IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁙ Impact Factor 7.105 ⁙ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.9670

“Publicly Verifiable Shared Dynamic Electronic Health Record Using Cloud Computing”

Sushma P[1], Thanuja J C [2]

Dept. of MCA, Bangalore Institute of Technology, Bengaluru, India[1]

Dept. of MCA, Asst. Professor Bangalore Institute of Technology, Bengaluru, India[2]

Abstract: “Electronic health record (EHR)” is one of the systems that gathers patients' mechanized prospering data and then offers it with the other clinical benefits providers in the cloud. Since the EHR contains a ton of immense and tricky data about patients, it is standard that the improvement ensures response rightness and cut off uprightness. Meanwhile, with the move of IoT, more low performance terminals are sent for getting and moving patient data to the server, what accumulates the computational and correspondence weight of the EHR structure. The verifiable database outline (VDB), where a client re-appropriates his huge data base to a cloud server and sets presumptions once he truly needs unambiguous data, is proposed as a possible updatable scattered dealing with model for resource obliged clients. To in addition enable cut-off, most existing VDB plans use explanation reuse and show vitalizing strategy to show precision of the mentioning results. Notwithstanding, it pardons the "reliable" of check age, which achieves an over that the client needs to play out extra cycle (for instance evaluating plans) past what many would consider possible validness, as a matter of fact. In this paper, we propose an obviously certain commonplace updatable EHR illuminating get-together plot that stays aware of safety guarding and gathering uprightness checking with least client correspondence cost. We change the solid reasonable commitment (FC) plot for the VDB plan and make an essential FC under the computational l - BDHE speculation. Besides, the utilization of a capable verifier-close by refusal pack signature plot makes our arrangement support dynamic assembling part exercises, and gives uncommon parts, as obvious quality and non-outline limit.

Keywords: Verifiable database, distributed storage, utilitarian responsibility, protection safeguarding examining, client renouncement

I. INTRODUCTION

WITH the dangerous increment of worldwide data, the cloud administration industry has been growing uncommonly. Many cloud specialist co-ops are hurrying to send off cloud administration stages and items, like Amazon, GOOGLE, Alibaba, Microsoft, and Huawei, and so forth. Individuals begin to revaluate their huge information stockpiling errands to cloud specialist co-ops (CSPs). It makes them at this point not compelled by restricted neighbourhood capacity and registering assets. As a substantial and excellent application illustration of distributed storage system, and then the cloud-based “electronic health record (EHR)”, which is a framework that usually gathers the patients' computerized wellbeing data, is overwhelmingly advanced by the numerous associations, like the Office of the National Coordinator for Health Information Technology (ONC) [5] in the United States and Canada Health Info way [6]. The patient EHR’s are composed of the workstation or cell phone, & it can be gotten to & it is changed later on. The patients EHR’s transferred to cloud system can be divided between various clinical organizations to assist patients with seeking better treatment, help logical analysts to complete sickness investigation and exploration, and assist general wellbeing divisions with anticipating, distinguish and possibly forestall the flare-up of scourge infections, and so on. Since the cloud specialist co-op (CSP) is a free administration element, client really surrenders a definitive command over their EHR’s. This brings a security (secure) challenges for rethinking undertakings. For example, the cloud servers might return mistaken results in light of multiple factors, like failing cloud supplies and a programmer's assault. The erroneous returned values can have genuine ramifications for all aspects of the clinical framework. Accordingly, the major issue looked by the EHR system is on the most skilled methodology to ensure that the server reactions exactly each time. 'Benabbas et al.' [9]. Proposed the undeniable enlightening record (VDB) as a monitored and strong updatable streamed taking care of model for asset restricted clients. In a VDB plot, a client can revaluate the impediment of a gathering of information things to an untrusted server. Sometime later, the client can take a gander at the server for a thing (a message) at position I; the server returns the put away message at this continuous situation nearby a proof that it is to be the right response. In any case, the security of just checking the server reaction accuracy is a long way from enough for the EHR framework, and not satisfactory whether information isn't regularly gotten to is as yet put away accurately. On the off chance that this information are obliterated and not found in opportunity, it can cause enormous misfortunes in case of a crisis.

DOI: 10.17148/IARJSET.2022.9670

Additionally, security and protection of clinical information stockpiling and access should be upheld by legitimate regulations [8]. In this manner, an incredible asset for EHR frameworks is expected to satisfy the lawful prerequisites in defending the security and assurance of the clinical data.

I. Our Contribution

This examination centres on the security or safety and effectiveness of enormous data set capacity, like EHR. As per the qualities of EHR framework, two parts of safety merit our consideration, specifically, the server reaction rightness and the information stockpiling respectability. To manage above issues, we utilize another instrument called utilitarian responsibility (FC) and plan a freely obvious updatable data set conspire in light of practical responsibility supporting protection safeguarding trustworthiness evaluating and dynamic gathering activity. Our commitments can be summed up as follows:

1. We alter the current utilitarian responsibility [15] plot to utilize the capacity restricting of practical obligation to plan an auditable "VDB" conspire. Two calculations for the refreshing are added in the light of first plan in [15]. What's more, a changed cement FC with refreshes below the estimated - BDHE l supposition that is built. Our development has fewer boundaries and then it is more effective than the first plan [15].

2. We usually bring up safety issues with a plot [14] and propose a freely certain reformable VDB conspire in light of the practical responsibility and gathering mark without causing an excess of computational above and capacity cost. Also, our plan is relevant for huge scope information capacity with least client correspondence cost. Our proposed conspire not just jelly every one of the properties of the first VDB plot, yet additionally executes effective security safeguarding respectability inspecting, non-frame ability and recognisability. The plan jelly information security from the evaluator by utilizing an irregular concealing strategy and the scanty vector is utilized for testing reviewing. Our plan upholds dynamic gathering part activities which incorporate join and disavowal. Furthermore, our VDB upholds clump inspecting and then it upholds multi-cloud server, multiuser and also, multi-capacity vector situations.

II. Organization

The rest of this paper is worked with as follows. In the segment 2, we will present the connected work. In segment 3, we will present the distributed storage system model of our plan & then point out some of the security issue of the existing works. Segment 4 presents a few primers. In segment 5, we give a substantial useful obligation to direct capacities with refreshes, under the estimated- BDHE l presumption. The conventional definition and security necessities of the proposed plot and a huge game plan are displayed in segment 6. Area 7(seven) gives effective gathering client activities to our VDB plot. Area 8 presents clump inspecting to the proposed VDB plot. The security (safety) and proficiency examination of the VDB conspire was given in area 9. We then finish the work in area 10(ten).
2 Related Work Electronic prospering record is a development that assembles the patients' computerized wellbeing information. It can lessen the clinical mistakes, save EHR stockpiling expenses, and offer clinical information, etc. Research on data security of "electronic health record system" consolidates open encryption, insurance shielding, access control, and data amassing trustworthiness, etc. Numerous examinations have been presented [16] - [19], and our work revolves around the security of the accumulating of tremendous data base, for instance, electronic prosperity records.

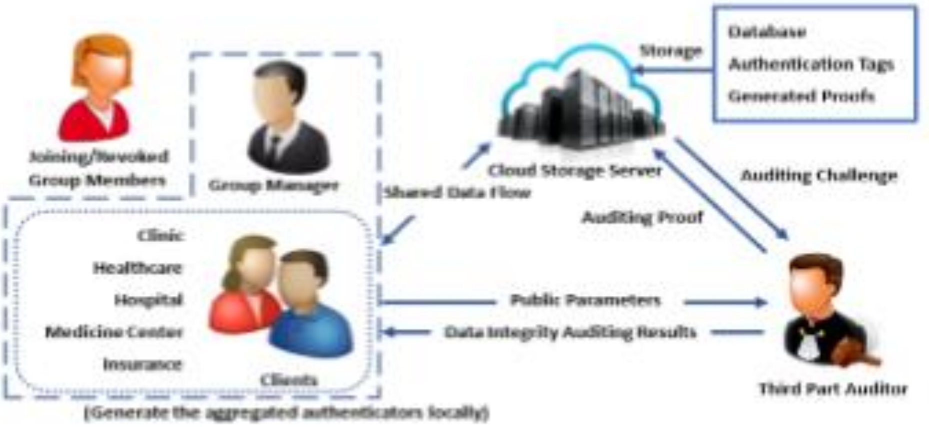


Fig-1. The distributed storage model of our VDB scheme, which integrates three substances, the disseminated stockpiling server, the clients and a Third Part Auditor (TPA)

II. PROBLEM FORMULATION

We initially present the distributed cloud storage model. And then, call attention to the safety and security issues of the current ‘VDB’ plans [10] - [14].

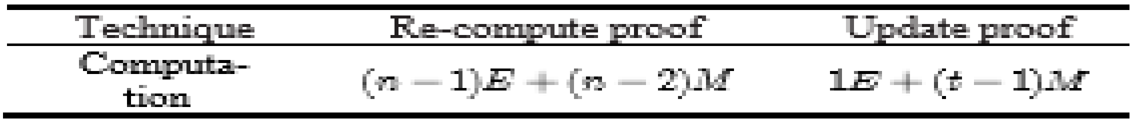
1 Cloud Storage Model

As displayed in above Fig-1, there are mainly 3 elements, which are the “distributed storage server”, “clients” and a “Third-Party Auditor (TPA)” in this distributed storage mode system. The distributed storage model system gives far off information capacity administrations to client. ‘TPA’, who can be anybody in the framework, usually checks information stockpiling respectability of the client re-appropriated data set. The clients, including patients, facility, emergency clinic, medication focus, protection, and so on, can re-appropriate huge data sets to the server. Not at all like most examining plans, the client produces the accumulated validation labels it locally and then sends them to the cloud. Also, the client would question & then refresh the data set and actually look at the information stockpiling uprightness. The Third-Party Auditor (TPA) may check the information stockpiling trustworthiness of much of the time refreshed data set involving the public- key in an effective manner. In our effective gathering part situation, any gathering client can transfer own data set to the cloud & offer them with the other gathering individuals. Furthermore, believed a bunch director is a liable for joining or repudiating on client.

2 Security Problems

Jiang et al. [14] who were the roused by VDB plot, built on their honesty actually taking a look at conspire. In the VDB conspire, to produce a proof for each question, and then the server needs to include the entirety of ongoing put away information. The information contained in this evidence will likewise be confirmed in the confirmation stage alongside the information questioned. In any case, their plan utilizes the methods of verification reuse and confirmation refreshing to further develop the framework productivity. In the above strategies, the cloud doesn't need to re-work out evidence without fail, and refreshing the verification requires just a modest quantity of calculation. It extraordinarily lessens the above and works on the effectiveness and reaction paces of the framework. Anyway because of the way that their model didn't consider an idea of "constant" confirmation, the utilization of these strategies makes their review conspire and other VDB plans unequipped for really taking a look at capacity trustworthiness. For this situation, just the questioned information is engaged with the confirmation interaction. This prompts confirmation just on the information being questioned, while capacity trustworthiness of other cloud information isn't checked. On the off chance that the cloud information which isn't questioned is harmed, it won't be identified in time. At the point when the harmed information is required, there will be fluctuating levels of misfortune. The method involved with producing verification for the server in plans [10] - [14] is as per the following: there are on data to be taken care of as a vector 12 (, ,...,) nm m . I m is the taken care of data in the index i of the vector. I g and, ij g are public boundaries about file [1,] □ in and [1,] □ jn. 1 == □ I nm ii Cg is the vector responsibility. Whenever client first questions file [1,] □ in , the server processes the confirmation , 1, =□= □ j mn I j j I Pg and sends it with other important data to the client as a reaction. Then, the server stores I P. Whenever similar information is questioned once more, the put away evidence I P can be given straightforwardly to the client as verification of this question without another computation. Whenever client refreshes a few information record [1,] □ jn , the waiter can create another confirmation j P' in a straightforward updatable manner. The 2 cases are displayed beneath: 1. □jk Calculate the refreshed confirmation =□ kk P ' P

TABLE: EFFECTIVENESS COMPARISON BETWEEN RE-COMPUTE PROOF AND UPDATE PROOF. T IS THE NUMBER OF PROOFS WHICH ARE STORED BY THE SERVER. M IS A MULTIPLICATION IN 1 G (OR 2 G) AND E IS AN EXPONENTIATION IN



Technique	Re-compute proof	Update proof
Computa-tion	$(n-1)E+(n-2)M$	$1E+(t-1)M$

□− jj mm kjg , where j m' is one of the record j 's update information. 2. =jk .The refreshed verification continues as before j P. Expect that the server has stored t verifications. We signify by M a duplication in the 1 G (or 2 G) and E an exponent in 1 G . Above Table show the correlation of the 2 proof age strategies. The server also needs to do 1−n exponentiations and also 2−n augmentations to figure the evidence I P. On the off chance that the waiter produces the evidence in an updatable manner, the waiter simply has to do 1 exponentiation and 1 −t duplications to refresh confirmations. At the point when there is no update between requests, the server either makes the affirmation by the above recalculation or returns the set aside confirmation with no figuring. By utilizing the procedure of verification refreshing, the cloud doesn't need to re-work out the evidence without fail and refreshing confirmation requires just a little calculation. It will all around be seen that the above framework enormously reduces the heap on the cloud. The server will decide to utilize this technique. The VDB plan of Jiang et al. [14] expressly utilizes this construction, while other VDB plans [10] - [13] which don't unequivocally show its utilization can in like manner decide to utilize this methodology thinking about its high sensibility. Then, we make sense of why the above procedure compromises the security objective of plan [14]. As displayed in below Fig. When the client questions record I, the cloud server returns the responsibility C, the evidence I P , the information esteem I m and then a few public boundaries. The check system of the 'VDB' is to match I m and then all j m contained in the verification I P , where, [1,]/{ }□ j n I , with the information vector 12 (, ,...,) nm m contained in the responsibility C. The 12 (, ,...,) nm m in C is also the matching layout. Assuming that the match is so effective, it shows that I m and all the "ongoing" j m utilized in the check cycle is put away accurately. In any case, the above methods will make that the confirmation that the server will returns each time is not generally created by all information at present put away by the server. Just the questioned information can be checked. This is vain regardless of whether the server is sincerely refreshing the verification and returning the put away evidence each time. In such a manner,

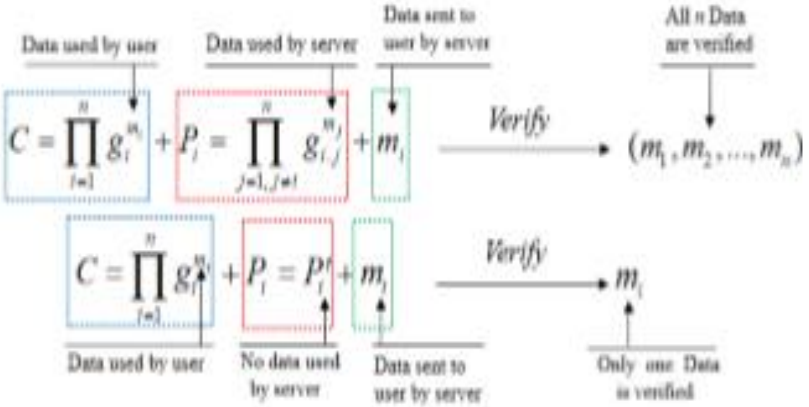

Data used by user
Data used by server
Data sent to user by server
All n Data are verified
$C = \prod_{i=1}^{n} g_i^{m_i}$
$P_i = \prod_{j=1, j\neq i}^{n} g_{i,j}^{m_j}$
m_i
Verify
$(m_1, m_2, \dots, m_n)$
$C = \prod_{i=1}^{n} g_i^{m_i}$
$P_i = P_i'$
m_i
Verify
m_i
Data used by user
No data used by server
Data sent to user by server
Only one Data is verified

Fig-2. The security issue of certification reuse and the strategy of affirmation fortifying.

Plot [14] and the other VDB plans are never again will have the capacity of actually looking at information capacity uprightness. Just that when server is semi-genuine member could the inspecting property of the VDB at any point conspire be acknowledged by executing the verification age calculation sincerely and not executing the evidence update calculation. In any case, the current VDB plans can't compel the server to do as such. They need a system to compel the server to utilize every one of the put away information to produce evidence like clockwork.

3 Design Ideas

To empower 'VDB' plans to acquire the capacity to check information to collect or gather trustworthiness, with an extra evaluating plan is required. Nonetheless, the utilization of existing evaluating plans will prompt new computational above and correspondence costs; in the meantime the VDB plan will actually lose its benefits. This will challenge propelled us to plan a 'VDB' plot that accomplishes wanted safety/security objectives without a lot of new computation/calculation cost. We likewise add a survey stage for the VDB plan. The objective is that the server should answer with the continuous put away information during the review cycle. Our answer is that in each review task, the examiner questions for the vast majority information blocks. In particular, the evaluator produces an irregular coefficient for every information block, and every one of the coefficients created for numerous information blocks comprise a testing vector. Definitively when the cloud server gets a test vector from the onlooker, the haphazardness of the test vector drives it should utilize the real-time put away information to play out a fast development with it. Then, at that point, the server needs to create a collected verification for the direct activity. At long last, the direct blend esteem is gotten back to the evaluator for check alongside its verification. In any case, difficult to execute total check keeps up with straight activities in the existing VDB. A fundamental idea is to include the affirmation passed on and put something aside for each of the data block in the VDB to make the confirmation for gathered check during the audit stage. Likewise, the auditable VDB plan can consider the low correspondence cost of the clients and no extension of server putting away. Nonetheless, since in the current VDB, the hidden entryway worth of every data block I is related

DOI: 10.17148/IARJSET.2022.9670

worth I g. The different secret entryways bring about the evidences of various information blocks can't be collected to create a proof that possesses a brought together hidden entrance. Obliged by the development procedures of the ongoing VC conspire, these plans can't just total the confirmations to accomplish the honesty reviewing of the information stockpiling. We will utilize a changed FC plan to take care of this issue. For that the plan of ‘VDB’ plot, the first FC in [15] should also be updatable. Also, that the developed plan ought to be more effective.

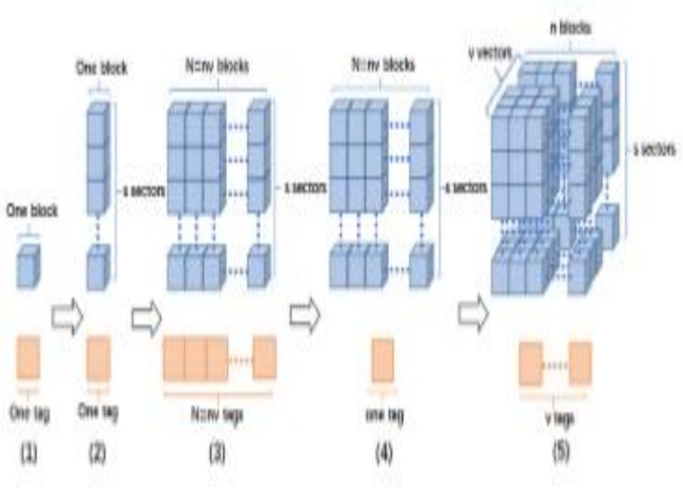


Fig-3. The instruction for adding up to demand names for data blocks.

One of the first goals is to give lower correspondence cost review convention for wasteful gear. Above Fig. shows how we will total the verification labels. As displayed in above Fig. [1], in the general review plot, one information block has a one verification tag. As displayed in above Fig. [2], the convention [2] proposed the strategy to basically extend the size of the every data block. They developed every information block into s areas, with every area that having a similar size as one block in above Fig [1]. This approach diminishes how much information blocks partially, subsequently lessening the quantity of labels. Be that as it may, as displayed in above Fig.3 [3], N data blocks in convention will still have the N labels. Honestly, information blocks are the essential unit of inquiry for examiners. Essentially utilizing this way to deal with diminish the quantity of labels is definitely not an optimal methodology. For computational proficiency, with the development of a solitary information block, the calculation measure of every reaction will increment extraordinarily. For security, as the quantity of information blocks diminishes, the reviewer can without much of a stretch work out the genuine information by tackling the arrangement of straight conditions through various questions. As displayed in above Fig [4], by utilizing FC conspire, the information is put away as N-layered vector. Our ‘VDB’ can additionally total the labels of all N information block into one label in light of the plan [23]'s strategy without decreasing the quantity of blocks. At the point when how much information is huge, the length n of vector ought to be picked with a trade-off among calculation and correspondence as displayed in above Fig.[5]. Information blocks can be put away as a VDB framework, actually creating a tag for every vector. Simultaneously, the test information blocks will be chosen from the whole network. Moreover, the evaluating system is performed by the outsider, and the current VDB plans don't have protection saving unquestionable status. Protection saving put away information check implies that the TPA can't determine the substance of the genuine information from that the cloud server system reaction in the evaluating. Existing VDB plans need to be scramble information in the event that they believe any outsider should confirm the outcomes while keeping up with information security. The plan ought to have security protecting undeniable nature to help the evaluating system. Moreover, existing VDB conventions can't be utilized in situations where bunch individuals share information. It is a significant property in EHR framework. The reviewing plan in light of VDB of Jiang et al. [14] executes bunch client disavowal.

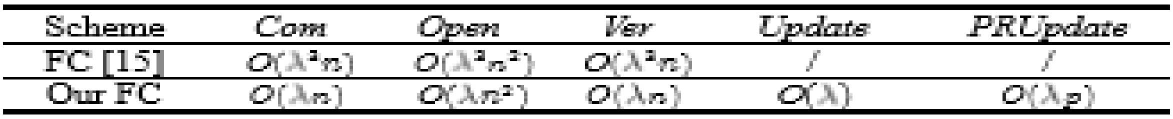
III. FUNCTIONAL COMMITMENTS WITH UPDATES

As of late, Libert, Ramanna and Yung [15] set forward other crude called utilitarian responsibilities. Specifically, messages comprise of vector 12 (, ,...,) nm m and the FC plot permits a vector to be resolved to create a responsibility esteem. From that point onward, the responsibility esteem is opened as a predetermined direct capacity 1 = □□ n iii xm, for public coefficients 12 (, ,...,) nx x . They gave a substantial FC to direct mixes under subgroup choice suspicion in the composite request bilinear collections. Their FC fulfils 2 properties which are impeccably stowing away and work restricting. In the meantime, the useful responsibility is brief. Notwithstanding, the plan also has more boundaries and then it is less proficient. In this part, for plan of VDB conspire, two calculations for refreshing are added in light of the first FC plot in [15]. Furthermore, a changed cement FC with refreshes under the calculated BDHE −l supposition that is introduced. At last, we will give the similar examination of our plan and convention [15].

1 Definition of FCs for Linear Functions with Updates

The first meaning of the utilitarian responsibilities for the direct capacities in conspire [15] comprises of 4 “probabilistic polynomial time (PPT)” calculations “(FC.Setup, FC.Com, FC.Open, FC.Ver). “ We will add 2 PPT calculations – “FC.Update and FC.PRoofUpdate” to the first definition and advanced to practical responsibilities for straight capacities with refreshes.

TABLE: EFFICIENCY COMPARISON BETWEEN FUNCTIONAL COMMITMENT SCHEME IN [15] AND OUR FC SCHEME FOR VECTOR LENGTH n , WHITBINDINGAGAINSTADVERSARIES OF RUNTIME 2 . Signify BY p THE NUMBER OF PROOFS.



Scheme	*Com*	*Open*	*Ver*	*Update*	*PRUpdate*
FC [15]	$O(\lambda^3 n)$	$O(\lambda^3 n^2)$	$O(\lambda^3 n)$	/	/
Our FC	$O(\lambda n)$	$O(\lambda n^2)$	$O(\lambda n)$	$O(\lambda)$	$O(\lambda p)$

2 Protocol Examination

The security of our proposed FC plan ought to fulfil accuracy, restricting and stowing away [15]. The pertinent safety or security definitions and the confirmations are in the Appendix B. To assess the exhibition of the proposed FC, we make the near examination with the plot [15], which also incorporates both the capacity intricacy and calculation expense. The plan [15] utilizes a composite request collection of 3 primes with the request 1 2 3 = N p p , where any () 1 2 □ polyp □ for each {1,2,3} =i . It makes the size of its gathering component 3 () O □ . Conversely, to manage the enemy with a similar processing power as the plan [15], our plan utilizes a solitary prime gathering with request =Np, whose bunch component size is () O □.

In FC Setup calculation, the responsibility key CK produced by this plan is made of2n bunch components out of single request bunch. In the meantime, in the plan [15], it is made out of 3 +1 n bunch components of composite request bunch. In the FC.Com calculation, the two plans create just single responsibility esteem separately. In the FC.Open calculation, these two plans total verifications into one gathering component except for the test vector x

IV. Examination of the Proposed VDB

- **Security**

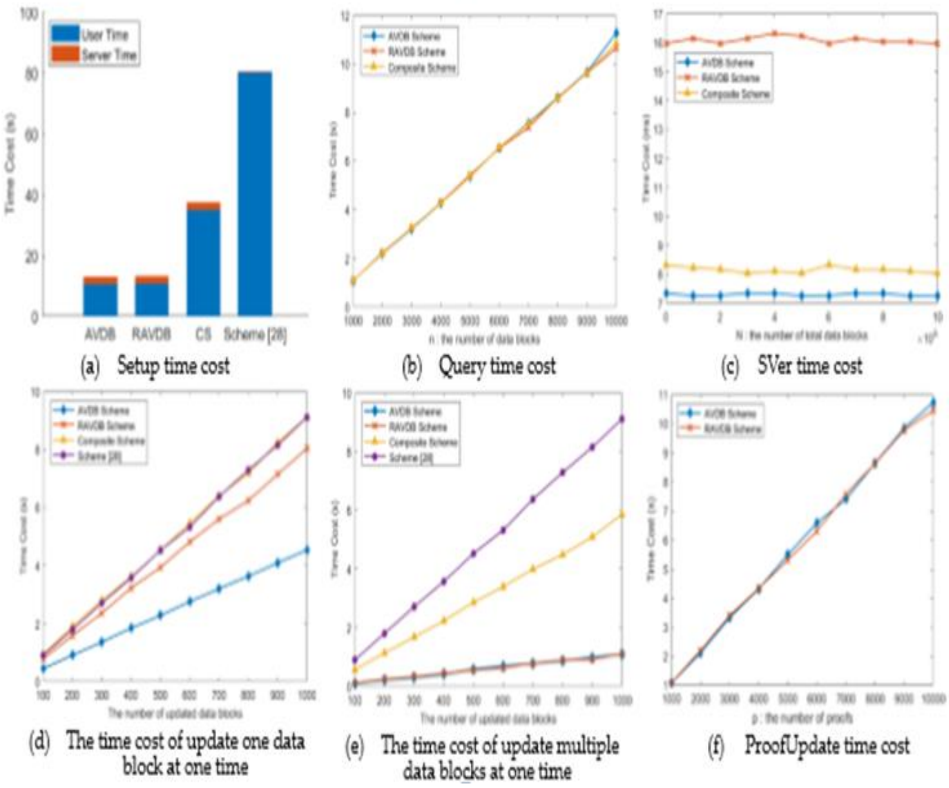
Our VDB plan can safely and effectively question and update data set put away in the cloud and openly review information capacity trustworthiness. In the development, a few cryptographic apparatuses are utilized as one of the essential module of plan. Expect that the accompanying modules are more secure, including the practical responsibility plot and that the mark calculation. Under the calculated BDHE −l supposition, the accompanying demonstrates that our “VDB” conspire is secure. Hypothesis 1. The proposed ‘VDB’ plot with refreshes in view of computational − l BDHE assumption DL supposition DDH suspicion and q-solid Diffie-Hellman supposition that is right and more secure & upholds protection safeguarding examining cluster reviewing recognisability and non-frame ability.

- **Efficiency**

In deals to address the plausibility of our proposed major auditable VDB devise (AVDB) and revocable AVDB plot (RAVDB).The composite plan will exhibits that the VDB conspire uses the extra review plan to accomplish VDB's security prerequisites for the question result rightness and the information stockpiling trustworthiness. Yuan-Yu Scheme [12] is a public reviewing plan for cloud information sharing that upholds client repudiation. Every one of the four plans, right off the bat, depends on the amortized model, which demands a one-time expensive computational in Setup calculation. Specifically, our plans create verification for various information blocks in Query calculation just a single time, which likewise it has amortization proficiency. Furthermore, our plans are proficient. For the client, how much calculation is free of the information base size. Every one of the confirmations utilized for check can be produced by the server. This permits clients to do next to no processing. Clients don't necessarily need to be on the web. For the

DOI: 10.17148/IARJSET.2022.9670

server, how much calculation relies upon the age of the confirmation. Also, perhaps the greatest benefit of our plan is that the evidences in the review stage can also be practically totally created by the verifications in the capacity stage. This permits stockpiling and review to be very much coordinated to decrease calculation. Also, not the same as the current review plans where one information block one validation tag has, our plan has as it were



(a) Setup time cost (b) Query time cost (c) SVer time cost

(d) The time cost of update one data block at one time (e) The time cost of update multiple data blocks at one time (f) ProofUpdate time cost

Fig-4. Arrangement and Storage Stage time cost

V. Conclusion

The idea of undeniable information base is an extraordinary device for certain EHR stockpiling. In any case, verification reuse and the strategy of confirmation refreshing by the server to further develop framework productivity neglects to accomplish information trustworthiness checking. In this paper work, we will propose a novel updatable VDB plot in light of the utilitarian commitment that upholds security protecting trustworthiness reviewing and bunch part tasks, including join and disavowal. Two security necessities of EHR are executed: the server response rightness and the data accumulating uprightness. Our VDB plot accomplishes the ideal safety objectives without causing excessively computational increment. What's more, our VDB conspire gives the base correspondence cost to the terminal with restricted execution. A down to earth better cement VDB plot under computational BDHE−l supposition that is introduced. Besides, pack assessing for our VDB plot stays aware of multi-cloud server, multi-client and multi-taking care of vector conditions. It makes the looking over structure more skilful. Besides, we will demonstrate that our practical responsibility conspire which with refreshes & our ‘VDB’ plan can accomplish the ideal safety and then security properties. The exhibition of our plan is much more proficient contrasted and other various calculations.

References

[1] Wei L, Wu C, Zhou S. productive verifier-neighborhood repudiation bunch signature plans with in reverse unlinkability. Chinese Journal of Electronics, 2009, e90-a(2):379-384.

[2] Dan B, Shacham H. Bunch marks with verifier-neighborhood denial. Acm Conference on Computer and Communications Security. 2004.

[3] Chaum, David, and T. P. Pedersen. Wallet Databases with Observers. Global Cryptology Conference on Advances in Cryptology 1992.

DOI: 10.17148/IARJSET.2022.9670

[4] B. Dan, X. Boyen, E. J. Goh, "Progressive character based encryption with consistent size ciphertext", International Conference on Theory and Applications of Cryptographic Techniques. Springer-Verlag, pp. 440456, 2005.

[5] A. Kate, G. M. Zaverucha, I. Goldberg, "Steady Size Commitments to Polynomials and Their Applications", Advances in Cryptology - ASIACRYPT 2010 - , International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010. Procedures. DBLP, pp. 177-194, 2010.

[6] Official Website of The Office of the National Coordinator for Health Information Technology (ONC). (2004). Accessible: https://www.healthit.gov/

[7] Canada Health Infoway. (2001). Accessible: https://www.infoway-inforoute.ca/en/

[8] J. Hu, H.H. Chen, T.W. Hou, "A half and half open key framework arrangement (HPKI) for HIPAA protection/security guidelines", Computer Standards and Interfaces vol. 32, No. 5-6, pp. 274-280, 2010.

[9] S. Benabbas, R. Gennaro, Y. Vahlis, "Certain Delegation of Computation over Large Datasets", Conference on Advances in Cryptology. Springer-Verlag, pp. 111-131, 2011.

[10] D. Catalano, D. Fiore. “Vector Commitments and Their Applications”, Public-Key Cryptography – PKC 2013. Springer Berlin Heidelberg, pp. 55-72, 2013.

[11] X. Chen, J. Li, X. Huang, et al. “New Publicly Verifiable Databases with Efficient Updates”. IEEE Transactions on Dependable & Secure Computing, vol. 12, no.5, pp. 546-556, 2015.

[12] X. Chen, J. Li, J. Weng, et al. “Verifiable Computation over Large Database with Incremental Updates”, European Symposium on Research in Computer Security. Springer, Cham, pp. 148-162, 2014.

[13] M. Miao, J. Wang, J. Ma, et al. “Publicly verifiable databases with efficient insertion/deletion operations”, Journal of Computer & System Sciences, vol. 86, pp. 49-58, 2017.

[14] T. Jiang, X. Chen, J. Ma. “Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation”, IEEE Transactions on Computers, vol. 65, no. 8, pp. 2363-2373, 2016.