International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Deep Learning Based User Identity Management Protocol for Improving Security in Cloud Communication

N. Rajkumar*[1], M. Gokul[2], K. Sathees Kumar[3], N. Mohanasuganthi[4]

Submitted: 22/07/2022 **Accepted**: 25/09/2022

Abstract: These instructions Deep learning (DL) based methods for communication protocol design have recently been explored inside the cloud computing paradigm. These learning-based systems can eliminate the need for manual protocol parameter tuning. To this purpose, we present a new DL-based framework for designing and evaluating networking protocols in a methodical manner. The suggested user identity management protocols, System for Cross-domain Identity Management (SCIM) is used to safeguard cloud computing clients and providers. Deep learning techniques employing SCIM were used to improve security and scalability. By preventing unwanted users from gaining access to the service/facility, the suggested deep Learning with SCIM would secure customers/cloud service providers' infrastructure and safeguard data at all levels, which is crucial for cloud computing facilities.

Keywords: *Deep learning, SCIM, Security, Cloud Computing*

1. Introduction

As a platform for multicast communication among group members, cloud computing has developed. Data security in a cloud environment is very important because the data is protected by a third-party provider. Encrypting and storing data in the cloud is the primary method of data security [1]. However, a secret key needs to be generated and distributed securely among cloud users when exchanging data with a group of individuals. Recent study has identified a number of key challenges, most of which are related to cloud data security. Cloud computing technologies are advantageous to users. Users can employ the services offered by cloud service providers in place of building infrastructure with their own resources [2]. Customers that use cloud computing, on the other hand, delegate administration of their systems and data to a third party, needing a high degree of trust in the firm with whom they will be collaborating.

To offer security at the domain and cloud service provider (CSP) levels, the Security Framework and Cloud Security Protocol have been suggested [3]. At both the CSP and Domain levels, choices are made in a distributive fashion in the proposed work. This protects cloud data from illegal access. Today's Internet and mobile communications networks have resulted in networks that are growing increasingly large-scale, diverse, dynamic, and systemically complex [4]. Because of these applications' higher availability and performance needs, "general-purpose" protocol stacks are no longer adequate and must be replaced by application-specific protocols. Fig. 1 shows how a user communicated with a server through a trusted authority. Different sorts of clod services are connected to the server. Mobile Cloud Computing (MCC) [5] is a wireless network-based hybrid of mobile and cloud computing. This allows users to access the Cloud and use its many services, including storage and computing resources. At MCC, however, the most challenging task is security. MCC users must undertake secure online identity identification to protect their identities. Traditional and widely used authentication techniques fail when attackers can get a user's ID and password, for example.

In both academia and industry, cloud computing [6] has developed as a desirable computer paradigm. Virtualization technology allows cloud service providers with their own data centres to organise actual servers into Virtual Machines (VMs) to give services, resources, and infrastructures to customers [7]. Profit-driven CSPs charge consumers for service access and virtual machine renting while lowering power usage and bills to boost profit margins. The key issue for CSPs is to reduce data centre energy expenses.

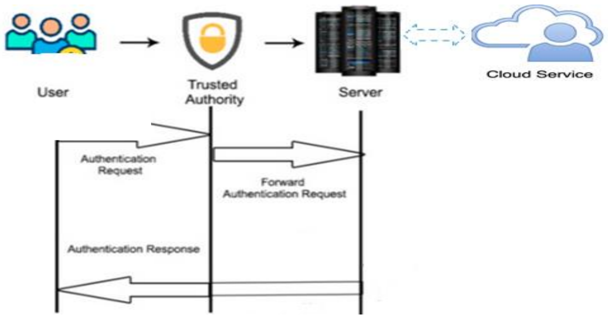

Fig. 1. System model for securable data transmission in cloud.

Various strategies for minimising energy expenditures via Resource Provisioning (RP) and/or Task Scheduling were proposed in previous studies (TS). They do, however, have scalability concerns or fail to address TS with task dependencies, which is a crucial aspect in assuring correct parallel task execution.

[1] *Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai – 600062, India*
ORCID ID : ORCID: 0000-0002-8216-8186
[2] *Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai – 600062, India*
[3] *Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai – 600062, India*
[4] *Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai – 600062, India*
** Corresponding Author Email: sivarajkumar.n@email.com*

Researchers are scrambling to apply deep learning to a range of protocol optimization problems, including as routing, congestion control, and the MAC protocol, to name a few. Human effort to fine-tune protocol parameters can be decreased using DL techniques. In this paper, we propose a DL-based paradigm for networking protocol optimization [8]. For instance, we focus our efforts on developing user identity management protocols using a DR-based architecture.

Integrating critical apps with governance solutions helps you to manage your identity and security procedures more efficiently and effectively [9]. Before allowing users the degree of access that the system has allocated, the identity provider might submit users' credentials to the service provider for authentication and authorisation.

1.1 The following is the contribution of this work:

» Created a system model for data transmission on cloud includes Query Processor, Load Balancer, Access control Policy and Cloud Database.

» Proposed mechanisms are well-equipped with data exchange and storage on the server.

» The suggested deep Learning with SCIM will protect customers/cloud service provider’s infrastructure by preventing unauthorized users to gain access to the service/facility.

The work is organized as follows: Section 2 discusses techniques, as well as a relevant work study and a literature review and also four important modules including Query Processor, Load Balancer, Access Control Policy and Cloud Database. Section 3 explored the proposed framework incorporates a number of measures for data security as well as channel security during inter-server communication. Result and discussion focuses on Section 4. Finally, Section 5 discusses the conclusion and the scope of future work.

2. RELATED WORKS

Shengmin Xu et al. [10] suggested a secure fine-grained access control and data sharing strategy for dynamic user groups that is efficient. The proposed scheme accomplishes this by: 1) defining and enforcing data-based access policies; 2) allowing the key generation centre to efficiently update user credentials for dynamic user groups; and 3) allowing untrusted CSPs to perform some expensive computation tasks without requiring a delegation key. The property of cypher text delegation and the coupled approaches of identity-based encryption were used to build an efficient revocable Attribute-Based Encryption (ABE). This technique is used in a cloud environment for on-demand services with a dynamic user group.

Sumagita and Riadi [11] presented a novel method for invoking a hash function, system repair code changes, and execution findings. Testing is carried through using user acceptability testing and penetration testing. Following patch usage, the input password is converted using the SHA 512 tool to a more secure hash algorithm for testing purposes. Hash functions are used in cryptography to guarantee data integrity, message authentication, and digital signatures. Hash functions are described as the function that compresses input of arbitrarily vast length into a small size fixed hash code. User acceptability testing and penetration testing are used for the application of the patch revealed that the inputted password had been changed to a more dependable hash function using the SHA 512 method, and the UAT result showed that result agreed and strongly agreed with 86, 00 percent. As a result, the implementation of the patch used to secure the password that was made during login can proceed as needed.

With an emphasis on the technology element and implementation layer, Ahmad [12] analyses several security issues in the context of cloud computing. He offers countermeasures to the security risks. Cloud computing is implemented as a software-only solution or based on cutting-edge virtualization technology supported by hardware. The article talks about cloud computing security concerns. The article also provides examples of security solutions for web services and virtualization, two of the key enabling technologies for cloud computing. It also describes the innovative idea of incorporating multi-level security into all cloud solutions as opposed to the idea of security as a service. The report concludes by mentioning crucial recommendations for creating service level agreements.

With their innovative idea of multi-level security against SaaS, AlZadjali et al. [13] produce a comprehensive manual for service level agreements that outlines everything we should pay attention to while negotiating these contracts. One must understand that hundreds of routing servers, database and mobile network servers, application and web servers, cloud servers, etc. are used during a single transaction of buying a product through mobile or system during online shopping, according to him. It should be highlighted that this transaction passes through a number of businesses, including the product owner, cloud provider, cloud producer, banking company, delivery firm, etc., and is therefore vulnerable to the dangers and security flaws existing in the broad cloud architecture. The author also provides a cloud computing technology framework that illustrates the many communication channels between Cloud Service Consumers, Cloud Service Producers, Cloud Service Providers, and Data Center Providers. The taxonomy of various sub-domains and domains will help you comprehend d the security challenges that the cloud architecture has to offer. Domains include (a) System virtualization (b) application programming (c) data (d) network and communication (e) commercial and legal difficulties, and their accompanying security concerns provided to locate and address the particular entity. The following Table 1 show the summary of survey.

Table 1: Summary of the survey

Authors	**Techniques**	**Methods**	**Conclusion**
Jian Shen , Member, IEEE, Tianqi Zhou, Xiaofeng Chen, Jin Li, and Willy Susilo [14]	It implements a group data sharing strategy for anonymous multiple users in public clouds using key agreement and group signature techniques	Symmetric balanced incomplete block design used for reliable and secure key agreement for sharing group data in a cloud storage system.	To securely share data among the group members, a conference key based on the key agreement protocol was employed.
Yue Zhang, Jia Yu, Rong Hao, Cong Wang and Kui Ren [15]	A novel key generation process was used, as well as a new private key updating technique. Rather than upgrading the authenticators of revoked users, this technique was used to update non-revoked private keys.	A novel storage auditing approach that allows users to be revoked regardless of the total number of file blocks they own in the cloud. This approach uses identity-based cryptography to cut the need for certificate managing in PKI systems.	Even if the authenticators are not changed, the integrity audits of revoked users' data can still be repaired.
Mazhar Ali , Revathi Dhamotharan , Eraj Khan , Samee U Khan , Athanasios V Vasilakos ,Keqin Li & Albert Y Zomaya [16]	The cryptography server holds the remaining portion. Using petri nets and the Z3 solver, this technique is tested and verified.	Secure Data Sharing in Clouds 1) data confidentiality integrity 2) Access control 3) Data sharing without using compute-intensive re-encryption; 4) Insider threat security 5) Forward and backward access control.	A single encryption key is used to encrypt the file, and two distinct key shares are formed, with the user receiving one of them. The user's possession of a single share empowers them to counter insider threats.
Sebastian Graf, Patrick Lang, Stefan, A, Hohenadel & Marcel Waldvogel [17]	Scalable technique - There's a difference between the keys used for encryption with hierarchical data and the encrypted updates on the keys that allow join and leave.	an adaptation for scalability and flexibility in key management in diverse contexts such as the cloud	This work makes use of cloud infrastructures to preserve data and key sharing confidentially in a collaborative setting.

The system model consists of three parts: 1. Cloud Customers 2. Cloud Service Provider 3. Trusted third party. 1. Cloud Customers: End users or clients who require cloud services. Each customer in this proposed system makes use of cloud service models. The TTP includes a new user by registering and providing a new customer id. 2. Cloud Providers: Providers are businesses that aim to deliver various types of cloud service models. 3. Reliable third parties: Certified agencies (servers) that can act as a middleware (server) between clients and providers. This agent approves and authorises both users and providers, as well as monitors all of their activities shows in Fig. 2.

2.1 LDAP

The Lightweight Directory Access Protocol, or LDAP, is a standard protocol for on-premise directories like Microsoft's Active Directory. LDAP is an identity management protocol that collects and organises data—such as user or device information—so that it's simple to discover. LDAP searches the directory contents and relays authentication and authorization information above the TCP/IP stack. Because legacy LDAP is based on plain text, it is not a secure protocol, therefore corporations have started migrating to LDAPS, or LDAP over SSL. LDAPS protects credential theft by encrypting LDAP data in transit between the server and the client.

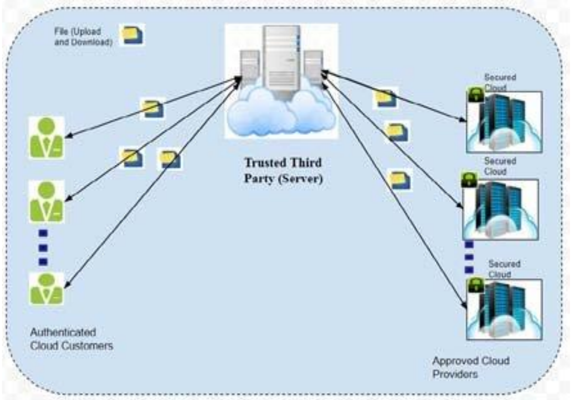
File (Upload and Download)
Trusted Third Party (Server)
Secured Cloud
Secured Cloud
Secured Cloud
Authenticated Cloud Customers
Approved Cloud Providers

Fig. 2. The System model

2.2 SAML

SAML is an open-standard identity management solution that allows users to exchange their credentials across numerous services and apps. SAML integrates users' identities and attributes—which may be kept in several identity management systems—to provide a seamless user login experience. SAML is an extensible markup language that interacts between the identity provider and the service provider and asserts user authentication. This approach depends on digital signatures rather than passwords. For the authentication method to operate, both the service and the identity providers must use the same settings.

2.3 SCIM

SCIM stands for System for Cross-domain Identity Management, and it's an open-standard protocol for cloud-based apps and services. It provides a common user schema for apps like Microsoft 365, G Suite, Slack, and Salesforce to automate provisioning. Fig. 3 shows the System for Cross-domain Identity Management. By syncing user data across applications, SCIM streamlines procedures. A SCIM connection, for example, can automatically deploy a new user to your organization's cloud services when you onboard a new employee and generate an Active Directory record. When an employee quits the organisation, administrators only have to terminate the user in the central directory to withdraw access to all SCIM-enabled apps. For supplying and maintaining web-based identity data, the SCIM Protocol is a REST-based application-level protocol. The System for Cross-domain Identity Management user scenarios and use cases are mentioned in this paper. In a word, SCIM automates the user identity lifecycle management process, which secures user data and streamlines the user experience. As a firm expands, innovates, and sees personnel turnover, the number of user accounts climbs tremendously.

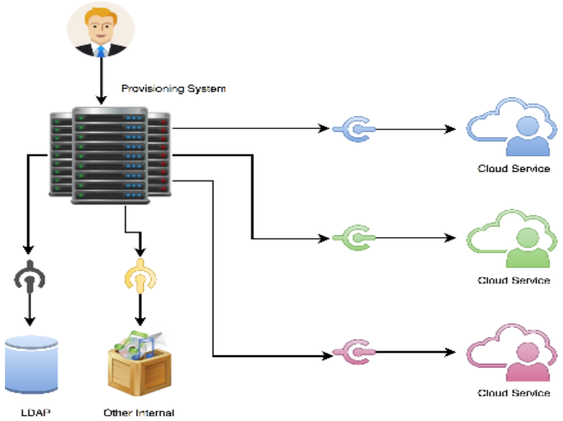

Fig. 3. System for Cross-domain Identity Management

The module's input is a collection of requests to the cloud that the user needs to complete the tasks at hand. The resources that are required are identified initially, coupled with a comparable request for resource mapping, according to the job specifications.

Fig. 4 depicts four important modules, including Query Processor, Load Balancer, Access control Policy and Cloud Database. The user can send requests using the cloud user requests module. It then passes the query to the query processor after checking resource availability. The query processor checks the load with the load balancer, and the security manager verifies access control policies after load balancing, allowing the query processor to manipulate data. Data from the cloud database is saved or retrieved here.

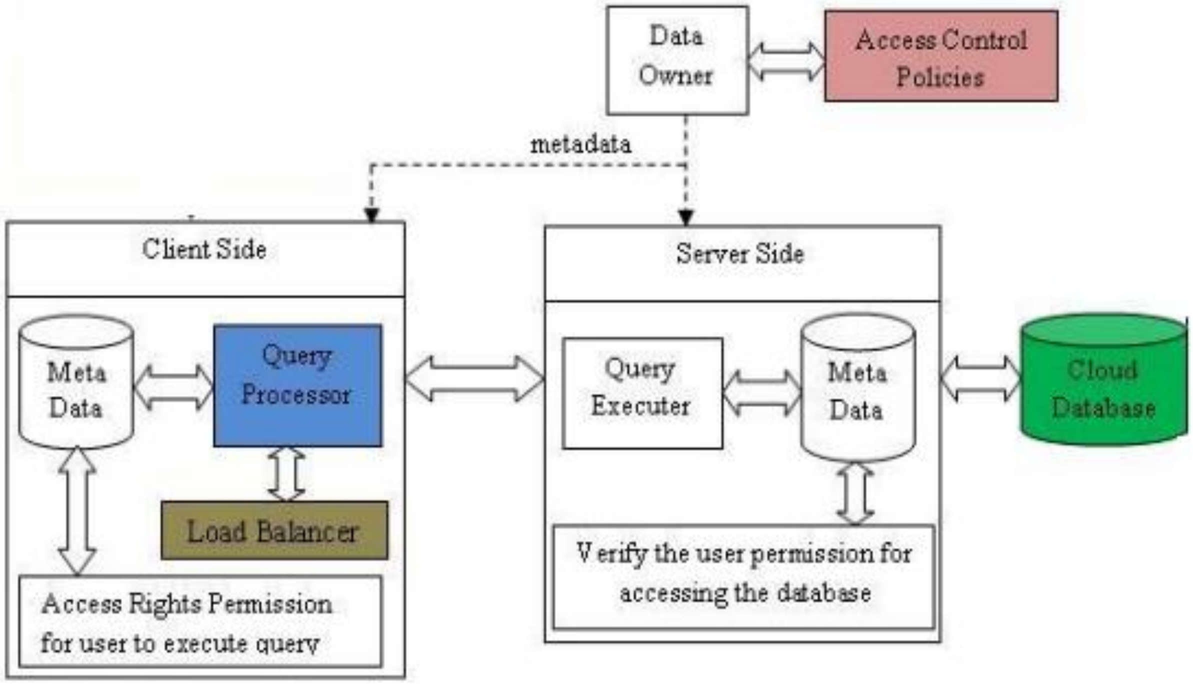

Fig. 4. System model for data transmission on cloud

PROPOSED FRAMEWORK ARCHITECTURE

The suggested paradigm in the cloud system consists of four primary entities: Proxy Server, Trusted Authority, Storage Servers, and Data Owner. The suggested system's framework is depicted in Fig. 5 below:

A. Proxy Server (PSer)

Users of cloud applications can benefit from a range of features provided by the cloud proxy server. As the key point of interaction between Storage Servers, Trusted Authorities, Data Owners, and Data Users, it must enable smooth communication with security and database management. It manages system users, file records, and secret keys, as well as file upload, fragmentation/merger, ciphering/deciphering, code creation, and other processing and request handling activities.

B. Trusted Authority (TAut)

In most infrastructures, the Trusted Authority is the most trustworthy entity; it is considered to be devoid of harmful behaviour and dangers. The Trusted Authority is in charge of manufacturing and assigning secret keys to the application's registered users in the scenario proposed.

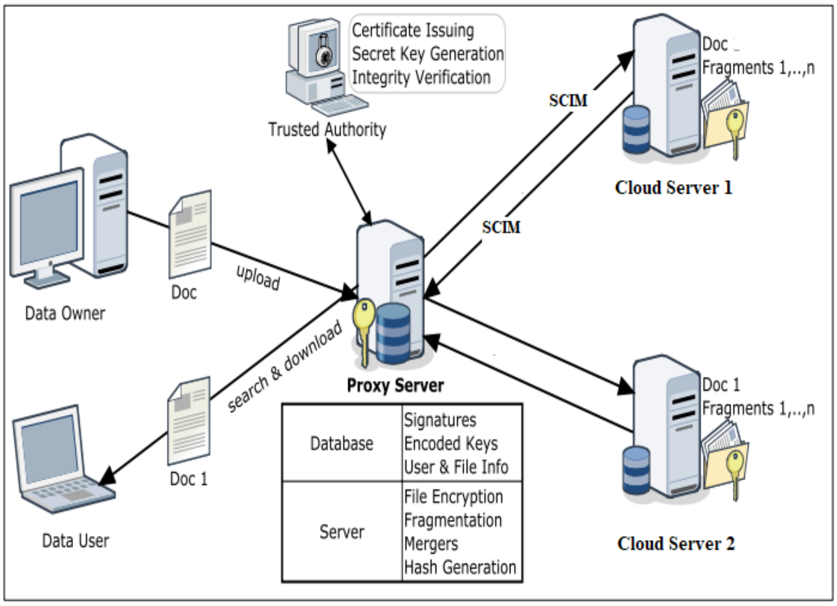

Fig. 5. The proposed system's architecture model

The secret key is then encrypted and stored in the database using the RSA approach, which generates a key pair consisting of a public and a private key. The production of SCIM codes and data integrity verification both need Trusted Authority. The PS creates a SCIM code for the encrypted file as well as file fragments when you submit a file. These hashcodes may be checked for integrity in the future by comparing them to the updated hashes of the already existing file.

C. Storage Servers (SSer)

Storage Servers are responsible for storing encrypted file fragments in their database. For every view or download request, it sends fragments to the Proxy Server, which decrypts the fragments and merges them into a file, then sends a download link to the authorised user. Because storage servers seldom save file keys and rely on the Proxy Server's strong Diffie-Hellman Key Exchange mechanism for each communication session, they maintain a high level of anonymity.

D. Data Owners (DOwn)

Data Owners are people who submit their files to the cloud system via various apps and provide privileges to other users. Users with access credentials can use a browser to access and download files. In essence, each data owner may be classed as a data user, but not all data users can be classified as data owners since they must provide data to be deemed a data owner.

E. Algorithm Implementation

Initializing the System Setting up the Proxy Server, Trusted Authority, and Storage Servers is the first step in the cloud system setup procedure. The Notations Used in Algorithm are shown in Table 2.

Table 2: Notations Used in Algorithm

Notations	Meaning
Usr	User
PSer	Proxy Server
TAut	Trusted Authority
SSer	Storage Servers

Fi | FDesc	Raw File | File Description
F'	Encrypted File
Bi | BF	Binary | File Binary
Enc (…,..)	Encrypt Function
Dec (…,..)	Decrypt Function
UId | FID	User ID | File ID
SKey | SKey'	Secret Key | Encrypted Secret Key
SCIM	System for Cross-domain Identity Management

i) System Initialization

Setting up the Proxy Server, Trusted Authority, and Storage Servers is the first step in the cloud system setup procedure shows in equ (1) and equ (2).

int PSer.| SSer |.Taut … (1)

where SSer | ={SSer1, SSer2,...SSerN} … (2)

PSer uses the proposed System for Cross-domain Identity Management (SCIM) method to verify the authenticity of |SSer| shows in equ (3).

PSer →V=Verify (|SSer|)→SCIM (PSer|SSer|) … (3)

If the result is correct, the storage servers are deemed to be legitimate and are connected to the proxy server shows in equ (4).

|SSer| = Valid ←→ V = True, connect(|PSer|SSer|) … (4)

ii) User Registration

To add a user to the application on running on cloud, a register request is sent to PSer with the user details. After encrypting SK, it sends encrypted SKey', PriK and Uid to the PSer for storage in the DB.

reg (Usr) request sent to PSer … (5)

Proxy Server generates a User ID for the user and sends request to Trusted Authority to generate Secret Key.

PSer → gen Uid (Usr) … (6)

PSer → request (SKey) → TAut … (7)

Trusted Authority uses SCIM algorithm to generate the Secret Key and generates public key and private key using SCIM PKI algorithm.

TAut → gen SCIM Secret key (Usr) = SKey … (8)

TAut → gen SCIM Keys ( ) = Pub K, Pri K … (9)

TAut encrypts the SKey using PubK to get encrypted SKey' and stores

TAut → Enc (SKey, Pub K) = SKey' ,send (SKey') →PSer … (10)

PSer stores the encrypted SKey' Private key PriK of SCIM and User ID to its DB

PSer → store (SKey', Pri K,Uid) … (11)

User registration process shows in equ (5) to equ (11).

iii) File Upload and Encryption

Upon receiving file upload request from the user, proxy server assigns an ID to the file shows in equ (12) and equ (13).

Usr (Fi, FDesc) → PSer … (12)

PSer→ generate FId (Fi) == ID_F. … (13)

iv) Decryption and Download

User directs the file download request to the PSer with User ID and File ID shows in equ (14).

Usr → reqFile (ID_F , Uid) sent to PSer … (14)

Proxy Server fetches the encrypted secret key allotted to user from its DB i.e., SKey' ID shows in equ (15).

PSer → get EncSecretKey(Usr)= SKey' … (15)

Proxy Server deciphers the encrypted secret key SKey' using private key PriK to get the original secret key i.e. SKey

A download link is displayed to download the demanded file shows in equ (16).

PSer → genLink (FId) → Usr … (16)

For the purpose of securing data in the cloud, we created a technique named "Deep learning with SCIM". To provide quicker access to cloud resources in its storage system, this framework uses a new user authentication strategy. The suggested system not only offers a better user experience in the cloud, but it also offers a strong authentication technique that is very resistant to several authentication-based attacks and DDoS attacks in the cloud. a framework that includes several safeguards for channel security and data protection while servers are communicating with one another. The system's overall stability and efficiency in terms of speed and security are enhanced by the employment of the most efficient encryption algorithms, fragmentation, key exchange strategies, and access control. Several sniffing attacks, such as MITM attacks, identity spoofing attacks, and discrete logarithmic assaults, are successfully constrained by our technique. Furthermore, adopting the most recent SCIM feature guarantees improved speed and security. An inventive design that can guard against assaults by validating the storage connections to the main server's integrity, making it challenging for attackers using sniffers to intercept data during file transmission. Performance and security are enhanced with the SCIM function. The findings show that the system can still retain a fantastic level of performance by utilising incredibly effective and safe strategies.

For secure data sharing and server storage, our suggested techniques are well-equipped with the most recent algorithmic support. In order to offer complete security, DOS assaults and internal attacks were the main targets. All of the studies that have been done have shown the effectiveness and dependability of the suggested procedures. The process of ongoing research and development goes into improving any system. The same principle also holds true here. Security of cloud storage has been researched several times, with each new study delivering an enhanced version of the preceding one.

Fig. 6 depicts the system paradigm and architecture for Deep Learning on the cloud platform. The system model, which includes the user workload model, cloud platform model, and energy consumption model, is covered in this part. DL-Cloud, a one-of-a-kind DL-based system with two-stage resource provisioning and task scheduling, was proposed as a means for cloud service providers with huge data centres and a high volume of user requests with dependencies to save energy.

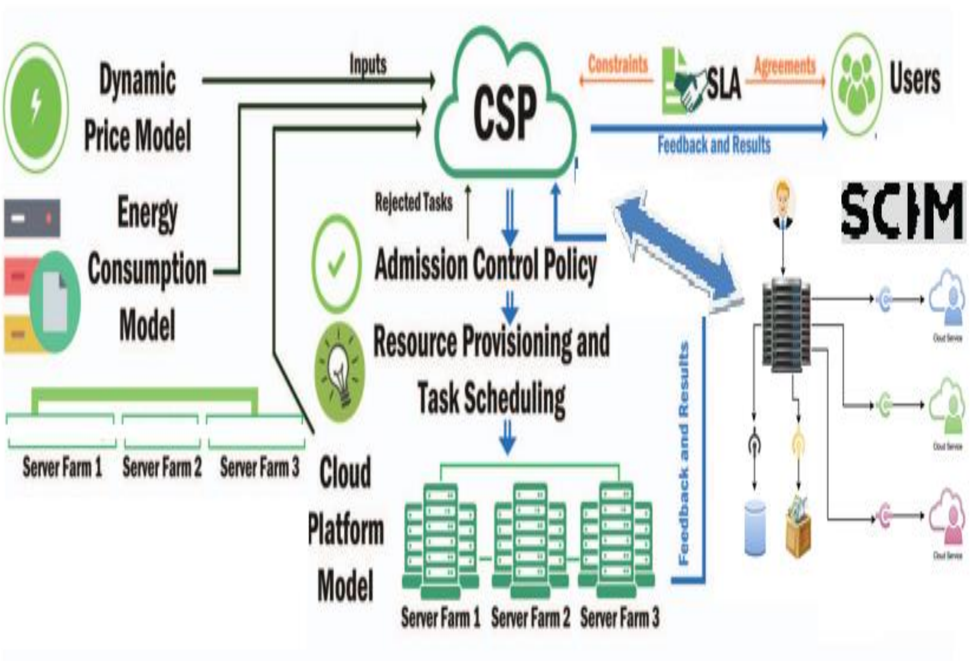

Fig. 6. Deep Learning system model and structure

A new DL-based approach with two-stage resource provisioning and job scheduling decreases energy expenses for cloud service providers with large-scale data centres and high numbers of user requests with dependencies.

4. RESULTS AND DISCUSSION

To perform the research, we employed a test bench with an Intel i5-2410M CPU, which has four cores and runs on a 128-bit processor. The programming language used is Java, which is compatible with Windows 7. Two Apache servers with two MySQL 8.0 databases are used for remote data storage on a local network with a bandwidth of 100MBPS, as shown in Table 3.To assess how effective the algorithms were, we tested the recommended framework with a variety of file sizes.

The SCIM method's performance is demonstrated in Fig. 7, where the ratio of time it takes reduces as file size increases, compared to encryption of smaller files. In terms of efficiency and security, the SCIM algorithm has been proven to be among the finest symmetric algorithms. As a result, increasing file size has a very minor influence on efficiency.

Table 3. Configuration of the system for experimentation

CPU	Intel i5-2410M Processor
Memory	8 GB
Storage	500 GB
Bits of Processor	128 Bits
The rate of processing	3.3 GHz
Server	Apache Tomcat Server
Tools	JDK 8 , Eclipse 11
Database	MySQL 8.0

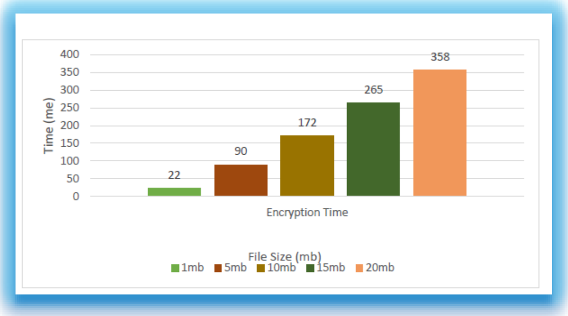

Fig. 7. Encryption Time

Viruses are the most prevalent security threats that network administrators confront. The two main roadblocks to cloud computing adoption are integration with current systems and network security. Separating public and private data from the network is the key to cloud computing success. Fig. 8 shows the encryption time in terms of time taken when applied to various file sizes.

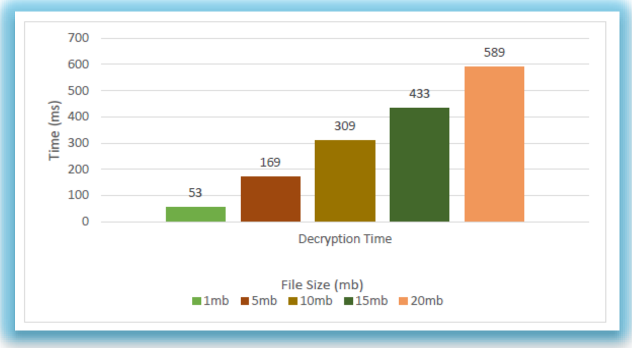

Fig. 8. Decryption Time

Viruses are the most prevalent security threats that network administrators confront. The two main roadblocks to cloud computing adoption are integration with current systems and network security. Cloud computing relies on separating public and private data from the network. Customer penetration testing might help to build trust in the cloud service provider's security approach.

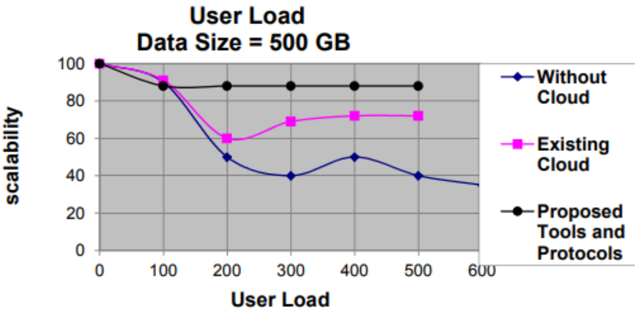

Fig. 9. Scalability Comparison Graph

The firms range in size from 38 percent with fewer than 500 people to 27 percent with more than 4000. We compare organisations based on their size. The basis for their decision to use cloud computing is that the existing cloud has 72 percent scalability and the planned work has 88 percent scalability shows in Fig. 9.

Data security is required on both the user and server sides in a cloud environment. In today's environment, some effort is placed into security and control-related operations by allocating a certain percentage of resources. The primary issue is the data, which is critical to the organization's success. We must assure the company that their data will be secure after they migrate to the cloud. And a cloud provider may do this by following all security regulations, encrypting data, and using personal firewalls. Single sign-on and single sign-off should be enforced to improve security and user experience.

In most organisations, access control lists are used to manage access control. The security model used by the cloud provider is of greater significance to the organisation. In most organisations, access control lists are used to manage access control. The security model used by the cloud provider is of greater significance to the organisation shows in Fig. 10.

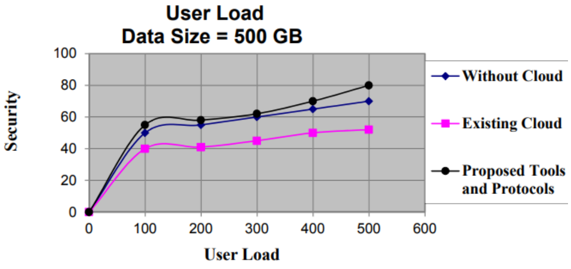

Fig. 10. Security Comparison Graph

Data security is required on both the user and server sides in a cloud environment. In today's setting, some effort is placed into security and control-related operations by allocating a percentage of resources. The primary issue is the data, which is critical to the organization's success. We must assure the company that their data will be secure after they migrate to the cloud. And cloud providers can achieve this by following all security regulations, encrypting data, and using personal firewalls.

The creation of a cloud environment for a safe business with data that is vulnerable to security risks Cloud Security Protocol was introduced. This will improve cloud speed, lower costs, and ensure user and server security. Then, to enable security at the user and provider levels, we created the Framework and Cloud Security Protocol. In a cloud setting, the Data Storage Protocol ensures data protection. The Data Storage Protocol was created to give verification at the user's end and data security at the server machine by utilising metadata. The data security of the server may be checked remotely by the user.

One of the most important factors in an organization's decision to migrate to a cloud network is cost. We took into account the cost of public clouds as well as their cost policies. We learned from our research that businesses are prepared to spend more money on cloud-based systems provided they can be assured of higher dependability and data protection. Cloud Service User Security Tools, Protocols, and Virtualization is a way that may assist decrease costs in their network because so much money is already spent on maintenance. For network growth, more data capacity is necessary, which increases the cost. As a result, cloud computing provides a low-cost solution to such problems. For a corporation with a high level of security, we feel that a private cloud solution will be substantially safer in terms of data security, reliability, and privacy. At the user level, the Cloud Service User Security tool, the Multilevel Framework or Cloud Security Protocol, and the Data Storage Protocol with private cloud provide improved security.

5. CONCLUSION AND FUTURE ENHANCEMENT

The proposed user identity management protocol protects both cloud computing users and cloud service providers. This protocol will authenticate and authorise customers/providers in order to construct worldwide security networks. Deep Learning with System for Cross-domain Identity Management will secure customers'/cloud service providers' infrastructure by preventing unauthorised users from accessing the service/facility. Deep learning techniques employing SCIM were used to improve security and scalability. Deep learning with SCIM is a way that we created to safeguard data in the cloud. This framework employs a novel user authentication approach to provide quicker access to cloud resources in its storage system. Although there has been a lot of focus on cloud-based systems in the past, there has been little or no study on multi-cloud systems. Designs are advised to safeguard data kept on storage servers while maintaining anonymity and integrity. To protect cloud computing customers and providers, the SCIM user identity management protocols are recommended. This protocol will authenticate and authorise customers/providers in order to construct worldwide security networks.

Future work could be extensions for the detection and protection of new types of hackers in the cloud environment could be provided. Numerous studies have been conducted on cloud storage security, but each one always results in an improved and expanded version of the previous study. The suggested work could experience new developments as a result of the use of bio-inspired algorithms or machine learning based. Finally, the capability trust computation model can be added to the access control with key management algorithm utilised in this research effort to improve the security model.

References

[1]. A. Zeroual, M. Amroune, M. Derdour, A. Meraoumia, A. Bentahar Deep authentication model in Mobile Cloud Computing, 3rd International Conference on Pattern Analysis and Intelligent Systems (PAIS), IEEE (2018), pp. 1-4, 10.1109/PAIS.2018.8598508URL: https://ieeexplore.ieee.org/document/8598508/

[2]. Y. Wang, T. Nakachi, H. Ishihara, Edge and Cloud-aided Secure Sparse Representation for Face Recognition2019 27th European Signal Processing Conference, IEEE (2019), pp. 1-5, 10.23919 / EUSIPCO.2019.8903137.

[3]. Boyapati, B. ., and J. . Kumar. “Parasitic Element Based Frequency Reconfigurable Antenna With Dual Wideband Characteristics for Wireless Applications”. International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 6, June 2022, pp. 10-23, doi:10.17762/ijritcc.v10i6.5619.

[4]. Grance, T. and Jansen, W. (2011), Guidelines on Security and Privacy in Public Cloud Computing, Special Publication, National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-144.

[5]. I. Indu, P.M. Rubesh Anand, Vidhyacharan Bhaskar, Identity and access management in cloud environment: Mechanisms and challenges, Engineering Science and Technology, an International Journal, Volume 21, Issue 4, 2018, Pages 574-588, ISSN 2215-0986, https://doi.org/10.1016/j.jestch.2018.05.010.

[6]. Gupta, D. J. . (2022). A Study on Various Cloud Computing Technologies, Implementation Process, Categories and Application Use in Organisation. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(1), 09–12. https://doi.org/10.17762/ijfrcsce.v8i1.2064

[7]. Rajkumar, N & Kannan, E. Deep learning-based key transmission (DLKT) protocol for secured group communication in cloud. Soft Computing, 2021, 25. 1-13. 10.1007/s00500-021-05959-z.

[8]. Annappaiah, Dinesha & Agrawal, V.K. (2012). Multi-level Authentication Technique for Accessing Cloud Services. 10.1109/ICCCA.2012.6179130.

[9]. Chen, Xiang & Xu, Lijun & Wei, Hua & Shang, Zhongan & Tingyu, Zhang & Zhang, Linghao. (2019). Emotion Interaction Recognition Based on Deep Adversarial Network in Interactive Design for Intelligent Robot. IEEE Access. 7. 1-1. 10.1109/ACCESS.2019.2953882.

[10]. Joy, P., Thanka, R., & Edwin, B. (2022). Smart Self-Pollination for Future Agricultural-A Computational Structure for Micro Air Vehicles with Man-Made and Artificial Intelligence. International Journal of Intelligent Systems and Applications in Engineering, 10(2), 170–174. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/1743

[11]. Tariq, Muhammad Imran, Memon, Nisar Ahmed, Ahmed, Shakeel et al., A Review of Deep Learning Security and Privacy Defensive Techniques, Mobile Information Systems, Hindawi, 2020, https://doi.org/10.1155/2020/6535834.

[12]. R. Cai, H. Li, S. Wang, C. Chen and A. C. Kot, "DRL-FAS: A Novel Framework Based on Deep Reinforcement Learning for Face Anti-Spoofing," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 937-951, 2021, doi: 10.1109/TIFS.2020.3026553.

[13]. Sally Fouad Shady. (2021). Approaches to Teaching a Biomaterials Laboratory Course Online. Journal of Online Engineering Education, 12(1), 01–05. Retrieved from http://onlineengineeringeducation.com/index.php/joee/article/view/43

[14]. Shengmin Xu , Guomin Yang , Yi Mu & Robert H Deng 2018, ‘Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in the Cloud’, IEEE Transactions on Information Forensics and Security, Vol. 13, No. 8, pp. 2101-2113.

[15]. Sumagita M, Riadi I, Soepomo JP, Warungboto U (2018) Analysis of secure hash algorithm (SHA) 512 for encryption process on web based application. Int J Cyber-Secur Digital for (IJCSDF) 7(4):373–381.

[16]. Ahmad, N., Cloud Computing: Technology, security issues and solutions. In Anti-Cyber Crimes (ICACC), 2017 2nd International Conference on. IEEE, 2017.

[17]. AlZadjali, A. M., A. H. Al-Badi, and S. Ali, An analysis of the security threats and vulnerabilities of cloud computing in oman. In Intelligent Networking and Collaborative Systems (INCOS), 2015 International Conference on. IEEE, 2015.

[18]. Jian Shen, Tianqi Zhou , Xiaofeng Chen , Jin Li & Willy Susilo 2018, 'Anonymous and Traceable Group Data Sharing in Cloud Computing', IEEE Transactions on Information Forensics and Security, Vol. 13, No. 4, pp. 912-925.

[19]. Yue Zhang , Jia Yu , Rong Hao , Cong Wang & Kui Ren 2018, 'Enabling Efficient User Revocation in Identity-based Cloud Storage Auditing for Shared Big Data', IEEE Transactions on Dependable and Secure Computing, pp. 1-13.

[20]. Mazhar Ali , Revathi Dhamotharan , Eraj Khan , Samee U Khan , Athanasios V Vasilakos ,Keqin Li & Albert Y Zomaya 2017, 'SeDaSC: Secure Data Sharing in Clouds, IEEE Systems Journal , Vol. 11, No. 2, pp. 395-404.

[21]. Sebastian Graf, Patrick Lang, Stefan, A, Hohenadel & Marcel Waldvogel 2012, 'Versatile Key Management for Secure Cloud Storage', IEEE 31st Symposium on Reliable Distributed Systems, USA, pp. 469-474.