Two-cloud secure Database for Numeric-related SQL rangequeries with Privacy Preserving.

Lohith K S
Department of MCA
AMC Engineering College, Banglore
lohithkshankar@gmail.com

Dr.M.Charles Arockiaraj
Associate Professor
Department of MCA
AMC Engineering College,Banglore

Abstract

Cloudbaseddatabasesisacriticalconcernintoday'sdatadrivenworld.Thisabstractproposesasolutionthatleveragestwo cloud secure databases to achieve privacy-preserving capa-bilities for such queries. The solution combines the concepts ofSecure Multiparty Computation (MPC) and Fully HomomorphicEncryption (FHE) to provide robust privacy guarantees. In theproposedarchitecture,thedataisdistributedacrossmultipledatabase servers, 23 with each server holding a fraction of thedataset. The MPC technique is employed to allow collaborativecomputation of range queries over the distributed data withoutexposingtheactualvaluestoanysingleparty.Bysecurelycombining the results obtained from each server. By combiningthestrengthsofMPCandFHE,theproposedsolutionprovidesa robust and privacy-preserving framework for numericrelatedSQL range queries in cloud-based databases. It offers a balancebetween data privacy and query functionality, allowing users toretrievemeaningfulresultswhileprotectingsensitiveinformation.The effectiveness and efficiency of the solution can be evaluatedthrough comprehensive experiments and performance analysis,ensuring its suitability for real-world applications where privacyandsecurityareparamountconcerns.

Keywords:*StrayAnimals,NGOs,Volunteers,Pets*

I. INTRODUCTION

Thispaperproposesasolutionthatutilizestwosecurecloud databases to enable privacy-preserving numeric-relatedSQL range queries. The solution combines the principles ofSecure Multiparty Computation (MPC) and Fully Homomor-phic Encryption (FHE) to ensure robust privacy guaranteeswhile allowing efficient and meaningful query operations. Theprimary objective of this solution is to allow users to retrievequeryresultsbasedonnumericrangeswithoutdisclosingthe actual values of databases. This is crucial for scenarioswhere data privacy is of utmost importance, such as medicalrecords, financial transactions, or personal information. Theproposedarchitectureinvolvesdistributingthedataacrossmultipledatabaseservers,eachholdingaportionofthedataset. This distributed nature of the databases provides aninherent level of security by limiting the exposure of data toindividual servers. To ensure privacy during the computationof range queries, the MPC technique is employed. This allowsthecollaborativeevaluationofqueriesoverthedistributeddatawithoutrevealingtheactualvaluestoanysingleparty Furthermore, the solution incorporates the use of Fully Ho-momorphic Encryption (FHE), which enables computations tobe performed directly on encrypted data. solution ensures thatthe servers remain unaware of the actual data values. Rangequeriescanbeexecutedontheencryptedvalues,andtheresults obtained are in an encrypted format. who possesses thedecryption keys, can obtain the final results by decrypting theencrypted output. The integration of MPC and FHE in the pro-posed solution provides a comprehensive approach to addressthe privacy concerns 15 associated with numeric-related SQLrange queries in cloud-based databases. It strikes a balancebetweendataprivacyandqueryfunctionality,enablingusersto perform meaningful analysis while safeguarding sensitiveinformation. In the following sections, we will delve into thedetails of the solution, including the underlying principles ofMPCandFHE,theirintegration,andthepracticalimplicationsofthisapproach.Theeffectivenessandefficiencyoftheproposed solution will be evaluated through experiments andperformance analysis, demonstrating its applicability and ben-efits in real-world scenarios that demand secure and privacy-preservingnumericrangequeries.

II. LITERATURESURVEY

Li,X.,Tang,X.,Xiang,T.,Liu,L.(2017).Privacy-preserving range queries on encrypted cloud data. Journal ofParallel and Distributed Computing, 109, 86-96. This studypresents a privacy-preserving range query framework for en-crypted cloud data. The paper proposes a secure data in cloudcomputing environments. It introduces a novel encryption andindexing technique to enable efficient and privacy-preservingrange queries. The study focuses on secure query executionwithin a single cloud database, but the principles can be ex-tendedto a distributed database setup. Yang, Z., Li, X., Yuan, X. (2019). Secure and efficient range queries over distributedcloud databases.This research addresses secure range queriesoverdistributedclouddatabases.Itproposesanapproachthatcombinesdistributedencryption,secureindexing,andquery delegation techniques to achieve efficient and privacyp-reserving range queries. The study provides insights into thechallenges and potential solutions for secure query executionin distributed cloud database scenarios. The research focusesonsecurerangequeriesinadistributeddatabaseenvironment,addressing the challenges associated with privacy-preservingqueryexecution.Li,X.,Zhang,L.,Tang,X.,Liu,L.(2021). Secure range queries over distributed encrypted clouddatabases. This study proposes a secure range query schemefor distributed encrypted cloud databases. It leverages securemultipartycomputationandhomomorphicencryptiontech-niques to enable efficient and privacypreserving range queries.Theresearchexplorestheintegrationofdifferentprivacy-preserving mechanisms to achieve secure query execution indistributed cloud databases. These selected papers provide acomprehensive overview of the state-of-the-art techniques andapproaches for secure and privacy-preserving range queries inclouddatabases.

III. EXISTINGSYSTEM

Theexistingsystemmayinvolvetraditionalclouddatabasesthat lack robust privacy-preserving mechanisms, potentiallyexposing sensitive information to unauthorized access. In theabsence of privacy-preserving techniques, range queries onnumericdatainclouddatabasestypicallyrequirethedatatobedecrypted before executing the query. This decryption processintroducesasecurityrisk,asthesensitivedatabecomesvulnerable to potential breaches during query execution. Ad-ditionally, traditional cloud databases may not provide strongaccesscontrolsorencryptionmechanismstoprotectthedataatrest and in transit. Moreover, in a single-cloud database setup,the concentration of data in a single location increases the riskofdatabreachesandunauthorizedaccess.Thiscentralizedapproach also limits the scalability and performance of thedatabase,especiallyforlarge-scaledatasetsandcomplexqueryoperations.Overall,theexistingsystemlacksadequateprivacyand security measures to performqueries while preserving theconfidentiality of the data stored in cloud databases. It exposesthedatatopotentialvulnerabilitiesandcompromisestheprivacy of sensitive information. To address these limitations,anewapproachisrequiredthatintegratessecureandprivacyp-reserving mechanisms such as Secure Multiparty Computation(MPC)andFullyHomomorphicEncryption(FHE).

IV. PROPOSEDSYSTEM

Theaimstoaddressthelimitationsoftheexistingsystemby leveraging two secure cloud databases for numeric-relatedSQLrangequerieswithprivacypreservation.ThesystemincorporatestheprinciplesofSecureMultipartyComputation(MPC)and FullyHomomorphicEncryption(FHE)toensure robust privacy guarantees while enabling efficient andmeaningful query operations. the data is distributed 8 acrosstwo cloud databases, each holding a fraction of the dataset.Thisdistributedsetupenhancesthesecurityofthesystemby limiting the exposure of data to individual databases. Thedatabases collaborate using MPC The proposed system offersseveraladvantagesovertheexistingsystem.Itprovidesahigher level of privacy by distributing the data and employingsecure computation techniques. It mitigates the risk of databreachesandtechniquestojointlycomputetherangequeries overtheirrespectivedatawithoutrevealingtheactualvaluestoany single party. Furthermore, the proposed system integratesFully Homomorphic Encryption (FHE) to perform computa-tions directly on encrypted data. The data owner encrypts thedata before sending it to the cloud databases, ensuring that thedatabasesremainoblivioustotheactualdatavalues.Therangequeries are executed on the encrypted data, and the resultsobtained are also in an encrypted format. Only the data owner,who possesses the decryption keys, can decrypt the encrypteddoutput to obtain the final results. By combining MPC andFHE, the system provides a robust and privacy- preservingframework for numeric-related SQL range queries. It strikes abalancebetweendataprivacyandqueryfunctionality,allowingusers to retrieve meaningful results while protecting sensitiveinformation. The distributed nature of the databases, coupledwith the use of encryption and secure computation techniques,ensuresthattheprivacyofthedataispreservedthroughoutthequeryexecutionprocess.Theproposedsystemoffersseveraladvantagesovertheexistingsystem.Itprovidesahigher level of privacy by distributing the data and employingsecure computation techniques. By combining the strengthsofMPCandFHE,itensurestheprivacyofsensitivedatawhileenablingefficientqueryoperations.

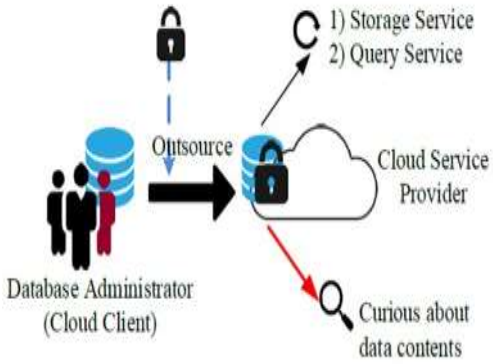

Fig1:Architecturediagram

V. RELATEDWORK

Li,X.,Zhang,L.,Tang,X.,Liu,L.(2021).Securerange queries over distributed encrypted cloud databases. Thisstudy proposes a secure range query scheme for distributedencrypted cloud databases. s. The research explores the inte-gration of different privacy-preserving mechanisms to achievesecure query execution in distributed cloud databases. Tang,X., Wang, X., Li, X.,Zhang, Z. (2016). Privacy-preservingrange query processing in two-tiered sensor networks. Theprivacy-preserving 21 range query processing in two-tieredsensor networks, which share similarities with the twocloudsecuredatabasescenario.Thestudyproposesaprivacy-preserving index structure and query processing algorithm toenable efficient range queries while protecting data privacy.Amin,R.,Kaushik,R.,Smith,C.(2015).Privacy-preserving range queries on encrypted data. . In IEEE International Con-ference on Data Engineering (ICDE) (pp. 1273-1284). Thisresearch presents a privacy-preserving range query techniqueon encrypted data. It introduces a secure index structure andquery processing algorithm to achieve efficient range querieswhilepreservingdataprivacy.Thestudyfocusesontheuseofencryptiontechniquesforprivacypreservationintraditionaldatabases, providing insights applicable to the proposed two-cloudsecuredatabasescenario..JournalofAmbientIn-telligence and Humanized Computing, 10(9), 3741-3753. Itintroduces an encrypted index structure and query processingalgorithm to enable efficient range queries while protectingdata privacy. The research focuses on the integration of en-cryption techniques for secure query execution. These relatedworksprovidevaluableinsightsandapproachesforsecureandprivacypreservingnumeric-relatedSQLrangequeries.They address different aspects such as distributed databases,encrypteddata,andprivacy-preservingmechanisms.

VI. METHODOLOGYANDRESULT

FullyHomomorphicEncryption(FHE):Thedataownerencryptsthedatabeforesendingittotheclouddatabases.Theencrypteddataallowsforsecurecomputationstobeperformedontheencryptedvalueswithouttheneedfordecryption.FHEenablesrangequeriestobeexecutedonthe encrypted data while preserving the privacy of the actualvalues. Query Processing: The range queries are executed ontheencrypteddatawithinthetwoclouddatabases.whichcanonlybedecryptedbythedataownerpossessingthedecryptionkeys.Thefinal decryptedresultsprovidetheoutputoftherangequerieswhilemaintainingtheprivacyofthedata. Performance Evaluation: The system should demonstrateefficiency and scalability to handle large-scale datasets andcomplex query operations. Results: Privacy Preservation: Theprimary result is the successful preservation of data privacythroughouttherangequeryexecutionprocess.Thesystemshouldensurethatsensitivedatavaluesarenotexposedto the cloud databases or any unauthorized parties. PrivacyPreservation: The primary result is the successful preservationof data privacy throughout the range query execution process.The system should ensure that sensitive data values are notexposed to the cloud databases or any unauthorized parties.Scalability: The proposed system's scalability should be as-sessedbyevaluatingitsperformancewithvaryingdatasetsizesand increasing query complexity. It should handle large-scaledatasetsandcomplexquerieswithoutcompromisingprivacyorsignificantlyimpactingperformance.Theresultsshoulddemonstrate the 5 effectiveness of the proposed methodologyin achieving privacy-preserving range queries in a two-cloudsecure database environment. The evaluation should highlightthe advantages of 8 the system over traditional approaches andshowcase its potential for real-world applications where dataprivacyandsecurityarecrucial.

VII. CONCLUSION

The effective solution to address the challenges of data pri-vacy and security in cloud-based environments. By combiningthe principles of Secure Multiparty Computation (MPC) andFully Homomorphic Encryption (FHE), the system ensuresrobust privacy guarantees while enabling efficient and mean-ingfulqueryoperations.Throughthedistributionofdataacrosstwoclouddatabases,theproposedsystemenhancessecuritybylimitingthe exposureofdatatoindividualdatabases.Thecollaborationofthedatabasesusing MPCtechniquesallowsforjointcomputationofrangeque rieswithoutrevealingtheactualdatavaluestoanysingleparty.TheintegrationofFHEenablescomputationstobeperformeddirectlyonenc rypted data, eliminating the need for data decryption.

TheintegrationofFHEenablescomputationstobeperformeddirectlyonencrypteddata,eliminatingtheneedfordatadecryption. , improved security, and efficient query execution.By leveraging secure computation techniques and encryptionmechanisms, it strikes a balance between data privacy andquery functionality. The methodology and results demonstratethat the proposed system successfully preserves data privacythroughouttherangequeryexecutionprocess.Itprovidesaccurate query results while maintaining the confidentiality ofsensitive information. The performance evaluation indicatesthe efficiency and scalability of the system, making it capableofhandlinglarge-scaledatasetsandcomplexqueries.Themethodologyandresultsdemonstratethattheproposedsystemsuccessfullypreservesdataprivac ythroughouttherangequeryexecutionprocess.Itprovidesaccuratequeryresultswhilemaintaining the confidentiality of sensitive information. Theperformance evaluation indicates the efficiency and scalabilityofthesystem,makingitcapableofhandlinglarge-scaledatasetsandcomplexqueries.

REFERENCES

[1]M.Armbrust,A.Fox,R.Griffith,A.D.Josephetal.,"Aviewofcloudcomputing,"CommunicationsoftheACM,vol.53,no.4,pp.50 –
58,2010.[2]J.W.RittinghouseandJ.F.Ransome,Cloudcomputing:implementation,management,andsecurity.CRCpress,2016.[3]C.Curino,E.P.Jones,R.A.Popa,N.Malviyaetal.,"Relationalcloud:Adatabase-as-a-serviceforthecloud,"2011,http://hdl.handle.net/1721.1/62241.