Mahendra Institute of Technology

Affiliated to Anna University | Approved by AICTE |NAAC Accredited with ' A ' Grade | An ISO 9001:2015 Certified Institution

(AUTONOMOUS)

MAHENDRA
EDUCATIONAL INSTITUTIONS
SINCE 1978

DEPARTMENT OF
COMPUTER SCIENCE AND ENGINEERING

A framework for securing decentralized resources In cloud server using block-chain

Guided By:

Dr,Nilabar Nisha AP/CSE

Mahendra Institute Of Technology

Mallasudram (637503)

Submitted By:

AnithKumar.B(611617104008)

Dinesh babu.A(611617104020)

Gowtham.B(611617104026)

NandhaKumar(611617104065)

A Framework For Securing Decentralized Resources in Cloud Server Using Block-Chain

Abstract:

- To process encrypted database, a server/node in CSP is "empowered" with two features equipping a secure processor and refer these as secure servers/nodes.
- A normal server/node is not capable of processing the encrypted database.
- To query the outsourced database, the database owner communicates with a single secure server as if the entire database is stored in it.

- In CSP, encrypted database is partitioned and stored. In addition honey encryption method is added.

- It protects the data by providing fake key and identifies intruder and block-chain has been impleemnted.

Problem Statement

- This analysis shows that the proposed scheme keeps location private from the LBSP under the semi-honest threat model.

- A low efficient experimental evaluation using the Open Street -Map dataset which evaluates more time cost of query signature and generation, as well as the search process.

Existing System

- A novel query scheme in which the user specifies locations of interest along with a minimum privacy degree and for each location.

- Consider a location A, the CSP returns an area B containing A that is sufficiently large to satisfy the constraint on the minimum entropy.

- Importantly, the CSP cannot infer information about A beyond the fact that it is contained in B.

- The proposed framework supports search by location attributes in addition to locations themselves.

- To construct it, the LBSP builds a hierarchical index, which closely mimics the geographic hierarchy of the locations.

- Then, each node in the index is replaced by a Bloom filter representing both the location and its attributes.

- The reason for using a Bloom filter is threefold:
  - (i) a cryptographic hash function makes it hard to recover the data content from the hash result,
  - (ii) a Bloom filter is space efficient which is important when dealing with many locations, and
  - (iii) size of a Bloom filter is independent of number of locations in a multi-location query, which in combination with subsequent encryption, makes it difficult for CSP to establish number of locations in a query.

- In order to hide the searched data and the pattern of the Bloom filter from the CSP, we encrypt the Bloom filter using Function-Hiding Inner Product Encryption (FHIPE).

- It utilizes the ability of FHIPE to calculate the number of matching bits.

- This way, the CSP determines whether a query vector matches an index vector by separately comparing the number of matching bits for the location and for the attributes.

Disadvantages

- Stored data are quiet insecure.
- Attackers can easily acquire the server details.
- More chance for data breach.

Proposed System

- DCS is based on re-designing the architecture to support security features on encrypted data that has been stored in server.
- It tightly couples database encryption with this architecture.
- With this method, the encrypted data from server/nodes can be operated in a secure manner and prone to attackers.
- As a result data are encrypted and moved to nodes, in which honey encryption has been implemented.

.

- As honey encryption has been implemented attackers are denied from accessing data and attacker receives an empty file.

- Due to the presence of cryptographic measures along with honey encryption DCS has been secured highly when compared with the existing features.

- Block chain methodology can be added to the DCS which ensures the data security and prevents attackers from accessing in an unauthorized manner.

Advantages

- The database owner requests a secure query service from CSP and the response to secure the data is more efficient..

- The CSP allocates the resources to nodes and sends public & private keys to database owner which enriches the security features.

- Due to implementation of cryptographic features and honey encryption user information in nodes are maintained securely compared with current security issues.

System Requirements

Hardware Requirements

Processor	:	i3,i5,i7
RAM	:	2GB
Hard disk	:	500 GB
Compact Disk	:	650 Mb
Keyboard	:	Standard keyboard
Mouse	:	Logitech mouse
Monitor	:	15 inch color monitor

Software Requirements

- Front End : PHP
- Back End : MYSQL
- Operating System : Windows OS
- Server : WAMP Server
- System type : 32 or 64 Bit OS

Literature survey

S.No	Title	Authors	Algorithm	Advantage	Disadvantage
1	Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking	B. Rogers, S. Chhabra, Y. Solihin, and M. Prvulovic	➤Location-based services(LBS) ➤Global Positioning System (GPS)	it removes the need to evaluate potentially complex service provider privacy policies	an adaptive quad tree-based algorithm that decreases the spatial resolution of location information to meet a specified anonymity constraint.
2	Dummy Based Privacy Preservation in Continuous Querying Road Network Services	Fincy Francis1, Aparna M.S, Anitta Vincent	➤Privacy Preservation Algorithm; ➤Clustering Algorithm.	Increase robustness for on-line signature verification	how to generate a dummy that is indistinguishable from a real user especially on road networks which have varied movement trends

S.No	Title	Authors	Algorithm	Advantage	Disadvantage
3	Location Privacy via Differential Private Perturbation of Cloaking Area	C. Gentry, S. Halevi, and N. P. Smart	Hilbert curve shifted	Provides user evaluate their queries and their data.	Limitations on recognition and its performance in behavioral verification
4	Achieving k-anonymity in Privacy-Aware Location-Based Services	E. Aktas, F. Afram, and K. Ghose	Dummy-Location Selection (*DLS*)	Data and information are stored in a secured (Encrypted) manner	Chance for lose of data

S.No	Title	Authors	Algorithm	Advantage	Disadvantage
5	Location Privacy-Preserving Task Allocation for Mobile Crowdsensing with Differential Geo-Obfuscation	C. Gentry, S. Halevi, and N. P. Smart	mixed-integer nonlinear program (MINLP)	Provides user evaluate their queries and their data.	Limitations on recognition and its performance in behavioral verification
6	Location Privacy Protection for Smartphone Users Using Quadtree Entropy Maps	E. Aktas, F. Afram, and K. Ghose	wireless service providers (WSPs	Data and information are stored in a secured (Encrypted) manner	Chance for lose of data

S.No	Title	Authors	Algorithm	Advantage	Disadvantage
7	Anatomization and Protection of Mobile Apps’ Location Privacy Threats	C. Gentry, S. Halevi, and N. P. Smart	LP-Doctor	Provides detailed status of crime data	Maintenance is a major failure
8	A Stochastic Game for Privacy Preserving Context Sensing on Mobile Phone	E. Aktas, F. Afram, and K. Ghose	minimax learning algorithm	Accessible throughout the nation.	Chance of lack of security of data.

S.No	Title	Authors	Algorithm	Advantage	Disadvantage
9	Trajectory Privacy Preservation based on a Fog Structure for Cloud Location Services	C. Gentry, S. Halevi, and N. P. Smart	Dummy rotation (DR) algorithm	Easier to identify the SCAM and its occurrences. .	Chance of misguidance
10	Efficient and Privacy-preserving Polygons Spatial Query Framework for Location-based Services	E. Aktas, F. Afram, and K. Ghose	special polygons spatial query algorithm (SPSQ)	Results of different areas can be easily predicted.	Quiet complicated to acquire data as large amount of data are used.

Algorithms

- **Existing System Algorithms**
  - Location Based Service Protocol (LBSP)
  - Bloom Filter Using Function-Hiding Inner Product Encryption (FHIPE)
  - Private Information Retrieval (PIR)
- **Proposed System Algorithms**
  - Advanced Encryption Standard (AES)
  - Honey Encryption
  - RSA

Modules

- Upload and View File Details
- Verify Secret Key
- Verify Trapdoor Unlinkability
- View Request and Send Response
- View Attacker

Upload and View File Details

- Each user who can access the cloud storage can upload their desired data to the cloud storage server.
- The entire data will be in an encrypted format in the cloud server.
- The admin i.e.: the cloud owner can view the file details such as size, location and as well as the user can retrieve their data from the cloud server.

Verify Secret Key

- The cloud owner verifies the secret key provided by the user to access the data.
- The user maintains the data privacy by using the honey encryption algorithm.
- Hence incase of attack of data the breacher cant access the user data.

Verify Trapdoor and Unlinkability:

- It has been done by the cloud owner i.e.: the server to gain the knowledge about the tracker or the attacker.
- After knowing the attacker details the cloud owner can block or make unavailable status to the attacker for accessing the data of the user.
- The data of the user has been stored with quiet higher security level.

- **View Request and Send Response:**

  - The cloud server transfers the user data into secure nodes to make the security of the user data.

  - The data has been stored in multiple secure nodes so that the gains zero knowledge about the user data.

  - If the user sends the request to the server to retrieve the stored data the server accesses the secure node and provides the data to the user.

- **View Attacker:**
  - The cloud owner can view and block the attacker who tries to breach the data that has been stored in the secure node.
  - The tracking of the attacker can be done based on identifying the IP or MAC address of the attacker.
  - So that the data breacher cant access the data that has been stored in the secure node.

Block – Chain

- Block – Chain has been implemented which increases the privacy measures and security of entire network.
- Due to implementation of block – chain confidentiality of entire network has been efficiently maintained.