A CONCEPTUAL DATABASE AUDITING MODEL USING RETINAL FUNDUS IMAGE DETECTION-BASED AUTHENTICATION

Karen B. Alexander*

Abstract---

Database Auditing is one in every of the key issues as so much as information security is bothered. We have a tendency to introduce a specific auditing framework that uses a biometric idea of human eye-retinal structure detection as a way of authentication determines whether or not this information adheres to disclosing policies, so as to form the data secure from malicious attackers. Retinal identification is that the most secure and correct technique since it's not possible to alter the structure throughout human life by plastic surgeries and alternative ways. The audit element of this model accepts audit expressions and returns all queries that are termed as "suspicious" that accessed the desired knowledge throughout their execution.

Keywords--- database auditing, database authentication, biometrics, Retinal fundus image, retinal anatomy.

* Department of Computer Science, Sipna College Of Engineering And Technology, Amravati

I. Introduction

Auditing the changes to the information is crucial as a result of identifying malicious behaviors, maintaining knowledge quality, and improving system performance. So as to enhance the protection of the info during a information we offer a framework that applies the biometric idea of human eye-retinal detection primarily based authentication and determines whether or not this information adheres to revelation policies. Users formulate audit expressions to specify the (sensitive) knowledge subject to revelation review. Associate degree audit part accepts audit expressions and returns all queries that area unit termed as suspicious, that accessed the required knowledge throughout their execution. The overhead of our approach on question process is little, involving primarily the work of every question move on with different minor annotations. Information triggers area unit accustomed capture updates for the backlog information. At the time of audit, a static analysis part selects a set of logged queries for any analysis. These queries area unit combined associate degreed remodeled into an SQL audit question that once run against the backlog information, identifies the suspicious queries expeditiously and exactly. Whereas some systems area unit designed for acceptable personal passwords, cards, keys etc. some others cash in of exploitation identity verification. Researchers area unit within the verge of developing varied strategies for unambiguously recognizing folks primarily based upon one or additional intrinsic physical characteristics of physical structure within the space known as life science. These developed identification systems area unit largely used in access management systems. Among the biometric strategies, like finger print, hand palm, ear, voice recognition, and digital signature, face recognition and iris recognition etc, retinal identification is one among the foremost secure and correct strategies since it's not possible to alter the retina throughout human life via plastic surgeries and different strategies, that isn't the case for finger prints detection case.

A. The retina anatomy

A fundus camera shows the retinal structure, forty millimetre skinny layer of cell at the rear of the eyeball as shown in Fig. 1. There exists a circular to oval shaped white space activity regarding a pair of *1.5 millimetre across the optic head that is found principally at the middle, however reckoning on the conditions, whereas taking the image, it can be settled on either right or left aspect of the image [1,3]. The cranial nerve contains the neural structure cell axons running to the brain, along with the incoming blood vessels opening into the tissue layer to vascularize the retinal layers and neurons. This type of a morphologic structure of tissue layer

image is employed to find major blood vessels spreading all round the retina ranging from blind spot, and different elements. Mostly, all retinal identification systems use these options. The macula, seen as oval-shaped, blood vessel-free red spot, is around settled four.5–5 mm, or 2 and a 0.5 disc diameters off from blind spot [2].

II. Concerned work

Many researches are done from information security perspective. Several database systems have thought of auditing changes in an exceedingly database exploitation RFID ideas, IP address tracing yet as different security tools. Exploitation retinal pictures taken from people, retinal identification is utilized in environments like nuclear analysis centers and facilities, weapon factories, wherever extraordinarily high security measures square measure required [5]. The prevalence of this methodology stems from the very fact that membrane is exclusive to each soul and it might not be modified throughout human life. One factor that is closely associated with compliance is that the privacy principle of restricted revealing, which suggests that a information should not communicate personal info outside base for any reasons apart from those that there's consent from the data subject. Clearly, these duo conditions depict that they're complimentary [6]. This principle of restricted revealing comes into play at that point once any question is dead against the information, whereas demonstrating compliance is post issue and is bothered with showing that usage of the information so discovered restricted revealing in each question execution indeed observed limited disclosure in every query execution.

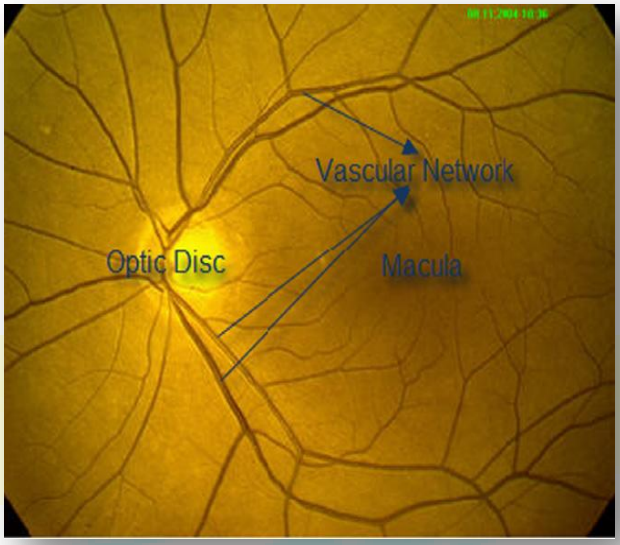

Fig 1. Retina anatomy

III. Proposed work

The planned data audit system satisfies some vital properties:

- Non-disruptive: this system puts stripped burden on question method.
- Fast and precise: this system is in an exceedingly position to quickly and specifically establish all the queries that accessed the required data.
- Fine-grained: this system is possible to audit every single field of a selected record.

This planned audit system satisfies the on high of desired properties. Figure a pair of shows the final style of our system [4]. As the simplest way of authentication, the data user will have a singular identification that's that the retinal structure. As way as retinal detection is concerned, this system consists of 2 major modules that are: vessel segmentation module, and human identification module. the foremost steps involved in our Identification system area unit (1) segmenting blood vessels, (2) extracting background image, (3) investigation degenerated areas inside the retinal image, (4) eliminating degenerated areas of the vessel structures if necessary, (5) applying scale, rotation and translation tolerance methods to achieve a scale, rotation and translation freelance identification system, (6) scrutiny the vessel structures of the sample and keep footage, conniving the foremost vessel matches for this sample line, (8) conniving the

similarity measures between the sample and keep pictures, that's used to seek out the foremost similarity worth. Finally, the identification result's used as a key in an exceedingly table at the side of the privilege details. Throughout the normal operation on the data, the string of every question processed by the data system is logged at the facet of some annotations just like the time once the question was dead, the precise time once the user submitted the question, and thus the query's purpose. this system uses data triggers to capture and record all updates to all-time low tables in backlog tables for maintaining the state of the data at any past purpose in time. choose (read) queries, or say, statements that area unit typically predominant; do not appear to be thought of to be written to the backlog data. To perform this system of auditing, the auditor performs the formulation of audit expressions that declaratively specifies the data of interest. Audit expressions area unit designed to be the image of the SQL queries, so allowing audits to be performed at the extent of a private cell of a table. The audit expressions are processed by the audit question generator that performs a static analysis of the expression initial to choose a collection of logged queries which may probably disclose the required data. Next, it combines Associate in Nursing and transforms the chosen queries into an audit question by augmenting them with extra predicates derived from the audit expression. This audit question, that's expressed in traditional SQL, once run against the backlog data yields the precise set of logged queries that accessed the chosen information [6].

The indices on the backlog tables build the execution of the audit questioning faster as potential. therefore this system is more practical from security side. There are refined ways that within which the combination of the results of a series of queries might reveal sure data. as an example, just in case of a statistical information literature [7], there's a discussion regarding how the individual data is deduced by running many combination queries and therefore the information security literature [3] shows however covert channels is wont to leak data. we have a tendency to limit ourselves to the matter of decisive if the required information was disclosed by a single query once that query is taken into account in isolation. we have a tendency to conjointly assume that the queries don't use outside information to deduce data while not detection. The SQL queries we have a tendency to contemplate comprise one choose clause. an oversized category of queries (including those containing existential sub queries) is regenerate into this type Specifically, we have a tendency to contemplate queries containing choice, projection (including distinct), relational join, and aggregations.

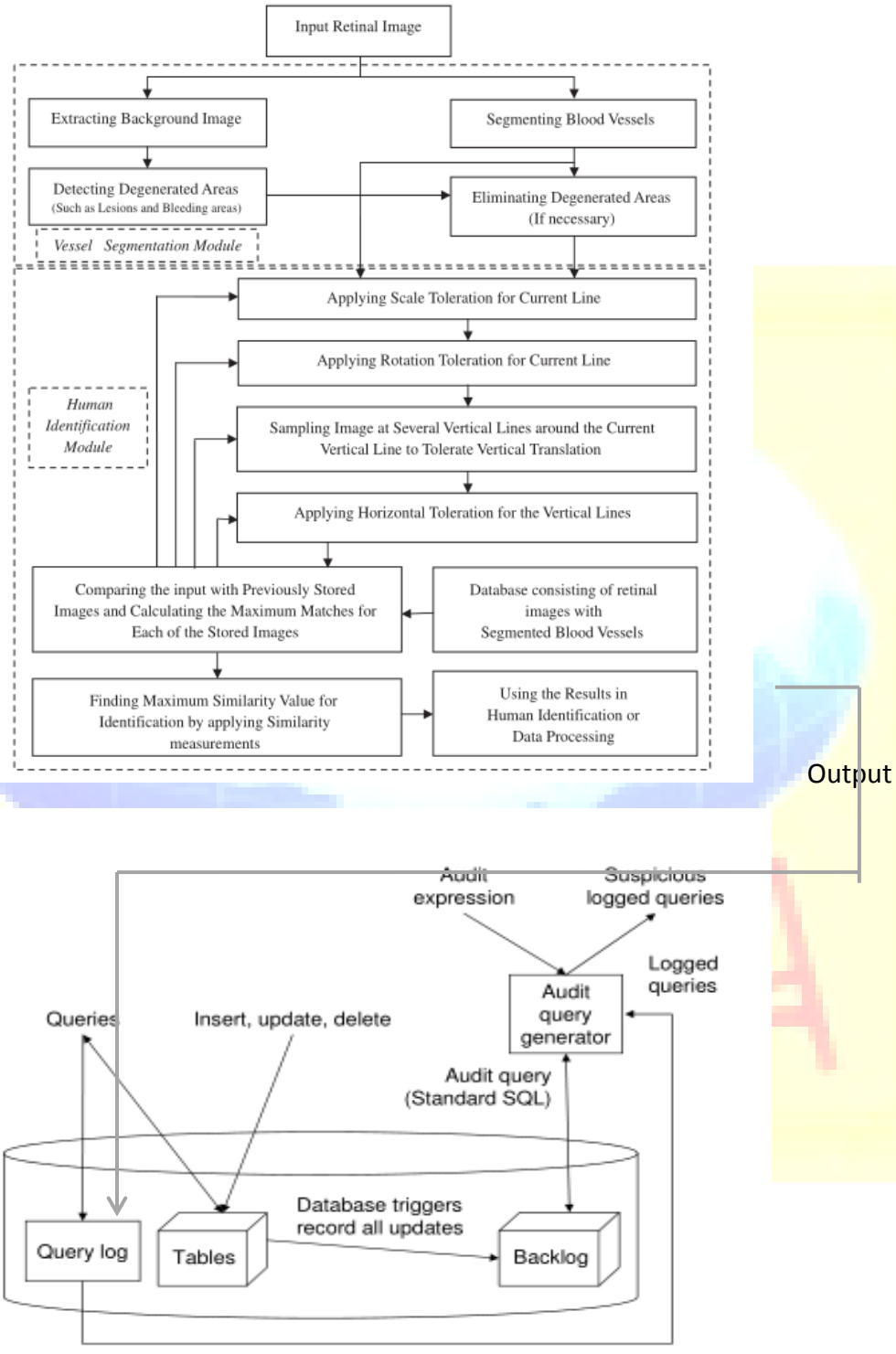

Fig 2. Proposed system architecture

IV. Conclusion

Thus within the above paper we've given a short summary of considering a retinal primarily based authentication for an efficient information security side permitting the auditor to effectively audit the information so as to trace any mischief within the information stored within the information itself thereby serving to the database administrator to effectively notice the perpetrator for his/her malicious and ruining activity.

Additional contributions embody a carefully designed and enforced system that meets the look goals known within the introduction: Convenient: This audit system reuses the acquainted SQL syntax, providing a well-known, declarative and expressive means that for specifying the info whose revelation is subject to review. Fine-grained: this technique permits the auditor to specify even one field of a record as subject for review. quick and precise audits: Our system combines the audit expression with logged queries into an SQL audit question that examines only the precise information necessary to determine suspicion. guided by our implementation and experimentation with varied backlogging and indexing methods, we tend to proposed system structures to support efficient audit question execution. Non-disruptive: Our system imposes solely low burden on the execution of most queries. instead of logging query results or the tuples accessed by a query, it logs the query strings, whereas update operations require some extra backlog database maintenance.

References

[1] Hill, R. B. (1999). *Retinal identification*. In A. Jain, R. Bolle, & S. Pankati (Eds.), Biometrics*: Personal Identification in Networked Society (pp. 126)*. Berlin, Germany: Springer.

[2] Afariani, H. (2003). *Human identification based on retina image*. Master of science thesis in biomedical engineering, KNT University of technology.

[3] Yamamoto, S., Yokohuchi, H., & Suzuki, T. (1974). *Image processing and automatic diagnosis of color fundus photographs*. In Proceedings 2nd international joint conference on pattern recognition, Copenhagen (pp. 268–269).

[4] N. Adam and J. Wortman. *Security-control methods for statistical databases*. ACM Computing Surveys,21(4):515–556, Dec. 1989.

[5] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu. *Hippocratic databases*. In 28th Int'l Conference on Very Large

Databases,Hong Kong, China, August 2002.

[6] S. Castano, M. Fugini, G. Martella, and P. Samarati. Database Security. Addison Wesley, 1995.

[7] N. Adam and J. Wortman. *Security-control methods for statistical databases*. ACM Computing Surveys,21(4):515– 56, Dec,1989