Secure Biometric Image Retrieval in IoT-Cloud

Zaid Ameen Abduljabbar[1,2], Hai Jin[1], Ayad Ibrahim[2], Zaid Alaa Hussien[1,3],
Mohammed Abdulridha Hussain[1,2], Salah H. Abbdal[1], Deqing Zou[1]
[1]Cluster and Grid Computing Lab, Services Computing Technology and System Lab
School of Computer Science and Technology
Huazhong University of Science and Technology, Wuhan, 430074, China
[2]University of Basrah, Basrah, Iraq
Email: zaidalsulami@yahoo.com, hjin@hust.edu.cn
[3]Southern Technical University, Basrah, Iraq

***Abstract*—Within the IoT-cloud, security has a very significant role to play. One of the best means to safeguard confidentially, security and privacy of a biometric image is through encryption. However, looking through encrypted data is a difficult process. A number of different techniques for searching encrypted data have been devised, but certain security solutions may not be used for smart devices within an IoT-cloud, and this is due to the fact that such solutions are not lightweight. In this paper, we present a lightweight scheme that provides the privacy-preserving biometric image search, which is a special case of *content-based image retrieval* (CBIR). A fusion of homomorphic encryption, cosine similarity and garbled circuit-based approaches are adopted in our scheme to achieve the best performance while simultaneously ensuring the privacy of the biometric image, and protection of any data access patterns and the user's input query. We conduct several empirical analyses on real image collections to demonstrate the performance and security of our work.**

***Keywords*—IoT-cloud, privacy-preserving CBIR, similarity measure, SURF**

I. Introduction

The IoT heralds a new field of computing in which every conceivable object is provided with or joined to a smart device that permits data collection and communication via the Internet. Smart mobility devices in the IoT have changed the daily lives of humans as these devices create, process, and save massive amounts of data that are proliferating at an evidential degree worldwide. Simply stated, in 2014, the numbers of users who used smart devices was more than 1.2 billion people globally [1].

Due to great advances in cloud computing technologies, several companies like Google, Microsoft, and Amazon have successfully provided their smart devices users with large-scale resources in the pay-as-you go style. Such resources include: software, hardware, and data-storage [2]. Despite the cloud technical advances and economic benefits, moving particularly vulnerable or important information, like biometric image to cloud servers that have not been deemed secure, presents an issue when safeguarding user's private biometric image. In order to deal with unsolicited attempts of access, smart devices users generally choose to encrypt such data prior to outsourcing it to the cloud. Nevertheless, this presents a notable barrier when traditional encryption services are used and when looking for and through encrypted data. Additionally, despite smart devices computing power increasing, it remains behind the capacity of personal computers.

In recent years, several of *searchable encryption* (SE) methodologies have been developed [3–7] that facilitate selective retrieval of encrypted documents by means of keyword searches. Within these systems a user would send a secured keyword to look for specific encrypted text documents. Conversely, other modern *informational retrieval* (IR) systems, such as Google, have introduced an original technology that allows clients to send an image as a query, search through the images that are retained on the database in question, and identify those images with comparable visual content. Original technological processes are referred as CBIR. Thus, biometric image matching is a special case of CBIR. Therefore, the development of a searchable encryption scheme to deal with biometric image-based searches in a proficient and precise manner is recommended.

As a result, a lightweight bio-image matching scheme is needed with regard to the cloud environment in the IoT. Furthermore, biometric image privacy-preserving is among the most essential of all security services regarding the accounting for all security applications and security systems. Nevertheless, interest and recourse for such security services are not forthcoming concerning smart devices communication within IoT-cloud.

Simply stated, in some cases, protecting the privacy of biometric images during the matching process is necessary. Consider the following example to determine the importance of a security issue in IoT-cloud. Suppose a security agency is outsourced a biometric images related to a potential terrorist suspect or sensitive images to *cloud servers* (CSs) using the appealing benefits of clouds. The security agency agents may wish to check whether bio-images related to the suspect can be found in cloud server databases. In particular, such agents may use smart devices to suit the nature of their work in prosecuting suspects and mobility during labor. However, for security purposes, neither the agency nor the agents want to reveal their bio-images and query, respectively, unless a need access by authorized agents. One way to identify such a need is to detect similarities between the agency's agent query (in the form of bio-image) and the cloud database. Once the need for matching is verified, the cloud server can send only similar bio-images.