HCIS | Human-centric Computing and Information Sciences

RESEARCH (Research Manuscript) **Open Access**

Human-centric Computing and Information Sciences (2023) 13:11
DOI: https://doi.org/10.22967/HCIS.2023.13.011
Received: December 28, 2021; Accepted: April 22, 2022; Published: March 15, 2023

A Hybrid Solution for Secure Privacy-Preserving Cloud Storage & Information Retrieval

Ankit Kumar[1], Turki Aljrees[2], Sun-Yuan Hsieh[3], Kamred Udham Singh[4,5,*], Teekam Singh[6], Linesh Raja[7], Jitendra Kumar Samriya[8], and Rajesh Kumar Mundotiya[9]

Abstract

Cloud storage is an emerging archetype used by businesses for data storage. Clients require easy access to data in the cloud, which helps clients with limited computing power move their high-value, high-risk principle jobs to the cloud. The primary concern of this study is towards flawless verifying, checking data bundles, and determining modules to carry out the project. As discussed at several research platforms, each client is concerned about data storage and retrieval. Data security is critical in cloud computing, and thus monitoring has evolved into a vigilance that abstracts the monitoring process. Request made by clients for security planning is always computationally exclusive. As a result, each customer is concerned as to their verified condition. This paper will highlight a secure cloud communication method for client data to address the afore-mentioned issues. Synchronization creates secret hare keys, combined with a model-encrypted data packet sent to the cloud. These secure data are then sent over a public network, subject to monitoring to avert data leakage to an unauthorized party. They lack the cohesion to outsource data storage to the cloud deliberately. As an outcome of this model's distribution, the perception of authorized data owners would be changed regarding cloud storage up to 97.6%, addressing the trust issues between data owners and cloud ace affiliations.

Keywords

Cloud, Privacy, Storage, Information Retrieval, Security, Encryption

1. Introduction

Cloud storage is an emerging new typology of data storage applied by corporates to store their extensive data in the present scenario of cut-throat competition. Clients are eager to know and perform

***Corresponding Author:** Kamred Udham Singh (kamredudhamsingh@gmail.com)
[1]Department of Computer Engineering & Applications, GLA University, Mathura, UP, India
[2]College of Computer Science and Engineering, University of Hafr Al-Batin, Eastern Province, Saudi Arabia
[3]Department of Computer Science and Information Engineering, Institute of Medical Information, Institute of Manufacturing Information and Systems, Center for Innovative FinTech Business Models, and International Center for the Scientific Development of Shrimp Aquaculture, National Cheng Kung University, Tainan, Taiwan
[4]School of Computing, Graphic Era Hill University, Dehradun, India
[5]Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan, Taiwan
[6]Department of Computer Science and Engineering, Graphic Era Deemed to be University Dehradun, India
[7]Department of Computer Application, Manipal University Jaipur, Jaipur, India
[8]Department of Computer Science and Engineering, National Institute of Technology Delhi, Delhi, India
[9]School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India

data submission and retrieval from the cloud. Customers with restricted computing resources can re-adjust their large estimate unparalleled principal employment to the cloud by focusing on distributed calculating [1]. Providing perfect verification, examining information bundles, and determining modules to carry out the project are the key concerns of this inquisition, and as such, it is being conducted. It can be gauged that each customer is concerned about storing and retrieving their data files. In the era of cloud computing, data security is increasingly critical. Because of this, monitoring has developed into vigilance, which isolates the complexity of the monitoring process from the observer. Security planning in response to client demands is always computationally too expensive because of many variables. Therefore, prospects are concerned about the verified condition while executing private requests. Accordingly, this article describes a safe technique of communicating client data via the cloud to address these concerns. Internetworking environment creates secret hare keys through the process of synchronization. This will be merged with a data packet transferred to the cloud through encryption performed by and mixed with the model. These secure data packets are subsequently transmitted through a public network, where monitoring is employed to prevent information leakage to an unauthorized individual or group of people. Information owners do not have the necessary cohesiveness [2] to outsource cloud storage on purpose. When the distribution of this model addresses the trust issues between data owners and cloud networks, data owners will change their attitude toward the collection of cloud stores, thereby overcoming the confidence difficulties between cloud owners [3]. In a cloud setting, the capacity to exchange data among several users is important for success. A private cloud is being proposed for usage in the cloud in order to protect patient information privacy. The encryption of data before it is saved on a cloud server helps to preserve the privacy of the health information that is kept on the cloud server [4]. By doing so, we may be able to restrict the user's ability to do keyword searches. Because it is difficult to search for plaintext in encrypted data [5]. A keyword search strategy is necessary once more in order to discover the encrypted source file, albeit this time the method is more complicated to implement. The most essential qualities of the system are its effective key management along with its safe storage and retrieval of sensitive information.

1.1 Data Privacy

Data owners are extremely cautious to keep their data anywhere other than inside their control constraints due to security weaknesses in looped figuring. Also, confirming data in remote regions has become a significant source of mental anguish for indispensable professionals. The investigation's primary focus is on data security in the cloud's organizational structure. For the most part, cloud customers are not aware of the security techniques acknowledged by cloud service providers since they are primarily concerned with disseminating information to a mass audience over the internet and supplier assurance [6]. It was believed that the request made by market sellers did not provide relevant and appropriate information, despite many efforts made by the government to assure the collection of information.

1.1.1 Attackers on cloud

The two prominent techniques of exploiting cloud archives exist in external assaults and attacks within the cloud's internal architecture (structure). In this case, the outside aggressors are software developers who ambush data coming from outside the jurisdiction of the cloud service providers. Officials from cloud computing organizations with genuine benefits over enlisting resources are considered inside aggressors. Data security continues to be questionable in the progression of conveyed processing with respect to the arrangement, construction, and association instruments [7] (Fig. 1).

Customers do not grasp where data is stored during registration appropriation because of dispersed figuring, which confuses them. The concept of distributed figuring confuses customers as to where their data is held upon registering. Customers must build security measures in the presence of CloudPro centers since the data confirmation segment has been altered to deter external attacks. To increase and supply

data security in the future, masters and academia must build models for secret client data protection. This study analyzes and solves the exact issue potential customers encounter by providing data security models for cloud storage facility designs.

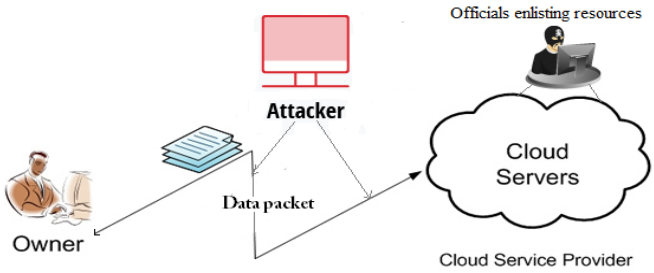

Fig. 1. Attackers on the cloud.

1.2 Research Goals and Objectives

The first goal is to develop a comprehensive information assurance system that will ease customer concerns while increasing the usage of cloud-based information storage and retrieval operations. Currently, information is considered a static piece that an insurance company cannot safeguard, so they must rely on each other. If public trust in cloud-based administration is not upheld, expanding the range of cloud-based services will be undermined [8]. This study is being done to overcome the issues mentioned above—goals of the study are to identify variables that affect information security, protection, and controllability in cloud systems. A second goal is to examine alternative solutions to issues of reliability. The information structure is novel and allows information to self-ensure and self-protect itself. This test will determine whether or not the proposed data flow system via the cloud meets the relevant information assurance criteria. The purpose of this project is to provide a fully secured and protected chain mechanism [9, 10] for data storage and retrieval over the cloud. This ensures that data is stored and retrieved safely from a cloud server.

1.3 Scope of the Paper

Conveyed figurative work warrants a significant amount of research. Everything from the establishment to the stage and programming was available on a pay-per-use basis. This notion is based on the fact that datasets are grouped in the cloud storage structure. Any security flaw in a customer's dataset stored in a cloud storage facility will undermine the client's faith in the system. Cloud master communities must verify that security breakdowns are prevented to earn their consumers' trust. Specifically, we'll be looking for information on dealing with cloud specialist centers that provide mysterious protection for their customers' data. There is the established assumption that cloud professional associations can never be trusted with unstable customer data and the cloud provider has ordered all of the customers' data. The proposed systems provide a key management scheme to improve efficient and privacy-preserving data storage and retrieval which are its most significant features. The key contribution of this paper is to encrypt data before it is stored on a cloud server and to provide a safe cloud storage platform for storing and retrieving data. The user may also utilize the system's keyword search capability to identify a suitable file for their purposes.

2. Related Work

The primary research query concerning cloud computing concerns how to ensure the order of a client's data on the cloud. Client data is stored in distributed storage providers, which the customer should

validate. Distributed computing has proved to be a consistent success in information technology (IT) and will continue to dominate IT organizations [11] going forward. On the other hand, cloud computing is beset with incredible difficulties, and is shaping to become increasingly important [12] to secure the appropriate physical, canny, and employee security safeguards, particularly in the cloud data collection industry. In addition, in transmitting such huge volumes of data, it is possible that the arrangement of the data may not be completely dependable. This zone represents the investigation efforts relevant to maintaining the security of data in distributed storage.

2.1 State-of-the-Art

This is a term referring to a cutting-edge model for rising preparation in which it is possible to use machines in far-reaching server ranches for passing on to organizations in a flexible manner [13]. As organizations have progressed to requiring large-scale shoddy figuring, cloud enrolling has emerged as a buzzword. There are several facts associated with circulated processing, including the possibility of guileful influence groups gaining access to information maintained through this evolution. Furthermore, cloud computing is a promising [14] technological development that standard professionals have recently become acquainted with. The use of vast volumes of data, electronic thinking, new information, and communication breakthroughs has prompted reasonable advancements and an increase in the size of the business workforce. As of now, cloud organizations are appointed with special system requirements for several forms of business connectivity. These requirements were met by several distributed registration configuration layers, such as establishment, stage, or programming as an organization, among others. As a result, the nature of information technology organizations has undergone dynamic changes, and associations have been arm-twisted to review their plans and consider implementing a suitable processing structure [15], which may contribute to attaining and improving business objectives.

Attribute-based encryption is a splendid preference for data affirmation in data re-appropriating structures, such as sent figures. The use of an encryption framework, on the other hand, may need some standard operations to be retrained over a mixed dataset, primarily in the field of data restoration. Attribute based data retrieval with proxy re-encryption (ABDR-PRE) is demonstrated in this study [16] to assure that both fine-grained get the chance to control and recover over the figure works while showing a property-based data recuperation using go-between re-encryption (ABDR). The proposed arrangement achieves fine-grained data delivery to the board by accepting the KP-ABE framework; a delegator can create the re-encryption key and look records for the figure works to be shared over the goal agent's attributes, as well as make the re-encryption key and look records for the figure works to be transmitted over the goal agent's attributes. The calculation of the Advanced Encryption Standard (AES) [17] is one of the world's most notable and widely utilized symmetric square figure estimate techniques. This estimator has a defined structure that allows it to encode and comprehend complex data, and is used in equipment and programming the world over to do this. In the case of AES computation, it is challenging for software programmers to obtain accurate data while encoding.

According to the current design, every bit of information and substance is being stored in the cloud owing to distributed capacity organizations. The vast volume of data collected from each customer may influence the delivered material. This strategy is commonly used to reduce the limited cost and resource needs of data benefits in the cloud by eradicating redundant information and storing only one copy of each piece of information. De-duplication [18] is most effective when many customers re-appropriate comparative data to the suitable stockpiling organizations, although it raises concerns about pursuit and security.

San Francisco-based Salesforce Inc. (https://www.salesforce.com) [19] is a distributed computing and social undertaking programming-as-a-service provider that specializes in customer relationship management (CRM). The Salesforce CRM item, which includes Sales Cloud, Service Cloud, Marketing Cloud, Force.com, Chatter, and Work.com, is its most prominent cloud stage and application. Salesforce is a cloud-based platform and application that allows businesses to manage customer relationships.

The sophisticated Salesforce platform's abilities continue to expand as more advanced technology develops. The ability to control sales connections progresses on pace due to implementing a cutting-edge CRM framework [20]. This research illustrates a range of recent technological developments that assist a multichannel approach to deal with the structure of successful customer relationships. Rather than maintaining a fleet of laptops and tablets, organizations opt to retire them to update their business groupings.

Cloud processing is described in this study, allowing clients to remotely store and retrieve their information based on interest management without the burden of local information hoarding and protection [21]. In any event, the guarantee of protecting the private information handled and created throughout the computation is increasingly becoming a legitimate security issue for everyone. In its most basic form, distributed computing enables clients with limited computational resources to redistribute their enormous calculation outstanding workloads to the cloud and financially benefit from the massive computational power, data transmission, stockpiling and even appropriate programming that can be reaped as compensation for each utilization method shown in Table 1.

Table 1. Comparative analysis of exiting work

Study	Service throughput	Service availability	Utilization/ scalability	Application circumstances	Limitations/gaps
Dhaya et al. [17]	-	-	Yes	IaaS/PaaS, I/O-based operation performed	Service authentication
Dickinson et al. [18]	Yes	Yes	Yes	S3, Azure	Required SSL certificate to validate
Casola et al. [19]	Yes	Yes	Yes	AWS/ PaaS	Limited platform
Celiktas et al. [20]	Yes	Yes	Yes	GCB, run data sensitive app	Complex architecture
Tabassum et al. [21]	-	Yes	Yes	Service-oriented app	Throughput is not reliable

This paper describes the monitoring measures so that the most excellent possible use of the could min algorithm may be made for the information. With the growth in internet traffic and demand for more resources, sketch-based solutions have been proven to reach greater levels of accuracy [22] for the same price as what conventional methods used to perform.

The proposed technique [23] aims to address a weakness in user clustering caused by a lack of comprehensive utilization of contextual information such as cloud service placement and an inefficient way for identifying the similarity of two vectors. The Scream dataset examination suggests a decrease in the cloud service recommendation process error rate.

Immutability, transparency, and a distributed structure are all advantages of blockchain technology, which serve to mitigate these disadvantages. An Internet-of-Things (IoT) solution based on blockchain technology is presented in this study to help identify intruders through virtual surveillance [24]. As a result of the blockchain-based tamper-proof data storage, this application has a significant advantage over other monitoring methods.

Deep learning has been extensively researched and deployed at the cloud and edge levels to enable accurate data analysis with minimal latency [25]. But studies have yet to address centralized administration, adversarial attacks, security, or privacy.

3. Research Methodology & Proposed Work

The main aim of this component is to introduce a few types of procedures utilized for accomplishing the destinations, and to answer the varying questions. The technique will introduce a secrecy security model to ensure client information in cloud frameworks [26]. We have included all of the investigations of ventures to fledgling in the research strategy, while issues are inquired about for achieving the privacy goals.

3.1 Methodology

Going for correct and gene unity of data is a prime need in a PC framework and correspondence systems. Single direction keygen cryptography is applied to encode a data packet into a fixed length and specify the marking. The counterfeit neural system permits consolidating, scattering, and compacting is the information succession of bits. Later, securing against man in the middle attacks and birthday assaults monitoring will be used. Previously, it was accounted for that generally utilized hash works as MD5 and SHA-1 [27] never gained security. So, we are leveraging neural system innovation to create hash codes to meet down-to-earth necessities. Sending and receiving data over this process is converted into a practical execution model developed by Salesforce.

3.2 Architecture

While developing this model, the system engineering team incorporates a theoretical model to describe the system's viewpoints, structure, and behavior. The model's design enables the project's execution, acquisition, maintenance, correction, and future development. The cloud archive framework's system architecture, depicted in Fig. 2, comprises numerous segments and their corresponding relationships.

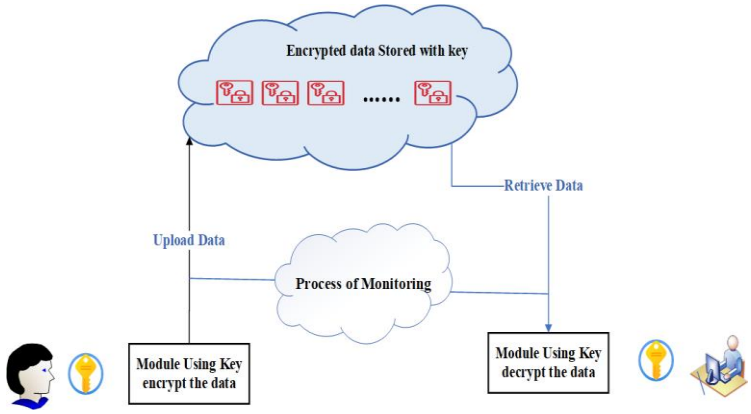

Fig. 2. Proposed model architecture for data security.

In Fig. 2, “System architecture for cloud archive framework permission” would be granted to a client, as defined in the framework design, to log into a nearby client area. The critical age and encryption module are used to generate the mystery key when a particular encryption computation is used. When a record with explicit content is sent to distributed storage, this module converts it to a record with figure content. Naturally, this technique results in the creation of a mystery key. The customer-facing modules are located on the model's customer-facing side. Subsequently, the encoded document is moved to the cloud vault framework, which is located on the model's cloud side of things. It is a cloud archive architecture-based distributed storage framework, and contains distributed storage servers connected to the reinforcing foundation through fiber optic cables to ensure consistency. A cloud customer leases this space from a cloud specialist organization and pays for the volume of data transferred on a per-transfer basis [28, 29]. As a result of this approach, storing the transmitted figure data in an encoded organizational structure is necessary. The download module enables an authorized client to download encrypted figure content from the cloud store framework. Customers who have been assigned an access key will have access to this module and the ability to download records. Controlling and disseminating the access key is the responsibility of a framework head. The process's unscrambling module is located at the client's end. This program must decode the downloaded figure content structure on the client's PC. Unscrambling figure material warrants the provision of a secret key by the client.

3.3 Proposed Approach

The entire procedure is isolated into the following three different stages. One process is in the client intra-network, another one is on the cloud base module, and the third one is monitoring it. In this approach, the main idea is to keep the data in safe mode on the cloud to transfer a key-generated data packet to the cloud. Also, as seen by the different types of hackers on the network, a monitoring system is to be applied to check the sender's correct order at the receiver's end shown in Fig. 3.

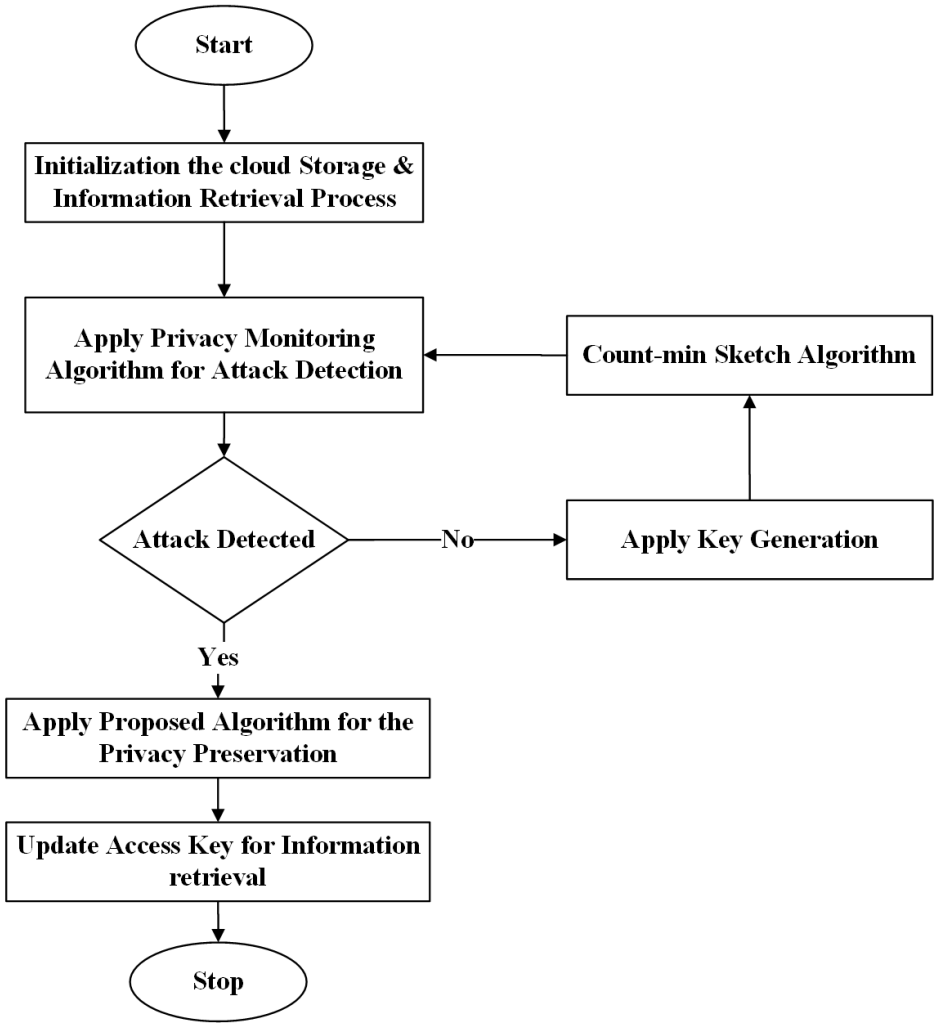

Fig. 3. Proposed workflow chart to preserve data privacy over the cloud.

3.3.1 Key generation

During the first stages of the synchronization process, the tree parity machines of A and B begin with weight vectors w_iA/B that have been picked at random and are not correlated. A random K public input vectors x_i is created in each time step, and the matching output bits A/B are computed for each of the K time steps. Following that, A and B send their output bits across the network. If they differ, $\tau_A \neq \tau_B$, the weights are not modified [30]; otherwise, they are. A neural system-based learning rule suited for synchronization of mystery key age system must be implemented if none of the preceding learning rules is applicable. The weights of the machines are equal once they have been synchronized. They can be used

in the construction of a shared key pair. In any case, only weights are affected by these learning rules, which are stored in hidden units with the $\sigma_i = \tau_i$ formula. The Hebbian learning rule concept is applied in this study as follows:

$$w_i + + = \ w_i + \sigma_i x_i \, \theta(\sigma_i \tau) \, \theta(\tau_A \, \tau_B). \tag{1}$$

3.3.2 Module for sending and retrieving data

A cloud computing and social undertaking programming organization regulates contact information and directions online for persistent customers. A module has been made to send the key delivered group and recoup it affirmed. This module has been developed by Salesforce. The main focus of this module is to fetch the value of the mystery key stored in a file and associated with each record that moves to the cloud. Later, when the data records were accessed, the key was compared with the saved vital file, and it did get the record of being open; otherwise, it indicated an error.

3.3.3 Secure count-min sketch

The security issue in network a refreshed sketch-put together calculation based concerning count-min empowers to secure traffic checking over the cloud. The count-min sketch query is a query operation that seeks the maximum or minimum data among the data items gathered in the specified epochs and region [31]. As an outcome, the following MAX/MIN inquiry, represented by a triple tuple, will be considered:

$$Q = (\Theta, T, \Gamma), \tag{2}$$

where MAX, MIN represents the query type, T the set of requested epoch numbers, and denotes the queried sensor node IDs indicating a query region.

For example, $Q = (\text{MAX}, t, \{s_1, s_4, s_6, s_{11}\})$ where query $\Theta \in \{$ MAX, MIN$\}$ seeks the highest volume of data gathered by sensor nodes $\Gamma \subseteq \{s_1, s_2, \ldots, s_n\}$. In epoch *t*, we will concentrate on the basic MAX query targeted at one cell $(\mathcal{M}, \{s_1, s_2, \ldots, s_n\})$ and one epoch *t*; that is, $Q = (\text{MAX}, t, \Gamma)$, where, $\Gamma \subseteq \{s_1, s_2, \ldots, s_n\}$. Other complex searches spanning many epochs and cells can be readily decomposed into multiple simple ones. As seen on system traffic, the observing assignment is to follow the recurrence of the data packet by applying the refreshed count-min the sketch calculation's actualized hash capacity that will slam into an IP address of related utilized. After the related emit key, the bundle is anticipated by the aggressor because it is not ready to fit for foreseeing the idea of parcel information [32], just by watching the parcel aggressor not prepared to perceive the structure while knowing about observing calculation. Due to the key being obscure to the aggressor, it turns inexhaustibly unbending to the aggressor to crash. By looking for the base value, the proposed analysis determines the worth followed on a single information structure. The sum of all estimations is the value returned by the system, which figures the target counter for each section, to be examined of the data structure [33], and later re-establishes the base worth found for determining a real or fake IP.

3.4 Base Algorithm

Two base algorithms are to be taken to implement the concept, one from key generation and another from monitoring.

3.4.1 Neural key exchange algorithm

The collaborative learning synchronization of two neural networks may be utilized to create the neural key exchange protocol. The main difficulty is determining how to evaluate synchronization without a weight vector. All previous approaches delay evaluating synchronization, which impacts the security of the neural key exchange. An enhanced approach for measuring the synchronization of neural networks is provided to analyze the synchronization more rapidly and precisely. Firstly, the frequency with which the two networks have the same output in previous phases is utilized to measure their degree overall.

Secondly, when the degree surpasses a certain threshold, the hash function determines whether the two networks have achieved full synchronization. The enhanced approach can find full synchronization between the two networks using only the hash value of the weight vector. There are *K* perceptrons with separate receptive fields in each of the hidden units. Each neuron has *N* inputs and 1 output for *N* neurons (Algorithm 1). The input is entirely binary as denoted below:

$$x_{i,j} \in \{-1, +1\}. \tag{3}$$

Additionally, discrete values between $-L$ and $+L$ establish the input and output mapping.

$$w_{i,j} \in \{-L, -L+1, \dots, +L\}. \tag{4}$$

When the indexes *j*=1, *N* are used to denote the vector elements. The indexes *i*=1..., *K* denotes the i^{th} remote unit of the tree parity machine, and the indexes *j*=1..., *N* denote the vector elements, respectively.

$$h_i = \frac{1}{\sqrt{N}} w_i \cdot x_i = \frac{1}{\sqrt{N}} \sum_{j=1}^{N} w_{i,j} x_{i,j}. \tag{5}$$

The output σ_i of the i-the hidden unit is then defined as the sign of h_i as follows:

$$\sigma_i = \mathrm{sgn}(h_i).$$

Then, the total output τ of a tree parity machine is given by the product (parity) of the hidden units as follows:

$$\tau = \prod_{i=1}^{K} \sigma_i. \tag{6}$$

As a result, if the number of inactive hidden units with _*i*=-1 is even (=+1) or odd (=-1), the value merely shows that fact. As a result, there are 2 (*K*–1) distinct internal representations (1, _2, … *K*), all of which lead to the same output value. For a situation where there is just one remote unit, the symbol is equivalent to 1. As a result, the tree parity machine with *K*=1 exhibits the same behavior as a perceptron, which may be seen as a specific instance of the more sophisticated neural network described above.

Algorithm 1. Neural key exchange algorithm

Input: Parameters: Input layer, hidden layer
Output: Secret key for critical exchange to share the data

Procedure: Start

Step 1:	Initialized the input parameters of the neural network;
Step 2:	Initialized randomly to all network weights of hidden layer;
Step 3:	Calculate the input and feed and compute their weight;
Step 4:	Repeat Steps 4 to 7 until synchronization occurs in the network;
Step 5:	Compute the input of hidden layer;
Step 6:	Exchange of output bit between two machine A and machine B;
Step 7:	Comparers the output vectors of both the machines are identical, i.e., $\tau_A = \tau_B$.
Step 8:	The Hebbian learning rule, the anti-Hebbian learning rule, and the random-walk learning rule are all used to modify the weights of the corresponding variables.
Step 9:	After perfect sync, the synaptic weights in both networks are the same as one another.
Step 10:	Computed weights are used as a secret key.

3.4.2 Count-min sketch algorithm

When presented with a data stream featuring the count–min sketch functions as a probabilistic data structure that serves as a frequency table of events, the mapping of events to frequencies is accomplished by using hash functions (Algorithm 2).

Algorithm 2. Count-min sketch algorithm

Input: Frequency of input bit (r, c)
Output: Encrypted hash function

```
initialize (r, c) do
    F [1 . . . r, 1 . . . c] ← 0r, c
   h1, . . ., hr: [n] → [c] // r hash functions from a 2-universal family.
end initialize
function update (tj, ωtj) // reads item tj with value ωt from the stream σ
   for ı = 1 to r do
        F [ı, hı(t)] ← F [ı, hı(t)] + ωtj
  end for
end update
 get_Estimation(t).
       returns ft
       return min {F [ı, hı(t)] | 1 ≤ ı ≤ r}
end function
```

3.5 Proposed Algorithm

Execution of complete circle of data over the cloud using both neural key exchange and count-min sketch algorithms is to be modified and attached with the Salesforce application. Customers often access public, commercial cloud services through the internet, whereas private/ hybrid cloud services must be accessed over the company's internal network. A service's total performance is reflected in its cloud infrastructure and the network that connects it to end users. A user's perspective on cloud service performance should therefore consider both service and networking.

3.5.1 KeyGen algorithm

A persuasive method to accomplish the objectives is to substitute the first hash work by putting an arbitrary key worth using info. as a solid key. It becomes difficult for beast power to make hash impacts with the goal. Because system observing is frequently required to be dynamic, it must be changed at each association at runtime. If it is necessary to re-establish the key as precision profits by keeping this value low, the sum of lines of the sketch could be a decent measurement to choose. Counters on their way to reaching their maximum value should also cause a significant shift. As a result, it is impossible to imagine exchanging the key and using the same information structure because two identical objects would be assigned to different locations. Consider a switching period to be the time between two events in which a switch of some kind presses a comparable key. After each checking period, an essential recharge should be performed, while the information structure should be copied to an alternate memory before the key is discarded (Algorithm 3).

Algorithm 3. KeyGen algorithm

Input: Number of Input Layer, hidden layer
Output: Generated secret KeyGen

Step 1:	Fixed the value of *k* as 8, hidden layer auto increment in n and set input layer units in Step l;
Step 2:	The network weights to be initialized randomly;
Step 3:	Repeat Steps 4 to 7 until status becomes zero;
Step 4:	The inputs of the hidden units are calculated.
Step 5:	The output bit is generated on 32 bits indicating the length of the key.
Step 6:	A time slap is calculated on each slot on a generated key.
Step 7:	Weights are modified using the Hebbian learning rule till symbolization does not occur.

Step 8: After complete synchronization, the synaptic weights are stored in a secret key file.

3.5.2 Updated monitoring algorithm

In this regard, it should be noted that estimations that rely on more than one information structure will not have the same exactness guarantees as to the first count-min calculation, with most of the error of the count-min calculation increasing in proportion to the number of information structures on which the estimation is predicated. However, because item values are often obtained on an as-needed basis for a limited time period, the executive only has to preserve the put-away information structures still necessary for the estimations on hand. The more established ones can be removed, ensuring that the accuracy is only slightly altered in a limited way overall. In contrast to a hash table, this approach uses sub-linear space to count the number of times a frequency occurs. There are “w” columns and “d” rows in a matrix, which is made up of that. The parameters establish the trade-off between precision and the limits of space and time on the system. Each row has a hash function that is connected to it. When an element is received, a hash for each row is discovered. The index of the matching row in the table is increased by one. The worth returned by the approach is the sum of all of the assessments made by the participants. According to the procedure, the objective counter is calculated to be examined once for each line of the information structure. The base worth is estimated once those gains are obtained (Algorithm 4).

Algorithm 4. Privacy monitoring algorithm

Input: wid, hei, and nip
Output: Corresponding index for the matrix to generate a key

```
Execute random (1:9) // to generate a number between 1 to 9
A[i][j] = wid[i] * hei[j]
Execute procedure fiddlehead up to counter value
Packetforwarded ()
Procedure findkeyhead ()
        input = <w, d, nip>
        tCol = rand(key) %width
       tSlot = tRow + tCol
           if tr == 0 then
     rowRes = counter_read ("c”, tarSlot)
  Break
Else
          if rowRes =counter[tarSlot]
          end if
        result = minimum (result, rowRes)
        tRow = tRow + width
Return tRow
```

4. Implementation and Results

This section summarizes the results obtained from implementing the experimental output. The algorithms proposed to execute the keygen and results obtained through MATLAB, with the method for locating interruptions provided. Finally, the test is displayed, and discussions about the execution of the discovery strategy are presented [29, 34]. Also attached is a screenshot of the developed module from Salesforce, indicating our real-life execution task. Based on their research methodologies, the currently available approaches to evaluating cloud service performance are divided into the two categories of measurement-based approaches and analytical modelling-based approaches [35]. The latter includes queueing theory-based, network calculus-based, and other stochastic models such as SRN-based methods.

4.1 Key Generation Output

The KeyGen algorithm generates a 20-length stream character when implemented on MATLAB. This program contains characters and special symbols for using randomized keys shown in Table 2. Fig. 4 shows the different values of *t* with *n* input units.

Table 2. KeyGen of input units

	Parameter	Value
Input unit = 1	*t*	0.5676
	No. of hidden units	8
	Length of key	20
	No. of iterations	786
	Generated key	@@@@@@@@@@@@@@@@@@@@
Input unit = 2	*t*	0.3913
	No. of hidden units	4
	Length of key	20
	No. of iterations	464
	Generated key	$) %! #&%# %#'%#&%#%$(
Input unit = 3	*t*	0.8682
	No. of hidden units	4
	Length of key	20
	No. of iterations	787
	Generated key	%! $)#$)" $'%)"!!&!&
Input unit = 4	*t*	0.7271
	No. of hidden units	4
	Length of key	20
	No. of iterations	534
	Generated key	&&-) #)/0)!'- (&*%'("$
Input unit = 5	*t*	1.2080
	No. of hidden units	4
	Length of key	20
	No. of iterations	749
	Generated key	# (, /- (#%%!"*) "%&&+
Input unit = 6	*t*	4.1877
	No. of hidden units	4
	Length of key	20
	No. of iterations	2,239
	Generated key	$$&'-) %$(, $&- (&)) (()
Input unit = 7	*t*	3.4139
	No. of hidden units	4
	Length of key	20
	No. of iterations	1,604
	Generated key	/-1.-311+--,'*+. ())
Input unit = 8	*t*	11.5521
	No. of hidden units	4
	Length of key	20
	No. of iterations	4,850
	Generated key	/, -*'-14-+*012/0, -'+

4.2 Monitoring Algorithm Output in Different Phases

In addition, the uncertainty related to the estimations produced by a secured sketch, as indicated in Tables 3–6, respectively were analyzed in MATLAB. In this example, five IP packets are evaluated as a sample of traffic gathered on the network's access point to the internet, as depicted in Figs. 5 and 6.

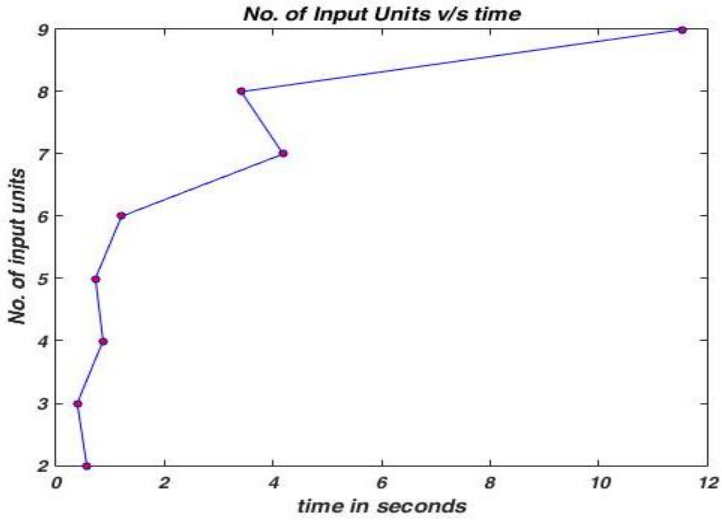

Fig. 4. KeyGen time versus input unit.

Table 3. Number of IPs add read per iteration

(Value of X)	(Value of Y)	
15	6	9
16	4	12
17	4	13
18	10	8
19	3	16

Fake IP add: 582 515 418 0 0 0 0 0 0 0. Total number of errors is 3.

Table 4. Sketch values

831	931	531	631	731	131	331	431
782	982	682	382	882	482	282	182
333	433	633	833	733	233	933	133
784	284	184	384	684	884	484	584
615	415	715	215	915	815	115	315
286	486	386	986	886	686	586	786
697	297	797	497	997	597	397	197
218	318	618	518	818	718	118	918

Table 5. Random generated IP

234	982	234	758	297	365	0	0	0	0
436	983	983	154	0	0	0	0	0	0
492	734	492	492	0	0	0	0	0	0
818	818	243	818	818	454	116	243	116	454
582	515	418	0	0	0	0	0	0	0

Table 6. Counter values

6	4	1	3	3	2	2	1
3	3	3	2	1	3	5	1
2	3	2	3	3	1	1	1
7	5	2	3	3	2	4	1
5	1	2	1	3	2	3	1
5	2	1	3	2	2	2	1
3	8	1	1	1	1	1	4
6	4	3	3	4	2	2	1

The value of *k* is 3 8 3 8 1 8 9 1.

The randomized packets executed in the cloud pathway, through which the network switch could process them all, are shown in Fig. 6. Each packet is monitored and the sketch for the item is queried. This process provided an estimated frequency and the true frequency specifying the error. Analysis of experimental data and comparisons with the existing system [23] resulted in showing that it improves the storage efficiency by 3.6%.

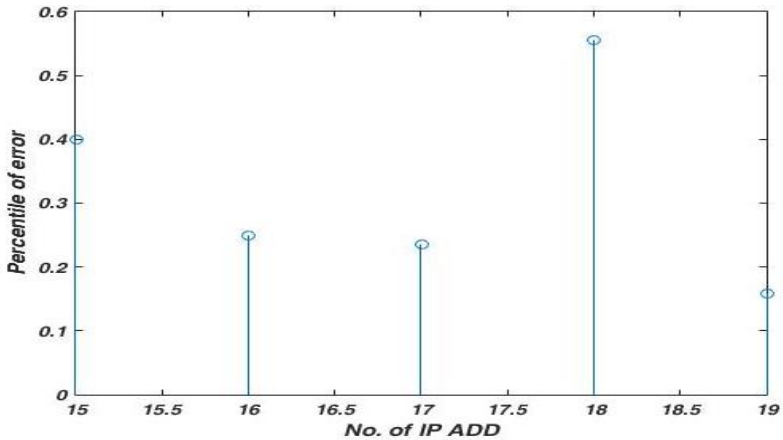

Fig. 5. Percentile of an error on specified IP.

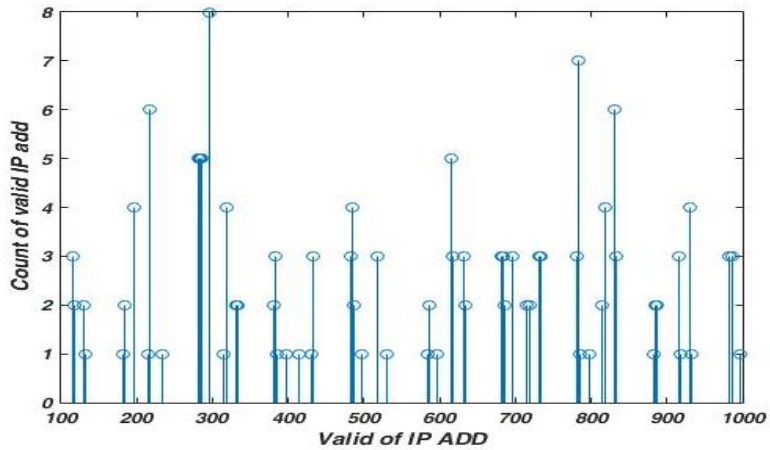

Fig. 6. Resultant of valid IP.

5. Conclusion and Future Scope

As seen in the real world, most businesses and customers individually lack the infrastructure needed to keep their data safe on the internet. With cloud storage prices getting prohibitive, it is becoming increasingly attractive to use cloud storage for various purposes cost-effectively. The proposed framework provides more robust security because it is not helpless against any known leap. We could hear about a beneficial system built in such a manner that it accomplishes input/ yield protection, clever flexibility, and productivity in the cloud, among others. While data is stored in a cloud repository, it is kept encrypted. For a user to access the cloud and download encrypted data, they must first obtain an access key. With the correct access key, the user will access the cloud repository and download the encrypted data to a local computer installed at one's location. To decode this information, the user will also need a secret key. As such, it is advised that users encrypt data at their end before uploading it to cloud storage servers to keep costs down and confidential material safe from prying eyes. This paradigm enables the user to keep track of secret keys they have created. As for the duty for encryption, now the onus is on the user for crucial management and critical storage. This model works on specific attack models and manages the cryptographic key, especially its distribution, to mitigate the attack. Thus, it is suggested to analyze the behavior of more cloud models and their loopholes related to data privacy.

Author's Contributions

Conceptualization, AK, KUS. Investigation and methodology, TA, LR. Supervision, SYH. Writing of the original draft, AK, KUS. Writing of the review and editing, TA, KUS, JKS, RKM, TS, SYH. Formal analysis, TS, LR.

Funding

None.

Competing Interests

The authors declare that they have no competing interests.

References

[1] M. Xu, D. Wang, Q. Wang, and Q. Jia, "Understanding security failures of anonymous authentication schemes for cloud environments," *Journal of Systems Architecture*, vol. 118, article no. 102206, 2021. https://doi.org/10.1016/j.sysarc.2021.102206

[2] L. Yang, H. Qin, J. Zhang, H. Su, G. Li, and B. Bai, "Cloud model for security state recognition based on factor space," *IEEE Sensors Journal*, vol. 21, no. 22, pp. 25429-25436, 2021.

[3] P. Zhang, H. Chi, J. Wang, and Y. Shang, "Data security protocol with blind factor in cloud environment," *Information*, vol. 12, no. 9, article no. 340, 2021. https://doi.org/10.3390/info12090340

[4] N. Sathyabalaji, G. Komarasamy, and S. D. M. Raja, "Secure and privacy-preserving keyword search retrieval over hashed encrypted cloud data," *International Journal of Communication Systems*, vol. 33, no. 5, article no. e4272, 2020. https://doi.org/10.1002/dac.4274

[5] A. Razaque, M. B. H. Frej, B. Alotaibi, and M. Alotaibi, "Privacy preservation models for third-party auditor over cloud computing: a survey," *Electronics*, vol. 10, no. 21, article no. 2721, 2021. https://doi.org/10.3390/electronics10212721

[6] T. Zhao, T. Gasiba, U. Lechner, and M. Pinto-Albuquerque, "Raising awareness about cloud security in industry through a board game," *Information*, vol. 12, no. 11, article no. 482, 2021. https://doi.org/10.3390/info12110482

[7] R. Punithavathi, M. Kowsigan, R. Shanthakumari, M. Zivkovic, N. Bacanin, and M. Sarac, "Protecting data mobility in cloud networks using metadata security," *Computer Systems Science & Engineering*, vol. 42, no. 1, pp. 105-120, 2022. https://doi.org/10.32604/csse.2022.020486

[8] G. Sharma, G. Bousdras, S. Ellinidou, O. Markowitch, J. M. Dricot, and D. Milojevic, "Exploring the security landscape: NoC-based MPSoC to cloud-of-chips," *Microprocessors and Microsystems*, vol. 84, article no. 103963, 2021. https://doi.org/10.1016/j.micpro.2021.103963

[9] M. M. Salim, I. Kim, U. Doniyor, C. Lee, and J. H. Park, "Homomorphic encryption based privacy-preservation for IoMT," *Applied Sciences*, vol. 11, no. 18, article no. 8757, 2021. https://doi.org/10.3390/app11188757

[10] J. Cha, S. K. Singh, T. W. Kim, and J. H. Park, "Blockchain-empowered cloud architecture based on secret sharing for smart city," *Journal of Information Security and Applications*, vol. 57, article no. 102686, 2021. https://doi.org/10.1016/j.jisa.2020.102686

[11] R. Sivan and Z. A. Zukarnain, "Security and privacy in cloud-based e-health system," *Symmetry*, vol. 13, no. 5, article no. 742, 2021. https://doi.org/10.3390/sym13050742

[12] Z. Li, V. Chang, H. Hu, D. Yu, J. Ge, and B. Huang, "Profit maximization for security-aware task offloading in edge-cloud environment," *Journal of Parallel and Distributed Computing*, vol. 157, pp. 43-55, 2021.

[13] J. Lu, R. Xiao, and S. Jin, "A survey for cloud data security," *Journal of Electronics & Information Technology*, vol. 43, no. 4, pp. 881-891, 2021.

[14] G. K. Mahato and S. K. Chakraborty, "A comparative review on homomorphic encryption for cloud security," *IETE Journal of Research*, 2021. https://doi.org/10.1080/03772063.2021.1965918

[15] A. S. Mohammad and M. R. Pradhan, "Machine learning with big data analytics for cloud security," *Computers & Electrical Engineering*, vol. 96, article no. 107527, 2021. https://doi.org/10.1016/j.compeleceng.2021.107527

[16] D. S. David, M. Anam, C. Kaliappan, S. Arun, and D. K. Sharma, "Cloud security service for identifying unauthorized user behaviour," *Computers, Materials & Continua*, vol. 70, no. 2, pp. 2581-2600, 2022.

[17] R. Dhaya, R. Kanthavel, and K. Venusamy, "Cloud computing security protocol analysis with parity-based distributed file system," *Annals of Operations Research*, 2021. https://doi.org/10.1007/s10479-021-04413-5

[18] M. Dickinson, S. Debroy, P. Calyam, S. Valluripally, Y. Zhang, R. B. Antequera, T. Joshi, T. White, and D. Xu, "Multi-cloud performance and security driven federated workflow management," *IEEE Transactions on Cloud Computing*, vol. 9, no. 1, pp, 240-257, 2021.

[19] V. Casola, A. De Benedictis, S. Di Martino, N. Mazzocca, and L. L. L. Starace, "Security-aware deployment optimization of cloud-edge systems in industrial IoT," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12724-12733, 2021.

[20] B. Celiktas, I. Celikbilek, and E. Ozdemir, "A higher-level security scheme for key access on cloud computing," *IEEE Access*, vol. 9, pp. 107347-107359, 2021.

[21] N. Tabassum, T. Alyas, M. Hamid, M. Saleem, S. Malik, and S. B. Zahra, "QoS based cloud security evaluation using neuro fuzzy model," *Computers, Materials & Continua*, vol. 70, no. 1, pp. 1127-1140, 2022.

[22] L. A. Tawalbeh and G. Saldamli, "Reconsidering big data security and privacy in cloud and mobile cloud systems," *Journal of King Saud University-Computer and Information Sciences*, vol. 33, no. 7, pp. 810-819, 2021.

[23] H. Habibi, A. Rasoolzadegan, A. Mashmool, S. S. Band, A. T. Chronopoulos, and A. Mosavi, "SaaSRec+: a new context-aware recommendation method for SaaS services," *Mathematical Biosciences and Engineering*, vol. 19, no. 2, pp. 1471-1495, 2022.

[24] C. Rupa, G. Srivastava, T. R. Gadekallu, P. K. R. Maddikunta, and S. Bhattacharya, "A blockchain based cloud integrated IoT architecture using a hybrid design," in *Collaborative Computing: Networking, Applications and Worksharing*. Cham, Switzerland: Springer International Publishing, 2021, pp. 550-559.

[25] J. H. Park, S. Rathore, S. K. Singh, M. M. Salim, A. E. Azzaoui, T. W. Kim, Y. Pan, and J. H. Park, "A comprehensive survey on core technologies and services for 5G security: taxonomies, issues, and solutions," *Human-centric Computing and Information Sciences*, vol. 11, article no. 3, 2021. https://doi.org/10.22967/HCIS.2021.11.003

[26] V. R. Thakare and J. Singh, "A study of computational trust models in cloud security," *International Journal of Grid and High Performance Computing*, vol. 13, no. 3, pp. 1-11, 2021.

[27] C. Swarup, A. Kumar, K. U. Singh, T. Singh, L. Raja, A. Kumar, and R. Dubey, "Biologically inspired CNN network for brain tumor abnormalities detection and features extraction from MRI images," *Human-centric Computing and Information Sciences*, vol. 12, article no. 22, 2022. https://doi.org/10.22967/HCIS.2022.12.022

[28] S. Shamshirband, M. Fathi, A. T. Chronopoulos, A. Montieri, F. Palumbo, and A. Pescape, "Computational intelligence intrusion detection techniques in mobile cloud computing environments: review, taxonomy, and open research issues," *Journal of Information Security and Applications*, vol. 55, article no. 102582, 2020. https://doi.org/10.1016/j.jisa.2020.102582

[29] H. He, L. H, Zheng,P. Li, L. Deng, L. Huang, and X. Chen, "An efficient attribute-based hierarchical data access control scheme in cloud computing," *Human-centric Computing and Information Sciences*, vol. 10, article no. 49, 2020. https://doi.org/10.1186/s13673-020-00255-5

[30] B. Wang, C. Wang, W. Huang, Y. Song, and X. Qin, "Security-aware task scheduling with deadline constraints on heterogeneous hybrid clouds," *Journal of Parallel and Distributed Computing*, vol. 153, pp. 15-28, 2021.

[31] H. Wang, X. Chang, and K. Chen, "CLE against SOA with better data security storage to cloud 5G," *Security and Communication Networks*, vol. 2021, article no. 6695964, 2021. https://doi.org/10.1155/2021/6695964

[32] Y. Wei, S. Zhou, S. Leng, S. Maharjan, and Y. Zhang, "Federated learning empowered end-edge-cloud cooperation for 5G HetNet security," *IEEE Network*, vol. 35, no. 2, pp. 88-94, 2021.

[33] S. Rathore and J. H. Park, "A blockchain-based deep learning approach for cyber security in next generation industrial cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5522-5532, 2021.

[34] T. T. Khanh, V. Nguyen, X. Q. Pham, and E. N. Huh, "Wi-Fi indoor positioning and navigation: a cloudlet-based cloud computing approach," *Human-centric Computing and Information Sciences*, vol. 10, article no. 32, 2020. https://doi.org/10.1186/s13673-020-00236-8

[35] L. Megouache, A. Zitouni, and M, Djoudi, "Ensuring user authentication and data integrity in multi-cloud environment," *Human-centric Computing and information sciences*, vol. 10, article no. 15, 2020. https://doi.org/10.1186/s13673-020-00224-y