Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/12361
DOI URL: http://dx.doi.org/10.21474/IJAR01/12361

ISSN NO. 2320-5407

*RESEARCH ARTICLE*

# CONSISTENCY OF PRIVACY VIEWS ON HIPPOCRATIC AND MULTILEVEL DATABASES USING SMART CONTRACTS

**A. Anandita Iyer[1], R.K. Shyamasundar[2] and Umadevi K. S.[3]**
1. Student, School of Computer Science & Engineering, VIT, Vellore.
2. Professor, Indian Institute of Technology, Bombay.
3. Professor, School of Computer Science & Engineering, VIT, Vellore.

## Manuscript Info

*Manuscript History*
Received: 25 November 2020
Final Accepted: 28 December 2020
Published: January 2021

## Abstract

Nowadays the whole world is immersed in data. Starting from creating the data, using the data, sharing the data, everyone has control of their respective data. Even the companies rely highly on data as all of their storage and analysis have been computerized. In most traditional methods, the database which is being deployed is deemed trustworthy. But the threat always persists no matter how secure the database is. Attackers perform various types of attacks possible to gain access, tamper or perform any kind of compromising action on the database which will hamper the working of a company/individual. So, the goal is to achieve security against those attacks and additionally avoiding users to obtain information which they are not authorized to. However, there exists a series of relational data such as medical databases where there are two or more parties involved in a database and the trust factor automatically takes a hit.

In this paper, I propose a model that provides authorization, confidentiality, accessibility and privacy for a healthcare database.

## Introduction:-

These days security is one of the significant difficulties that individuals are confronting everywhere throughout the world in each and every part of their lives. Data or information is a significant resource in any organization. It is an important aspect to eliminate redundancy, prevent breaches and protect confidentiality. Practically all companies whether social, legislative, instructive and so forth have digitized their frameworks and other operational capacities. They have kept up the databases that contain the pivotal data as it will be easy to access (data will be organized) and safeguard all their data with proper measures. So, database security is a genuine concern as they can be hacked through their vulnerabilities. Hackers can compromise a database by gaining illegal access or by running any arbitrary code on the database.

Ensuring the classified/delicate information put away in a storehouse is really in need of database security, needed nowadays. For e.g. ensuring sure strong credentials and using appropriate measures to prevent unauthorized access will be one of the ways to ensure security. It manages securing databases from any type of illicit access, till

**Corresponding Author:- A. Anandita Iyer**
Address:- Student, School of Computer Science & Engineering, VIT, Vellore.

managing risk at any level. Database security requests either permit or decline client activities on the database and the articles embedded in it.

Organizations are in need of privacy of their databases as they want to safeguard their data from various privacy attacks such as leakage of personal details, so as they don't permit the unapproved access to their information/data. They additionally request the affirmation that their information is ensured against any malignant or incidental change. Information insurance and secrecy are the primary security concerns of the personnel working in the company and the company is obligated to provide those measures to safeguard the data.

Database security [2] is not an isolated problem - in a broad sense it is a total system problem. Database security depends not only on the choice of a particular database management product or on the support of a certain security model, but also on the operating environment, and the people involved. Database security has been subject to intensive research for decades together but remains as one of the major and fascinating research areas as the technology evolves. It is expected that the advancement in the technology will introduce new vulnerabilities to database security.

In this paper, Multilevel Databases and Hippocratic databases are used to check privacy breaches. Since the views on relational database systems [3] mathematically define arbitrary sets of stored and derived data, they have proposed a way of handling context- and content dependent classification, dynamic classification, inference, aggregation, and sanitization in multilevel database systems.

Inspired by the tenet of “Hippocratic oath” [4] preserving privacy, the future database systems must include responsibility for the privacy of data they manage as a founding tenet and enunciate the key privacy principles for such Hippocratic database systems. Privacy is the right of individuals to determine for themselves when, how and to what extent information about them is communicated to others. Privacy concerns are being fueled by an ever-increasing list of privacy violations, ranging from privacy accidents to illegal actions.

**Literature Survey:-**

Information to any company is a most important property. Security of delicate information is constantly a major test for a company at any level. In the present technological world, databases are helpless against hosts of assaults. Right now, significant security issues confronted databases are recognized and some encryption techniques are talked about that can assist with diminishing the assaults chances and ensure the privacy of delicate information.

It has been inferred that encryption gives classification yet gives no confirmation of honesty except if we utilize some advanced mark or Hash work. Utilizing solid encryption calculations diminishes the presentation. The ideas portrayed in [8] speak to a beginning stage for a model that ventures into new regions of database security. By acquainting rule-based grouping will oblige the entrance classes of the information, the model gives a system, tending to some derivation issues, conglomeration, sanitization, setting and substance subordinate arrangement, and dynamic characterization. There are, nonetheless, numerous troublesome issues that must be understood before these ideas can be acknowledged in a genuine framework.

[9] Have considered how to bargain secure data in factual databases whose inquiries utilize self-assertive trademark equations to choose subsets of records.Their outcomes apply to countless genuine database frameworks, including social ones, for example, System R or INGRES. The question framework will react to an inquiry q(C) just if the size of the question set is in the range [k, n - k], where n &gt; 2k is the quantity of records in the database. They thought about two sorts of trackers, which are trademark equations that help figure the values of “unanswerable” inquiries.

They have created [25] a multilevel secure object-oriented data model, SORION, which has developed from the ORION object model. They have additionally portrayed the fundamental highlights of SORION with models. Like ORION, SORION depends on the class, object, example variable and technique build. Moreover, the set build, IS-A chain of command and IS-PART-OF progressive system are likewise bolstered by SORION. They have likewise talked about required security in an item arranged framework dependent on SORION. They originally portrayed a staggered security arrangement and afterward talked about issues, for example, taking care of poly-launch and dealing with the surmising issue.

An exact model of the security issue for databases has been introduced [12]. Right now, they had the option to show how to control the questions, a client could make so as to prevent him from trading off the database. While they did this just for inquiries about midpoints and medians, they can stretch out the model to deal with questions of different sorts. This model offers access to various intriguing combinatorial issues which have applications to issues of appropriateness to originators or databases. While they have exhibited a prologue to issues right now, various related issues stay open.

Grouping remarks and cryptographic checksums [10] can be applied to finished relations, records, properties, or individual information components inside a record. Applying checksums at the information component level permits the database framework to return just that information expected to react to an inquiry. The cryptographic shortcomings regularly present with component-based checksums can be overwhelmed by utilizing an alternate key with every checksum. There are, in any case, security purposes behind requiring the database framework to consistently return total records. On the off chance that information utilized by the database framework during record choice has a more significant level than that returned in the reaction, derivation issues can emerge. Returning total records, additionally ensures against the danger of the framework returning wrong outcomes.

The paper [24] built up the standard arbitrary information random technique which may actuate genuine inclinations into client inquiries, if secret factors might be utilized for record choice. Since this strategy is one of the most broadly known strategies for accomplishing security in measurable databases, it is essential to scan for changes to RDP, and\or look for different other options. They have introduced here a total answer for the predisposition issue in the multivariate ordinary case. Besides, they guessed that this arrangement ought to likewise function admirably in non-normal cases and affirmed this through a reenactment study. Implementing information insurance implies defending information from unapproved or ill-advised exposures or changes.

In the paper [6], they have secured parts of two access control strategies. Optional approaches, administer the entrance by clients to information based on the clients' character and decide, indicating each subject permission on each item. Compulsory strategies, enlivened by the BellLaPadula model, administer the entrance by clients to information based on orders allotted to them. There have been broad investigations on elective queueing disciplines with lock-based simultaneousness control and planning of ongoing exchanges. While a large portion of the outcomes [3] depend on recreation, some of strategies have been executed on a tried framework.

These investigations give knowledge into a significant number of the issues experienced in the plan of RTDBS(Real time database management system). Be that as it may, the outcomes detailed in the writing are inadequate. For instance, despite the fact that planning imperatives and criticalities are two significant factors in determining ongoing exchanges, the connection between the two variables and their consolidated impact regarding framework execution has not been tended to inside and out. It is hard to look at different planning calculations without an appropriate benchmark that is illustrative of utilizations. Since inquiry about on RTDBS is still in its earliest stages, none of the realized benchmarks tends to exchange preparing in a constant situation.

One can see the assortment of all databases as an accumulated database to which just the NSO has some advantaged access for measurable inquiries. This is the determination that ought to be executed. Specifically, the NSO [21] ought not gain proficiency with any individual organization information. Secure multi-party calculation permits to unravel this problem, i.e., to execute this determination. Every database assumes the job of a player in a safe MPC convention. All the more for the most part, one can characterize discretionary inquiries on such or for all intents and purposes totaled databases, and they can be assessed with no other data spilling from the individual databases.

There is a developing enthusiasm for database security and the methodologies revealed, right now [22] show that there has been extensive achievement in creating answers for the issues in question. Open intrigue has expanded dramatically, however it is as of late that the issue of security outside the exploration network gets a need of appropriately mirroring its significance. Databases of things to come must guarantee the protection of the information subjects that they store data on [1]. The security usefulness offered by current business database items isn't sufficient to implement protection consistency.

Multi-level secure database frameworks are another kind of information stockpiling framework. These are frameworks that help the grouping of information questions inside an element, e.g., a record with properties at different degrees of security. This frequently forces the poly-instantiation [19] of a trait esteem. Much of the time the demands made by clients with more significant levels of exceptional status would be reacted to, by indicating all the launches of the information at or underneath their degree of security. Such databases hold the capability of inferential security break as examined right now some extra wellsprings of data.

Little work has been done right now; extensive models of inferential security and choice models are expected to take care of the information security issues in the staggered secure database situations. It has been recommended that joining man-made consciousness induction motors with information security control strategies would be valuable. This methodology has been utilized generally in a non-electronic structure by the U.S. Evaluation Bureau through the choice structure of what information is discharged and to whom. It isn't evident that a computerized variant of these deduction motors will be any increasingly effective in giving security to the information.

Propelled by the Hippocratic Oath, they [2] displayed an array of database frameworks that assume liability for the protection of information they oversee. They articulated the key security rules that such Hippocratic databases should bolster and displayed a strawman structure [2] for a Hippocratic database. At last, they distinguished the specialized difficulties and issues presented by the idea of Hippocratic databases. Restricted divulgence is a crucial part of information security, in the board framework. The paper [11] proposed a versatile engineering for implementing constrained divulgence rules and conditions at the database level, and they introduced a few models for cell-level restricted exposure authorization in a social database.

Application-level arrangements can't process subjective SQL inquiries productively. By pushing the requirement down to the database, they increase improved execution and inquiry power. This instrument can be sent without adjusting inheritance application code or existing database constructions. they demonstrated that the exhibition overhead of database-level security requirement is little, and intermittently the overhead is more than balance by the presentation picks up through record separating.

Blockchain owes its name to how it functions and the way in which it stores information, to be specific that the data is bundled into squares, which connect to form a chain with different squares of comparable data [26]. It is this demonstration of connecting hinders into a chain that makes the data put away on a blockchain so reliable. When the information is recorded in a square it can't be adjusted without changing each square that came after it, making it difficult to do as such without it being seen by different members on the system.

Bitcoin is a digital currency. It is a decentralized advanced cryptocurrency [14] without a national bank or single head that can be sent from client to client on the shared bitcoin organization without the requirement for delegates. Exchanges [16] are checked by organized hubs through cryptography and recorded in an open disseminated record called a blockchain. Bitcoins are made as a compensation for a procedure known as mining. They can be traded for different monetary forms, items, and administrations.

Bitcoin is an online correspondence convention [7] that encourages the utilization of a virtual cash, including electronic installments. Bitcoin's standards were structured by engineers with no obvious impact from legal advisors or controllers. Instead of store exchanges on any single server or set of servers, Bitcoin is based on an exchange log that is conveyed over a system of taking an interest PCs. It incorporates instruments to remunerate legit support, to bootstrap acknowledgment by early adopters, and to prepare for convergences of intensity. Bitcoin's plan takes into account irreversible exchanges, an endorsed way of cash creation after some time, and an open exchange history.

SmartContracts [5] are PC programs that can be reliably executed by a system of commonly doubting hubs, without the intervention, confided in power. On account of their versatility to altering, smart contracts are engaging in numerous situations, particularly in those which require moves of cash to regard certain concurred rules. These contracts can deal with enormous quantities of virtual coins [20] worth several dollars each, effectively making monetary motivating forces sufficiently high to draw in foes. In contrast to customary appropriated application stages, SmartContract stages, for example, Ethereum work in open (or consent less) systems into which discretionary members can join.

Smart Contracts are characterized as understandings [23] wherein execution is mechanized, for the most part by PCs. Such Contracts are intended to guarantee execution without plan of action to the courts. Computerization guarantees execution, regardless, by extracting human tact from contract execution. One case of a smart contract is the unassuming candy machine. On the off chance that the machine is working appropriately and cash is embedded into the machine, at that point a contract is available to be purchased and will be executed naturally. This is a Smart

Contract. Such a contract represents no lawful issues if the machine were to administer pop, however legitimate inquiries emerge if the machine rather apportions heroin. Should laws be passed to boycott candy machines since they can be utilized to encourage unlawful finishes? Or then again should their utilization be directed ex post?

Interoperability challenges between various supplier and medical clinic frameworks represent extra boundaries to viable information sharing. This absence of composed information the executives and trade imply wellbeing records are divided, as opposed to strong [17]. Patients and suppliers may confront huge obstacles in starting information recovery and sharing because of monetary motivators that empower "wellbeing data obstructing." An ongoing ONC report [27] subtleties a few models on this theme, specifically wellbeing IT engineers meddling with the progression of information by charging extreme costs for information trade interfaces.

Other than that, there are certain challenges with the Hippocratic databases such as
Efficiency, Limited Collection, Limited Retention, etc.

**Inference from the literature survey:**

Multilevel secure RDBMS use obligatory access control to forestall the unapproved divulgence of significant level information to low-level clients. It is likewise important to prepare for the risk to privacy that can emerge from implementing database trustworthiness constraints [6] across information from various security levels.

**Issues encountered:**

Assume that a client with a low security level wishes to embed the tuple. From an absolutely database viewpoint, this addition must be dismissed in light of the fact that it damages the essential key imperative. In any case, dismissing this supplement could be adequate to bargain security as the client with low security level could induce that the database has a higher security level.

Polyinstantiation is an answer for this issue. It grows the idea of essential key to incorporate the security level with the goal that more than one tuple may have the equivalent clear essential key on the off chance that they are at various security levels.

Notwithstanding ensuring against deduction, polyinstantiation is likewise valuable to forestall disavowal of administration to authentic clients just as to secure against capacity secret channels. Undercover channels use these framework factors and ascribes to flag data.

Other than that, there are certain challenges with the Hippocratic databases such as
Efficiency, Limited Collection, Limited Retention, etc.

To incorporate all the above I have referred to the following design.

**System Design:**

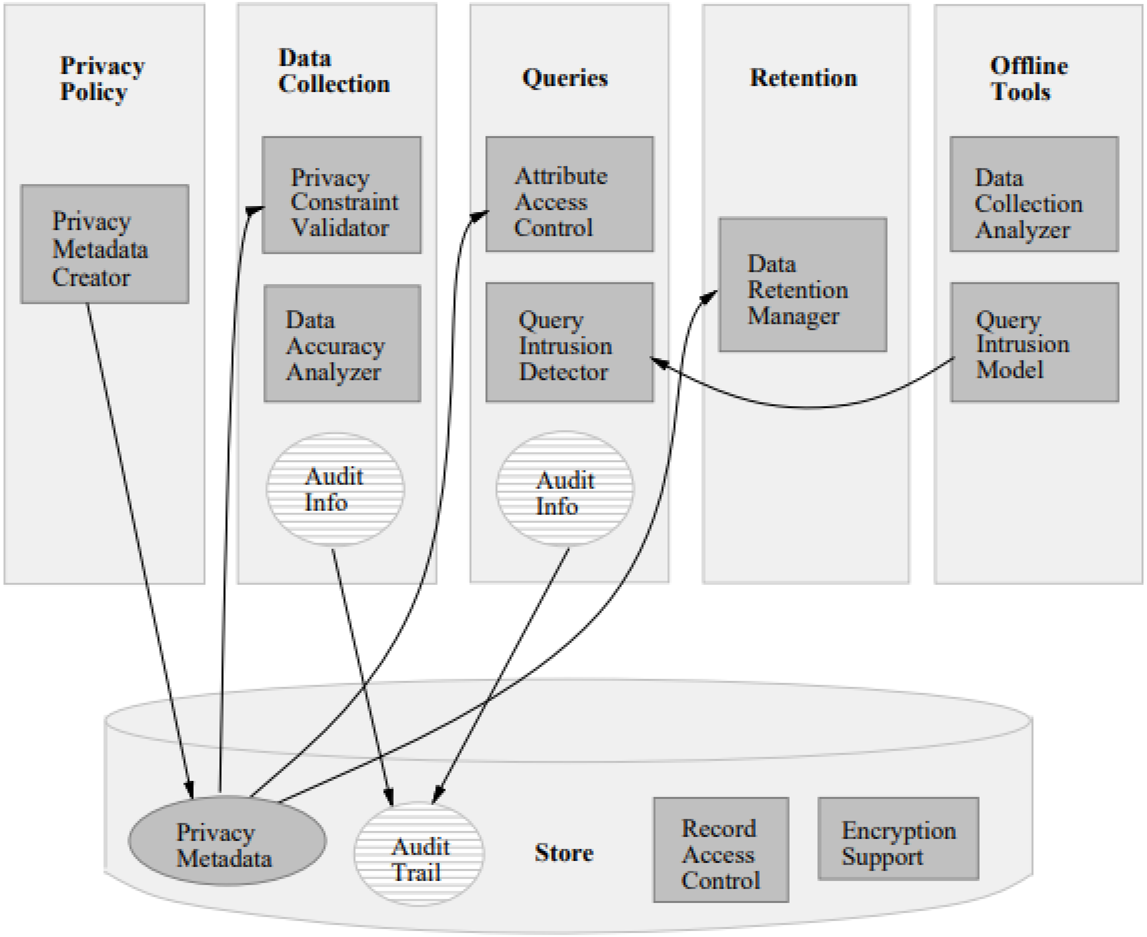


**Fig 1:-** Strawman Design. [1].

Layer 1 is a security portion executing the Bell and LaPadula model. The portion underpins required security (mystery and trustworthiness) for single-level articles, (for example, documents, and so on.), subjects (clients, forms, and so on.), procedure and memory of the executives, and other asset directors. As for the view model, this layer bolsters the hidden physical portrayal of the database, client clearances, and login get to class. The part will be utilized to execute the higher layers.

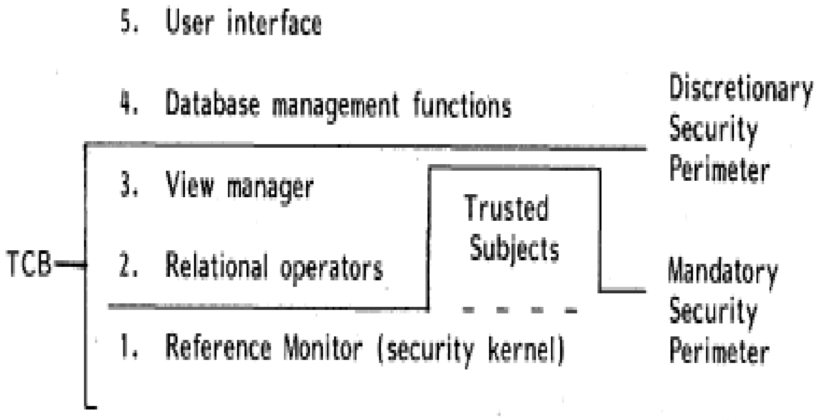

5. User interface
4. Database management functions
3. View manager
2. Relational operators
1. Reference Monitor (security kernel)
Trusted Subjects
TCB
Discretionary Security Perimeter
Mandatory Security Perimeter

**Fig 2:-** System Decomposition. [26].

Layer 2 executes single-level base relations. This layer gives the social administrators just as other numeric or representative administrators given by the database framework (e.g., for registering insights) and executes the entrance techniques, including record structures.

Layer 3, the view chief, executes views. This layer gives the mapping of staggered views onto the single-level base relations of Layer 2, and decays exchanges on staggered views into single-level exchanges on the single-level base relations of Layer 2. Layer 3 backings characterization limitations, including inference and purification rules, collection iterative, and optional access controls (e.g., get to control records or client/gathering/world vectors). It is liable for watching that a lot of limitations are finished and predictable, and  for allocating - get to classes to the information (through approaches Layer 1).

As appeared in the figure, I have recognized unmistakable security edges regarding compulsory and optional security. The TCB incorporates both. In spite of the fact that characterization and total requirements are inside the TCB, they are outside the reference screen since they are possibly very intricate and depend somewhat on the right execution of the social administrators.

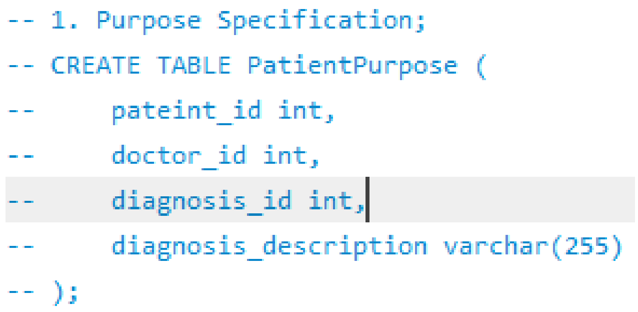
Layer 4 gives information about the executives capacities that are not required by the lower layers. Despite the fact that we are not yet sure what capacities can dwell right now, applicants can exchange the executives, parsing and question advancement, and circulate databases to the executives. We will likely place however much of the database framework as could reasonably be expected outside the TCB.

Layer 5 gives the UI. It compares to the application layer. Each progressive layer in the TCB (through Layer 3) presents further maxims, in this manner confining while at the same time improving the approach of the framework. Despite the fact that the higher layers can't give expanded access to the information past that given by the reference screen, by supporting characterization down to the component level, rule-based task of security marks, disinfection, induction rules, and total limitations, the higher layers can offer expanded help for security while permitting information to be characterized at its actual access class and not become over-arranged.

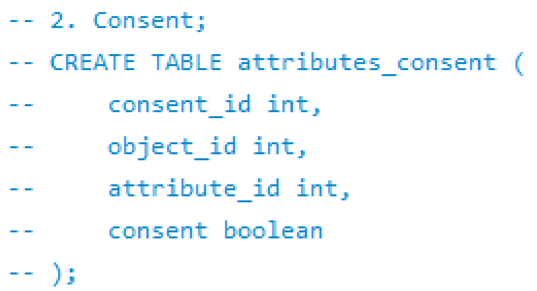
**Tools and Modules Involved:**

a. RStudio for analyzing data.
b. SQL Workbench to work ad query with databases.
c. Node.js and ganache-cli.
d. RWFM Labels Creation and Utilization.

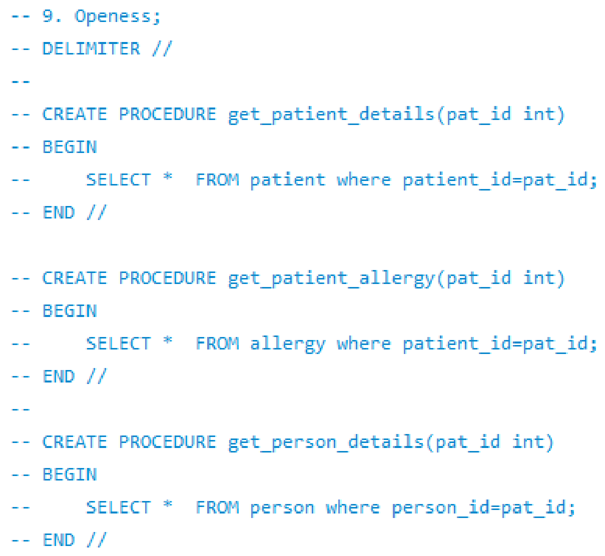
**Test views and SQL Function Modules;**



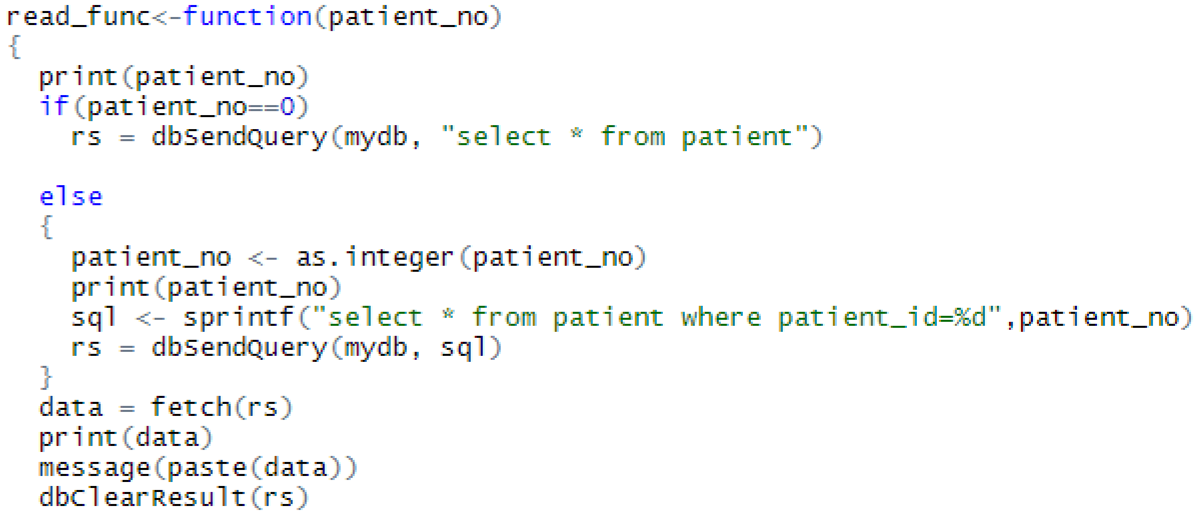
```
-- 1. Purpose Specification;
-- CREATE TABLE PatientPurpose (
--     pateint_id int,
--     doctor_id int,
--     diagnosis_id int,
--     diagnosis_description varchar(255)
-- );
```



```
-- 2. Consent;
-- CREATE TABLE attributes_consent (
--     consent_id int,
--     object_id int,
--     attribute_id int,
--     consent boolean
-- );
```



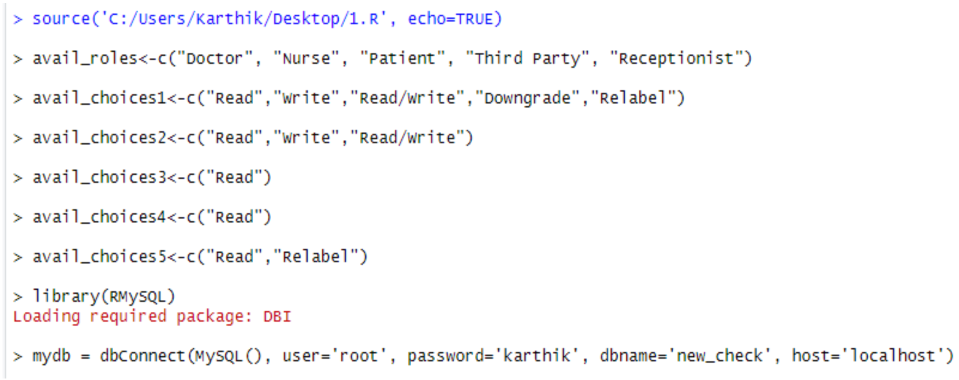
```
-- 9. Openess;
-- DELIMITER //
--
-- CREATE PROCEDURE get_patient_details(pat_id int)
-- BEGIN
--     SELECT *  FROM patient where patient_id=pat_id;
-- END //

-- CREATE PROCEDURE get_patient_allergy(pat_id int)
-- BEGIN
--     SELECT *  FROM allergy where patient_id=pat_id;
-- END //
--
-- CREATE PROCEDURE get_person_details(pat_id int)
-- BEGIN
--     SELECT *  FROM person where person_id=pat_id;
-- END //
```



```
read_func<-function(patient_no)
{
  print(patient_no)
  if(patient_no==0)
    rs = dbSendQuery(mydb, "select * from patient")

  else
  {
    patient_no <- as.integer(patient_no)
    print(patient_no)
    sql <- sprintf("select * from patient where patient_id=%d",patient_no)
    rs = dbSendQuery(mydb, sql)
  }
  data = fetch(rs)
  print(data)
  message(paste(data))
  dbClearResult(rs)
```

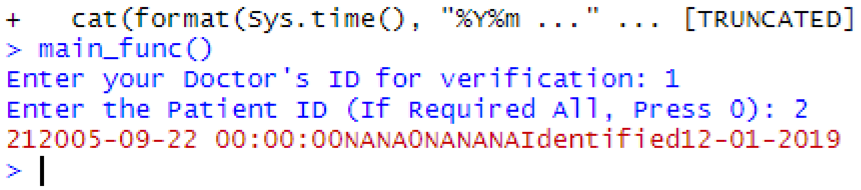
**Few Test Cases:**

a. Preparing Available Roles and their Respective Choices.



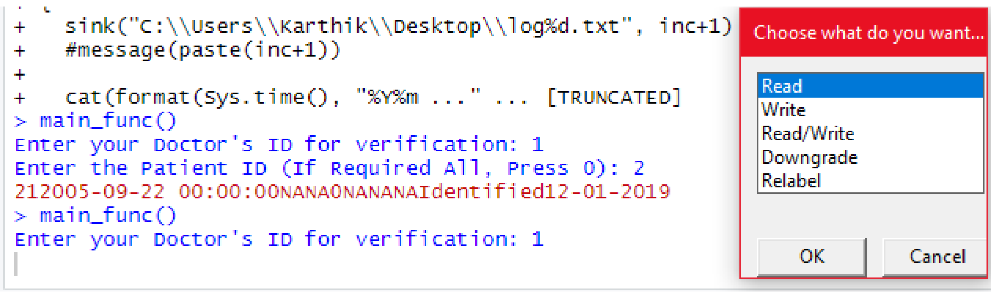
```
> source('C:/Users/Karthik/Desktop/1.R', echo=TRUE)

> avail_roles<-c("Doctor", "Nurse", "Patient", "Third Party", "Receptionist")

> avail_choices1<-c("Read","Write","Read/Write","Downgrade","Relabel")

> avail_choices2<-c("Read","Write","Read/Write")

> avail_choices3<-c("Read")

> avail_choices4<-c("Read")

> avail_choices5<-c("Read","Relabel")

> library(RMySQL)
Loading required package: DBI

> mydb = dbConnect(MySQL(), user='root', password='karthik', dbname='new_check', host='localhost')
```

b. Reading Data using R interface (in accordance with RWFM label).



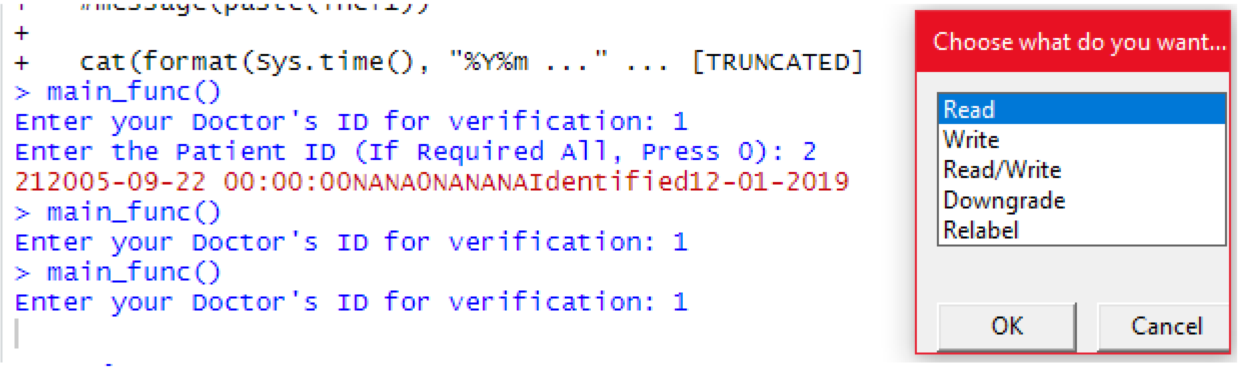
```
+    cat(format(Sys.time(), "%Y%m ..." ...  [TRUNCATED]
> main_func()
Enter your Doctor's ID for verification: 1
Enter the Patient ID (If Required All, Press 0): 2
212005-09-22 00:00:00NANA0NANANAIdentified12-01-2019
> 
```

c. Role based choices for each actor.

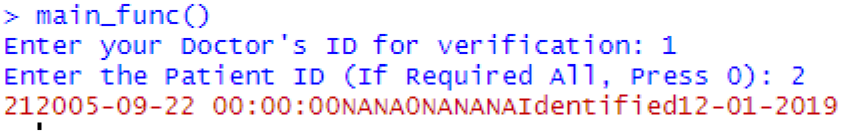


```
+    sink("C:\\Users\\Karthik\\Desktop\\log%d.txt", inc+1)
+    #message(paste(inc+1))
+
+    cat(format(Sys.time(), "%Y%m ..." ...  [TRUNCATED]
> main_func()
Enter your Doctor's ID for verification: 1
Enter the Patient ID (If Required All, Press 0): 2
212005-09-22 00:00:00NANA0NANANAIdentified12-01-2019
> main_func()
Enter your Doctor's ID for verification: 1
```

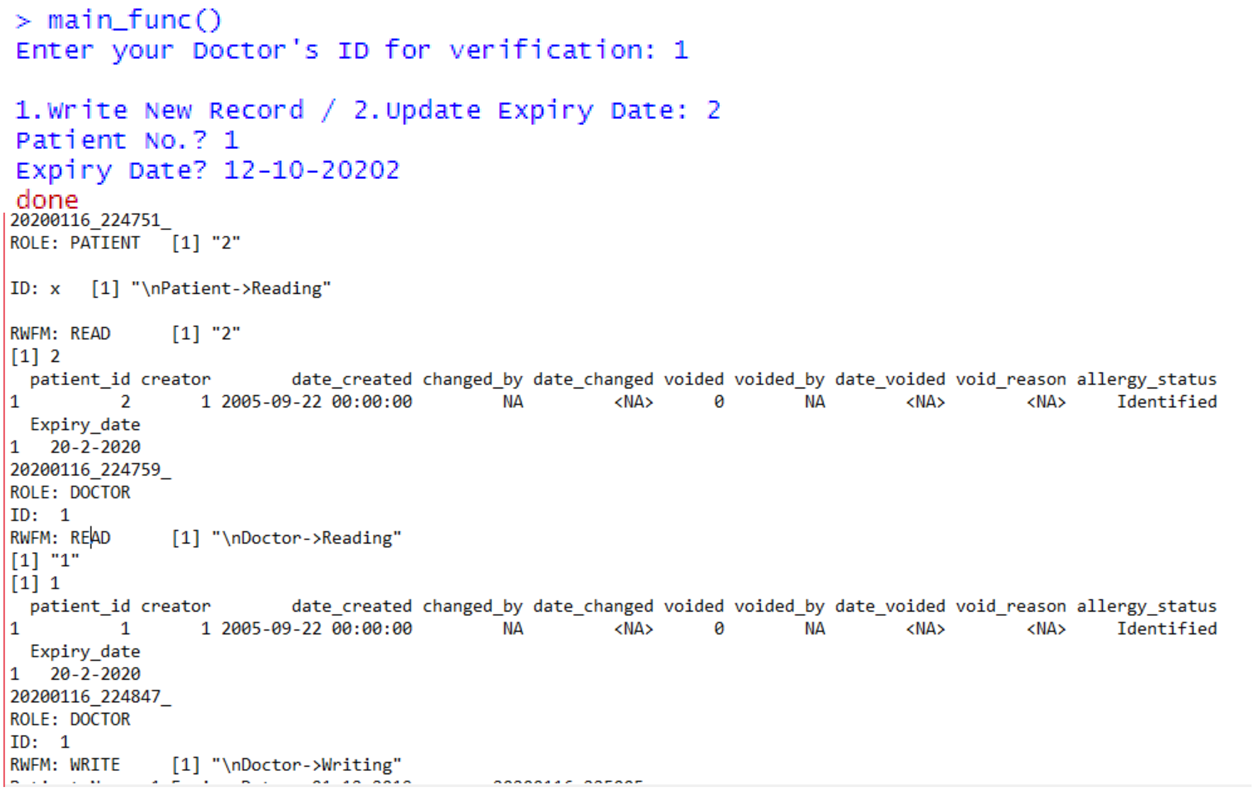
**Screenshots:**



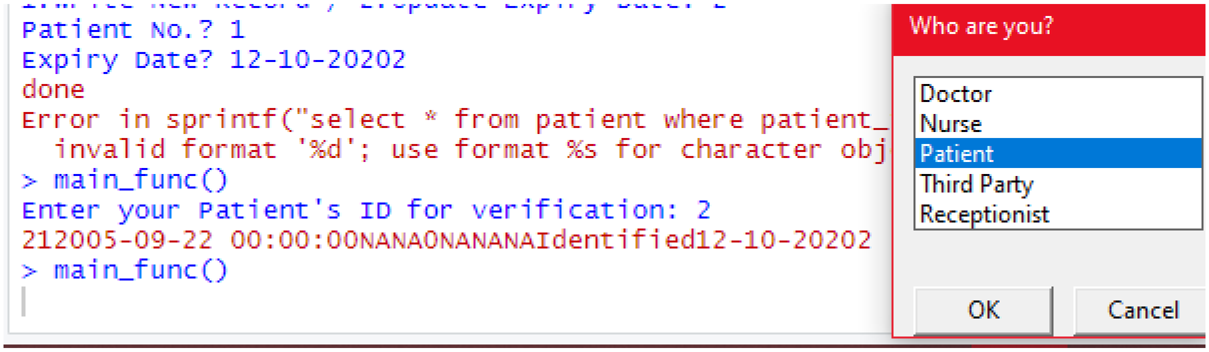
```
+    #message(paste(inc+1))
+
+    cat(format(Sys.time(), "%Y%m ..." ...  [TRUNCATED]
> main_func()
Enter your Doctor's ID for verification: 1
Enter the Patient ID (If Required All, Press 0): 2
212005-09-22 00:00:00NANA0NANANAIdentified12-01-2019
> main_func()
Enter your Doctor's ID for verification: 1
> main_func()
Enter your Doctor's ID for verification: 1
```



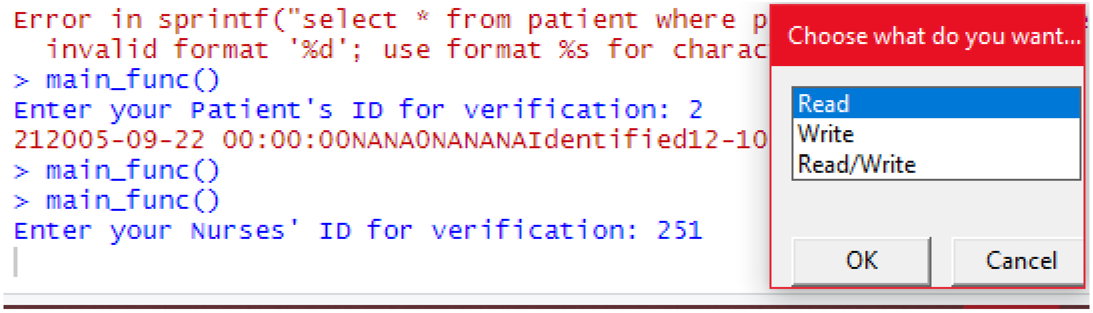
```
> main_func()
Enter your Doctor's ID for verification: 1
Enter the Patient ID (If Required All, Press 0): 2
212005-09-22 00:00:00NANA0NANANAIdentified12-01-2019
```



```
> main_func()
Enter your Doctor's ID for verification: 1

1.Write New Record / 2.Update Expiry Date: 2
Patient No.? 1
Expiry Date? 12-10-20202
done
20200116_224751_
ROLE: PATIENT   [1] "2"

ID: x   [1] "\nPatient->Reading"

RWFM: READ      [1] "2"
[1] 2
  patient_id creator         date_created changed_by date_changed voided voided_by date_voided void_reason allergy_status
1          2       1 2005-09-22 00:00:00         NA         <NA>      0        NA        <NA>        <NA>     Identified
  Expiry_date
1   20-2-2020
20200116_224759_
ROLE: DOCTOR
ID:  1
RWFM: READ      [1] "\nDoctor->Reading"
[1] "1"
[1] 1
  patient_id creator         date_created changed_by date_changed voided voided_by date_voided void_reason allergy_status
1          1       1 2005-09-22 00:00:00         NA         <NA>      0        NA        <NA>        <NA>     Identified
  Expiry_date
1   20-2-2020
20200116_224847_
ROLE: DOCTOR
ID:  1
RWFM: WRITE     [1] "\nDoctor->Writing"
```



```
Patient No.? 1
Expiry Date? 12-10-20202
done
Error in sprintf("select * from patient where patient_
  invalid format '%d'; use format %s for character obj
> main_func()
Enter your Patient's ID for verification: 2
212005-09-22 00:00:00NANA0NANANAIdentified12-10-20202
> main_func()
```



```
Error in sprintf("select * from patient where p
  invalid format '%d'; use format %s for charac
> main_func()
Enter your Patient's ID for verification: 2
212005-09-22 00:00:00NANA0NANANAIdentified12-10
> main_func()
> main_func()
Enter your Nurses' ID for verification: 251
```

## Results:-

Database applications such as health information systems exist with conflicting interests of the database owner and the users or organizations interacting with the database, With the above mentioned methods: RWFM labelled views, Role based privacy views:- we can conclude that privacy can be maintained w.r.t to user donating his health data and the organizations/hospital. That is the interface involved with roles shows that specific tasks can be done only by certain individuals with privileges mentioned in the form roles.

RWFM label suggests that individual data and role based data views can be achieved. This type of views is certain of handling privacy much better than the conventional methods. We've verified such labels with the help of MySQL in order to be certain that the RWFM labels are working properly or not.

The outputs show that the different layers of kernel shown in the model design is achieved with respect to interface, role based usage, RWFM label, logging and session generation. It's all timed and w.r.t to smart contracts working in the dummy database which is used to replicate the nature of an Ethereum blockchain.

## References:-

1. Agrawal, R., Bird, P., Grandison, T., Kiernan, J., Logan, S., &Rjaibi, W. (2005, April).
2. Agrawal, R., Kiernan, J., Srikant, R., & Xu, Y. (2002, January). Hippocratic databases. In VLDB'02: Proceedings of the 28th International Conference on Very Large Databases (pp. 143-154). Morgan Kaufmann.
3. Bancilhon, F., & Kim, W. (1990). Object-oriented database systems: in transition. ACM SIGMOD Record, 19(4), 49-53.
4. Basharat, I., Azam, F., & Muzaffar, A. W. (2012). Database security and encryption: A survey study. International Journal of Computer Applications, 47(12).
5. Bartoletti, M., &Pompianu, L. (2017, April). An empirical analysis of smart contracts: platforms, applications, and design patterns. In International conference on financial cryptography and data security (pp. 494-509). Springer, Cham.
6. Bertino, E., Jajodia, S., &Samarati, P. (1995). Database security: research and practice. Information systems, 20(7), 537-556.
7. Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives, 29(2), 213-38.
8. Denning, D. E., Akl, S. G., Heckman, M., Lunt, T. F., Morgenstern, M., Neumann, P. G., & Schell, R. R. (1987). Views for multilevel database security. IEEE Transactions on Software Engineering, (2), 129-140.
9. Denning, D. E., Denning, P. J., & Schwartz, M. D. (1979). The tracker: A threat to statistical database security. ACM Transactions on Database Systems (TODS), 4(1), 76-96.
10. Denning, D. E. (1984, April). Cryptographic checksums for multilevel database security. In 1984 IEEE Symposium on Security and Privacy (pp. 52-52). IEEE.
11. DeWitt, D. (2004, October). Limiting disclosure in hippocratic databases. In 30th Int. Conf. on Very Large Databases, VLDB Endowment, Toronto, Canada (pp. 108-119).
12. Dobkin, D., Jones, A. K., & Lipton, R. J. (1979). Secure databases: Protection against user influence. ACM Transactions on Database systems (TODS), 4(1), 97-106.
13. Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data. In Proceedings of IEEE open & big data conference (Vol. 13, p. 13).
14. Eyal, I., Gencer, A. E., Sirer, E. G., & Van Renesse, R. (2016). Bitcoin-ng: A scalable blockchain protocol. In 13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16) (pp. 45-59).
15. Garvey, T. D., & Lunt, T. F. (1991, November). Cover Stories for Database Security. In DBSec (pp. 363-380).
16. Göbel, J., Keeler, H. P., Krzesinski, A. E., & Taylor, P. G. (2016). Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. Performance Evaluation, 104, 23-41.
17. Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., &Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. Journal of medical systems, 42(7), 130.
18. Jajodia, S., & Meadows, C. (1995). Inference problems in multilevel secure database management systems. Information Security: An integrated collection of essays, 1, 570-584.
19. Keller-McNulty, S., & Unger, E. A. (1993). Database systems: Inferential security. JOURNAL OF OFFICIAL STATISTICS-STOCKHOLM-, 9, 475-475.
20. Luu, L., Chu, D. H., Olickel, H., Saxena, P., &Hobor, A. (2016, October). Making smart contracts smarter. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 254-269). ACM.
21. Maurer, U. (2004, June). The role of cryptography in database security. In Proceedings of the 2004 ACM SIGMOD international conference on Management of data (pp. 5-10). ACM.

22. Pernul, G. (1994). Database security. In Advances in computers (Vol. 38, pp. 1-72). Elsevier. “Extending relational database systems to automatically enforce privacy policies.” In 21st International Conference on Data Engineering (ICDE'05) (pp. 1013-1022). IEEE.
23. Raskin, M. (2016). The law and legality of smart contracts.
24. Tendick, P., &Matloff, N. (1994). A modified random perturbation method for database security. ACM Transactions on Database Systems (TODS), 19(1), 47-63.
25. Thuraisingham, M. B. (1989, September). Mandatory security in object-oriented database systems. In ACM SIGPLAN Notices (Vol. 24, No. 10, pp. 203-210). ACM.
26. Wright, A., & De Filippi, P. (2015). Decentralized blockchain technology and the rise of lexcryptographia. Available at SSRN 2580664.
27. Garg, A., Chakraborty, S., Malik, M., Kumar, D., Singh, S., & Suri, M. (2020). Investigation of Data Deletion Vulnerabilities in NAND Flash Memory Based Storage. arXiv preprint arXiv:2001.07424.