
3.2.2Matching and response

3.2.1 Data reconfiguration

This refers to altering data and further processing pre-processed data for the purpose of matching and might also involve database access.

3.2.2 Matching and response

Once the data reconfiguration is done, the database access and matching process takes place to find the desired result as per the request type. At the end of this stage, the obtained match, if any, are returned to the agent server who can then inturn return it back to the node from which the request originated.

IV. IMPLEMENTATION RESULTS

A full scale implementation is just approaching completion and a thorough analysis and comparison of results is to be done.

V. CONCLUSION

Having designed a secure model for a cloud based pattern matching infrastructure, the design has been implemented using MongoDB as the primary database. The open APIs of the infrastructure makes it readily integratable with any feature matching application having its own feature extractor.

REFERENCES

[1] Outsourced Pattern Matching, Security and Cryptography Laboratory, EPFL, Switzerland, Faculty of Engineering, BarIlan University, Israel, Department of Computer Science, Aarhus University, Denmark.

[2] Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing, Qian

[3] Wang1 , Cong Wang1 , Jin Li1 , Kui Ren1 , and Wenjing Lou2 1 Illinois Institute of Technology, Chicago IL 60616, USA.

[4] Fake Currency Detection Using Image Processing and Other Standard Methods, Anil Neerukonda Institute of Technology And Sciences (ANITS), Visakhapatnam.