Meta Heuristic Neural Network Model For Data Security In Cloud Platform

S.Suganthi Devi

Abstract: Cloud is a dynamic on-demand service providing end-users with a dynamic environment in which data quality is guaranteed to remain confidential in cloud databases. The Cloud database is a collection of information containing the highest level of security access to data. This research proposed a new data security model, a Meta Heuristic Neural Network (MHNN), which guarantees high confidentiality and security of the data in the cloud. The hybridized hashing idea has been used to store fragmented sensitive information. This data security model is introduced via dynamic encryption fragmented component. In the data security model the Meta Heuristic Neural Network is used to process data encryption for sensitive information in order to improve confidentiality. This works with a few cloud databases that achieve high information security and confidentiality.

Keywords: Meta Heuristic Neural Network, Security, Confidentiality.

1. INTRODUCTION

Cloud computing is a paradigm for potential Internet applications. Cloud computing. Large information centers and server-based web bases are used in cloud applications [1]. It is a model to allow the shared pool of configurable computing resources to access an all-embracing, adaptable network on demand and be rapidly provided and deployed with minimal administration efforts and interaction between services providers [2,3]. There are three models in the Cloud Model: Service software (SaaS), Service platform (PaaS), and Cloud infrastructure (IaaS). The four Cloud Computing Deployment Models are Private Cloud, Community Cloud, Public Cloud and hybrid. A cloud databases are used for cloud computing. Two fundamental deployment models: customers are able to function cloud based data databases [5,6] independently of their data processing. In this section, we discuss cloud databases, security and fragmentation; they can use the cloud to process virtual machine images or buy the Cloud Cloud Database, which the Cloud Provider supports [7].

The figure 1 shows the data security lifecycle. Organizations needed to manage and maintain their own information with serious physical and logical processes to protect their susceptible information [8]. Our research aims at resolving critical cloud data security problems and ensuring that the cloud environment is trustworthy. The main focus of our studies is on information privacy. Confidentiality ensures that no information is disclosed to unauthorized persons. Confidentiality loss occurs if any individual who is not authorized to access the information is able to view or read. High quality services and diverse cloud information applications ensure the confidentiality of data [9]. It offers a dynamic customer environment as well as ensures data confidentiality quality of the service. Fragmentation on the cloud information is used to enforce data confidentiality. A Fragment is a distributed design method of a database, so that a partition mix gives the initial database in a single link and/or class in two or more partitions, without a lost data [10,11]. The primary aim and purpose of this framework work is to prevent possible attackers from using confidential information [12,13]. This research suggests a new mechanism for security in the cloud. In order to improve cloud computing security, we use a new encryption approach using an artificial neural network. The neural network comprises of the interconnected processing component known as Neuron [14]. When training is used, a network can learn or can also learn when training is not provided. Learning can be monitored or uncontrolled. There is a Masters in supervised learning for the monitoring of the network learning activity where there is no master's in unmonitored learning to monitor learning [15]. Counter-propagation is one way to learn the neural networks and has been widely used for various applications [16].

LITERATURE SURVEY

Damiani et al., [17] proposed to maintain an balance between effectiveness and confidentiality the concept of indexing outsourced encrypted data (IOED), using deterministic encryption and hacking techniques as an index for efficient storage of data. The mapping needs to be kept confidential and therefore stored on the client’s side. These bucket-based methods do not support aggregation requests, like SUMs. Sumet Bajaj et al, [18] introduced an Outsourced Database Prototype (ODP) enabling clients, through trusted server-based hardware, to perform SQL queries in critical query processing phases under limited relationship compliance. The proposed work provides new cost models.
and benefits of use of trustworthy information handling, Trust DB design and development equipment, a trusted, hardware-based, relationship information basis which provides complete confidentiality of information and has no query interpretation constraints. Cong Wang et al., [19] proposed to support public audits a Secure Cloud Storage System (SCSS). Terms and conditions are particularly important for a homomorphic linear authentication and a random overview technology, ensuring that the TPA does not learn the data content that is kept in the cloud during effective audits, confidentiality and privacy risks. It supports multi-party auditing. Bonde et al., [20] outlined that information can be distributed and conserved in the cloud environment so strongly and agreeably. Back Neural networks contribute to data information, loading and precision. During the procedure, no party would like to share its own personal data with other parties, if multiple parties can join the neurotransmission network. The proposed scheme encrypts private personal data locally and uploads the cloud cipher text. Meta Heuristic Neural Network Model for Data Security in Cloud PlatformThis work focuses on identifying and understanding issues related to the security of cloud computing performance as well as appropriate security techniques used in modern cloud computing world. The Hybridized Fragmented Hashing Function (HFHF) offers sensitive data confidentiality and ensures data insulation. The hybridized fragmented hashing function extends, decreases and automatically supports dynamic data when inserted and deleted, with updating, deletion and add-on blocks. For encryption and decryption of sensitive information the Meta Heuristic Neural Network (MHNN) model is used. It ensures security of data for private and state keys through neural network encryption. For data confidentiality requests of all kinds and efficiency, the data security model is more efficient. This model offers lower cost, more efficient storage and a expandable security-enhancing storage system.

Data storage mechanisms must be efficient and confidential. The Cloud user store data remotely and obtains high quality service in different cloud applications. This research is aimed at achieving cloud confidentiality through horizontal and vertical splitting. Fragmentation is the method by fragmentation of the database into fragments to store the data in several cloud data centers. Data confidentiality is obtained through segmentation into different parts of the relation databases and processing them in different places. The Meta-Heuristic Neural Network (MHNN) architecture is shown in Figure 2. It describes the Meta Heuristic Neural Network model flow. It is used for effective and confidential storage of information in the cloud. The information are fragmented into fragments and stored in the cloud storage in various data centers. The delicate information is individually encrypted as S. The fragmented data is efficiently stored via the dynamic hacking device. Sensitive information is

![Figure 2. Architecture of Meta Heuristic Neural Network (MHNN) model](image-url)
encrypted with neural network cryptographic algorithms and stored to increase confidence. In this study, We are suggesting a new model: "a Heuristic Network Model: Make the data store environment securely cloud-based." In a cloud environment, high data confidentiality and sensitive data security are implemented. It involves database owners, suppliers of cloud services and customers. To verify the information of data, data users access the data from a service provider. Data owners ensure that the data is confidential only for authorized users. Sensitive datasets are fragmented into fragments in the Hybridized Fragmented Hash Function (HFHF). These fragments are kept in hybridized hash systems. The sensitive fragments are encrypted with neural network cryptographic algorithms and stored in various server places. The distinctive features of hybridized hashing include orders of magnitude faster than other systems and make it possible for customers to read, update, insert and alter. Hybridized Fragmented Hash Function (HFHF) Large data sets will be saved and retrieved from various data center cloud databases. The fragmented hash structure is an hybridized type, which increasing or decreasing its size through the fragmented supplied data sets. In fragmenting large cloud datasets and storing them in dynamic encryption hashings, HFHF plays a major role. In one database, the HFHF divide in two or more fragments one relation or class. Before being distributed in various storage areas, fragmented data must satisfy 3 basic requirements:

- Before any process is applied, the database should be in the third normal form, so that each table can be treated as different fragment.
- The amount of confidentiality gives importance to the information in a fragment.
- User requirements provide a set of additional conditions to distribute the fragments that the user should select.

Algorithm 1. The Fragmentation Process

<table>
<thead>
<tr>
<th>Input: Cloud data Set</th>
<th>Output: Fragmented Sensitivity Encrypted data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td></td>
</tr>
<tr>
<td>Read cloud information set with sensitive information</td>
<td></td>
</tr>
<tr>
<td>The sensitive data sets are separated.</td>
<td></td>
</tr>
<tr>
<td>In the hybridized haze the fragmented data sets are stored.</td>
<td></td>
</tr>
<tr>
<td>Using hash functions, a data set is readable.</td>
<td></td>
</tr>
<tr>
<td>The encryption done by Meta Heuristic Neural Network (MHNN) model.</td>
<td></td>
</tr>
<tr>
<td>The public key will be used for decryption to encrypt sensitive data, and the private key will be used.</td>
<td></td>
</tr>
<tr>
<td>The encrypted data is stored with a hashing structure in the cloud.</td>
<td></td>
</tr>
<tr>
<td>Stop</td>
<td></td>
</tr>
</tbody>
</table>

The HFHF is standardized by data sets prior to fragmentation and applied in various normal form levels. In the first ordinary form multi-value attributes are deleted and associated data tables created. The second standard equation satisfies all requirements in the first ordinary form, separates sub-sets of information into separate tables and creates relations among them. The third standard form fulfills the two first standards of form, eliminating transitive dependence. By following measures, you explain the operation of the Hybridized Fragmented Hash Function. HFHF is the cloud input, which is the crypted data saved in a manner that adapts to the Hash table; the HFHF reads the cloud database with sensitive information. Vertically and horizontally, the sensitive information sets are fragmented. The hybridized hash features can be used to read data sets. Algorithm 2. Hybridized fragment hash model

Input: Sensitive Crypted Data Set
Output: Indexing value

- The data is collected from the cloud database of different data centers.
- By the fragmented horizontal and vertical mechanism the key and unkey attributes are partitioned.
- During the hybridized hash, the data set fragments are arranged.
- The Hashing function allows sensitive data to be collected from the cloud.
- The MHNN model is given the output of the fragmented data set
- Stop

RESULTS AND DISCUSSION

1. Performance

In any computerized system, the scale is developed based on the system's performance, but there is a connection between security and performance. Performance is a speed indicator for data exchange and data implementation, and protection from threats is indicated by security. The system software and hardware parts rely both on one side and the user and service provider on the other. The proposed Meta Heuristic Neural Network (MHNN) achieves higher performance when compared to IOED, ODP, SCSS methods. The figure 3 shows the performance ratio of MHNN Model.
2. Accuracy
In decades accuracy of distributed data storage was investigated including I/O performance and security. Whereas the security and hardware of people developed much more concrete meaning, many issues are still in cloud computing accuracy. Based on the latest computation models, conventional reliability solutions may not be suitable for contemporary cloud computing applications. The proposed Meta Heuristic Neural Network (MHNN) achieves higher accuracy when compared to IOED, ODP, SCSS methods. The figure 4 shows the accuracy ratio of MHNN Model.

![Figure 4. Accuracy Ratio](image1.png)

3. PRECISION
Cloud service precision is described as a probability that an under consideration cloud service can be carried out effectively for a user within a specified time period. This probability of delivery of a successful service is affected by two types of failure. The proposed Meta Heuristic Neural Network (MHNN) achieves higher precision when compared to IOED, ODP, SCSS methods. The figure 5 shows the precision ratio of MHNN Model.

![Figure 5. Precision Ratio](image2.png)

4. RECALL
It requires that the accuracy and completeness of data are maintained and ensured. A data proprietor always expects her or her data to be stored properly and confidently in a cloud [21]. This implies that the information should not be manipulated, incorrectly altered, deleted or manufactured illegally. If unwanted activities corrupt or delete information, the proprietor should be in a position to detect corruption or loss. Moreover, the information users can still be obtained when a part of the outsourced information is deleted or lost [22, 23]. The proposed Meta Heuristic Neural Network (MHNN) achieves higher recall ratio when compared to IOED, ODP, SCSS methods. The figure 6 shows the recall ratio of MHNN Model.

![Figure 6. Recall Ratio](image3.png)
5. F-SCORE

The proposed Meta Heuristic Neural Network (MHNN) achieves higher F-Score value [24,25] when compared to IOED, ODP, SCSS methods. The figure 4 shows the F-Score value of MHNN Model.

CONCLUSION

The cloud is mainly concerned with ensuring confidentiality when accessing a high degree of cloud data security. In our research the proposed model ensures confidentiality of data via neural networks, which enhances cloud security. A Meta Heuristic Neural Network(MHNN) provides high confidentiality and security in cloud databases for the achievement of confidential data in the cloud database. This research proposed a new Meta Heuristic Neural Network(MHNN). The Hybridized Fragmented Hashing Function (HFHF) store and uses encryption for its safety, fragmented delicate information. Compared with Meta Heuristic Neural Network(MHNN), this work is efficient for all types of queries, achieving high levels of data confidentiality.

REFERENCES


[18] Sumeet Bajaj, Radu Sion, “TrustedDB: A Trusted Hardware based Database with Privacy and Data


