International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(17s) 2026 pp. 1173-1189
https://doi.org/10.70917/ijcisim-2026-4822
Article

A SECURE INTERNET BASED EDUCATIONAL INFORMATION SYSTEM USING AUTHENTICATION AUDITING AND STORAGE TECHNIQUES

S.Srinivasan[1*], S.Nagaraj[2], A.Kannagi[3], K.Raja[4], K.K. Ezhilarasan[5]

[1*]Dept. of Computer Science and Engineering, Karpaga Vinayaga College of Engineering and Technology, Chennai, India
[2]Dept. of CSE, Alliance School of Advanced Computing, Alliance University, Bengaluru, India
3School of Computer Science & IT, Jain Deemed-to-be University, Bengaluru, India
[4]Dept. of CSE, SRM Institute of Science and Technology, Ramapuram, Chennai, India
[5] Dept. of CSE, Karpaga Vinayaga College of Engineering and Technology, Chennai, India
Corresponding Author: srinikcgmca@gmail.com
srinikcgmca@gmail.com, nagarajsangeet87@gmail.com
a.kannagi@jainuniversity.ac.in, rajak1@srmist.edu.in, k.k.ezhil@gmail.com

Abstract: Nowadays many educational institutions maintained continuous quality improvement organization information system. Presently users from various government and private educational sectors are frightened because of their information stored in existing storage mechanisms are insecure due to threats and attacks in real world. Nowadays cloud storage is an innovative technology which has been provided by various cloud service providers in this information technology era. An efficient secure storage mechanism along with suitable authentication and auditing methods is needed for an internet-based educational institution. This well-organized system supports cloud computing-based multi-layer architecture which promotes different categories of users' spirits and ethics from clerical to management executive members which satisfy their requirements and recognize the defensible growth of internet-based educational information system. This secure internet-based educational information system provides both online storages such as dropbox, cloudme, cloud service providers storages and offline storages like redundant array of independent disk storage mechanism. This paper deals high level user authentication security, information integrity, user privacy and confidentiality while storing and sharing of confidential details in cloud computing-based internet educational information system through multi-level authenticated security with cryptographic-based encryption and decryption method with numerous storage methods. This internet based educational system ensures user and data authentication, information security, user privacy, data availability and information integrity. The improved merkle hash tree using bat mechanism ensure data authentication in this system. The Internet-of-Things is the most recent technology used in different areas across world. The Internet-of-Things based sensors can be used in this proposed method for the purpose of enforcing alert messages and generating alarm in this system based on measurement of size of storages maintained by the internet-based educational institutions. Utilization of storages by any user can be monitored through Internet-of-Things based sensor. This electronic based IoT sensor provides alarm sound system along with alert messages to user when user cross the limits of utilization of storage in this internet based electronic education system. Access of storages has some restrictions which can be measured then alarm and alert messages can activate when measurement values crossed beyond the limits of threshold value setup by the proposed system. User authentication is achieved by Aadhaar card or biometric based authentication and two-way user verification through email and cell phone or any other electronic or internet-based devices has been enforced in this proposed system. All administrative, academic, examination related details, sports and extracurricular along with transportation information, training and placement related materials and particulars, research-based facts, other specifics like conference information, workshop and seminar details are completely stored in offline and multiple cloud storages in form of encryption and decryption methods using RC4 cryptographic algorithm which ensure information confidentiality and data availability. This internet and cloud based educational information system acquire the storage services from Amazon Web Services, Windows Azure cloud computing services. The cloud storage services of various cloud providers

completely stored all educational information system details and protected from various types of threats and attacks. This system prevents confidential resources and information from various internet-based attacks like cross-site scripting and cross-site request forgery attacks. The user can store all educational confidential details and access in offline storages also because the user will not able to store and access the details in cloud storages due to some circumstances and unavoidable situation which makes to assure reduction of data leakage. User access privileges mechanism will be provided to all operations of educational system with respect to user priority level in this system. Access control privilege mechanism enforces the role-based access, rule-based control access, policy-based access and attribute-based access models in this internet based educational information system. There is a need of auditing in internet-based education system which guaranteed information integrity and enforces individual auditing as well as group auditing mechanism through k-means cluster mechanism. This system achieve better performance evaluation with respect to high quality of service in terms of data communication and transmission, comparison of bandwidth utilization of various methods, comparison of user visit count of different methods, reduced computational and data transfer cost, comparison of various online offline storages, comparison of user queried rate on number of files of different methods, comparison of data authentication rate on user task of various methods and protect confidential data from threats, internet based attack. The trusted internet-based education system adopts internet-based quality management system, multi-level security with better efficiency and reduced cyber-based attacks and vulnerabilities.
Keywords: Authentication, Cloud Storage, Security, Internet-of-Things, Access Privileges, Group Auditing, Merkle Hash Tree

1. INTRODUCTION

Nowadays many educational institutions maintained their administrative as well as academic details in offline storage with file management system as well as online computer-based storage management system. Presently most of the educational institutions adopted continuous quality improvement management system through internal quality assurance cell. Any educational institutions or any department under various educational institutions get quality assurance certificate and accreditation certificate like ISO, NAAC and NBA in India. In order to achieve those types of certifications by educational institutions through maintaining of all administrative and academic details in internet-based cloud storage system is more efficient and good for any type accreditation and auditing certification process. Nowadays different types of educational institutions web portal or manual or offline storage contains various infrastructure-based records, administrative-based confidential details, academic records of students and many more details are hacked or stolen by various types of hackers and malicious users. In order to avoid this dangerous situation, the internet-based online (Amazon Web Service - Bucket Storages and so on) and offline cloud storage has been enforced which make sure of highly strengthen the security and data availability for various educational institutions details in real world. The internet-based cloud computing service providers storages are highly secure, well-organized and highly protected during all periods throughout the year by various cloud based remote storage datacenters in different region across the world. Auditing is needed for any educational institutions which check all records, infrastructure and all information which is mentioned and maintained by any auditing agencies like ISO and so on. In this proposed system individual as well as group auditing can be achieved through cluster technique which is also required for any type of educational institutions which ensure data integrity and make sure of increase the level of quality and maintain the spirits, ethics from end users to management decision-making members. In general, many educational institutions management information system are single authenticated with less security system and maintenance of minimum storage system which leads to unsecure, more data leakage and data corruption. In order to overcome these difficulties, we have to propose multi-level authentication with provided high level security for confidential information in form of encryption and decryption algorithm with abundant storage methods in internet-based educational information system. Nowadays, many educational systems become i-(internet) based educational information system which ensure data authentication through data authentication and confidentiality through various methods like merkle hash tree algorithm using bat mechanism. The proposed i-educational information system measured and monitored use of storages which has been indicated by alarm and messaging system through Internet-of-Things (IoT) based sensors. IoT based sensors assists helps to measure and manage status of various equipment's, instruments, storages in various institutions by using with or without internet. The continuous quality improvement i-educational (internet-based education) management information system enforces multi-level user authentication by email or two-time password authentication and Aadhaar card or biometric based authentication system. In the

proposed i-educational information system, the various levels of user access control different priority mechanism have been enforced. This i-educational management information system will provide excellent performance in terms of data

transmission with reduction of cost, reduced auditing time and improved user queried rate with comparison of various storage methods. This paper implements internet-based continuous quality improvement information system, multi-level authenticated security with good efficiency and reduced web-based attacks, threats and vulnerabilities.

2. LITERATURE SURVEY

Daojiang Wanga et. al [1] implemented education information system action plan is web page application in China which illustrates updating of iterative educational system with rapid incremental development on different functionality of education system based on micro architecture with respect to business, user interface service and data center unit. Muhammad Furqon et. al [2] proposed an effective usage of learning management system in educational system which is the inspired a transformation in the realm of educational learning information system which shows academic performance of the students and assist the educational institutions or educators with respect to exploiting learning management system to simplify the educational development in real world. Nik Elyna Myeda et. al [3] measure the continuous quality management procedures and principles in educational institutions and create better culture and maintain good relationship stakeholders and management which will improve the performance of academic as well as administrative activities based on the stake holders' requirements. Serhii Petryk et. al [4] enforces and analyzes ISO 9001:2015 quality management tactics and standards in various institutions need a rapid growth of advanced continuous quality management structure at different levels and find various forms of performance assessment strategies in quality management system which assure quality service delivery with respect to academic, administrative and various areas of institutions.

Zheng Gu et. al [5] proposed a Linux operating system based elastic RAID model which encourages dynamic conversion between level 5 and level 10 of RAID Technique. Adnan Tahir et. al [6] indicated the different issues on cloud storages like information availability, data management and some factors of availability of cloud storage such as cost efficiency and so on. Different actions and outages on various cloud storage along with various techniques of cloud storage has been addressed. The different methods, models, structures of storages such as RAID, RACS, DAC and Syncopy are currently available in this information technology era. Dr.T. Kamala kannan et. al [7] shows fundamental concepts of cloud storages and its providers such as like CloudMe, Mega, Dropbox, iCloud and so on. Dr.T. Kamala kannan et. al [7] enforces the multiple third-party storages and resolve the issue of data integrity. Durga Venkata Sowmya Kaja et. al [8] indicates various issues of cloud data storage security such as information breach on various cloud storage providers, data theft and also specified wide-ranging investigation of different types of web-based attacks, threats, replay and timeliness-based cloud attack, SQL injection attack, byzantine attacks, sniffer attacks and its various moderation methods like NR protocol, Improved Merkle Hash Tree method and so on. Mohammed Aziz Al Kabir et. al [9] enforced IoT devices-based threats and cyber security-based attacks are highly vulnerable to all users in real world because of due to lack of security aspects in simple internal planning of any type cyber security on different models and low-powered hardware, limited software support, man-in-the-middle-attacks, botnets in an organization or educational institutions. To overcome these attacks, threats and vulnerabilities, Mohammed Aziz Al Kabir [9] proposed various remediation and mitigation mechanism such as access control methods, multi-secure communication protocols and periodic updates and patches on software and hardware's which ensure high-level security and privacy on IoT devices and web-based applications.

Yuchong Li et. al [10] indicated that high decision-based authorities of government and private organizations are nowadays panic due to cyberattacks and hazards of wireless communication methods. Presently whole world is fully dependent on information technology based electronic web-based business system. Therefore, protecting the confidential information or secret data of any educational institutions or any government or private organizations from web-based attacks or mobile-based attacks is one of foremost issue in real world. Yuchong Li et. al [10] investigated and indicated the emerging movements and current changes on cyber security attacks, challenges, issues, weakness

and strength of the various proposed methods, some techniques are in operational strategies and other methods are study phase with high-level standard security frameworks with respect to web-based or cyber-attacks in this information technology era. Srinivasan S et. al [11] suggested auditing of same resources or equipment's or confidential information on different group through *k*-means cluster techniques under policies of audit control management. Both Behnam Zahednejad et. al [12] and Srinivasan S et. al [13] suggested multi-way authentication of any client by electronic mail based secret code and mobile-based passcode, fingerprint-based biometric authentication techniques implemented in internet and mobile-based applications and platform [12,13]. All users in this system store their confidential information, credentials are accessed through various cloud service storage providers on-line storages as well as off-line storages such as RAID storage which required different authentication techniques like multi-way verification and validation techniques, fingerprint-based biometric method, mobile or email-based password mechanism and steganographic-based verification and validation method [12,13]. Mohammad Aldossary [14] suggested sensor based IoT applications with multi-layered architecture which provides high quality cloud storage services and extensible resources through mixed integer linear programming mechanism. The various servers which may be available in different geographical locations which assist to make better decision and data transmission and also providing various services and resources to users in optimium level as per the user demand. Wenjun Luo et. al [15] proposed white-box secret key cryptographic based security and privacy mechanism which suggest high level random perturbation encryption mechanism with privacy of the intermediate secret key which leads to protect the web-based attacks. A F Doni et. al [16] implemented the cryptographic based RC4 encryption and decryption algorithm for information security on various types of document-based data file such as pdf, xls and different file formats. He enforced confidentiality and data availability which able to secure the authenticity of data on various file format.

Raghda Sattar Jabbar [17] proposed secured digital based multi-encryption based cryptographic technique like elliptic curve encryption-based algorithms, Zigzag and RC4 methods on different images which may different file formats followed various standard metrics which protect from unauthorized access of malicious users and threats. Srinivasan.S et. al [18] implemented enhanced merkle hash tree mechanism through bat algorithm along with third party auditing method which ensure dynamic data integrity, data authentication and achieve public auditability. Srinivasan.S et. al [18] handled various synchronized multiple auditing tasks and achieved data authentication and data integrity through improved merkle hash tree using bat algorithm with assistance of optimal private key of various clients. Shayma Wail Nourildean et. al [19] suggested Internet-of-Things based sensors on various ad-hoc networks routing protocols which monitors various types of network and enhance performance of network against different categories of jammers with respect to various parameters like reduce delay on data transmission, IoT link can be controlled remotely, reduction of data fall-down points, applying wireless sensor technologies which able to sense and gather information from different infrastructure, status of devices and various cloud-based components. Joseph Williamson and Kevin Curran [20] proposed multi-way user authentication techniques like username and password mechanism, one-time password mechanism, personal identification number using mobile phone and other various bio-metric methods such finger-print or eye detection method. This type of multi-way user authentication techniques verified integrity and user identity by their confidential credentials and also protects users from web-based attackers and malicious users.

Nassim Ammour et.al [21] narrates the unique human characteristics and various human measurements which identify the various issues on physiological identities like face- recognition, bio-metric based fingerprint mechanism. Nassim Ammour et.al [21] proposed multi-model method of improved biometric methods includes fingerprint and electrocardiogram signals with processing of feature vectors using stacking and channelize methods which able protect the system from spoofing attacks. Swapnil Sutar et.al [22] executed secret sharing algorithm on internet-of-things related equipment's or devices. Cryptography-based block cipher Boolean masking scheme has been embedded on various physical equipment's through IoT based sensors which able to protect the entire system from various threats and ensure information confidentiality and data availability on various storages such as online and offline storages. Shivendra Bhonsle et. al [23] described the comparative study of information technological giants Microsoft Azure and Amazon cloud services with respect to networking capabilities, cloud storages, manageable remote data center,

computing services, database services and other services. Srinivasan.S and Raja.K [24] proposed various prevention methods for cross site request forgery and cross site scripting web-based attacks which enable security against cyber-attacks and improve high level security to various cloud service providers-based servers. Amardeep Kaur et. al [25] enforced access control list and policies which able to restrict access to infrastructure or resources or equipment or confidential information stored in storages with respect to role-based access control mechanism. In order to implement role-based access policies, many unauthorized users can be restricted to access the confidential information due to permission denied to restricted users as per policies of access control matrix. Due to the access control matrix and policies, utilization of resources by authorized user has been rapidly increased exponentially.

3. INTERNET BASED EDUCATIONAL INFORMATION SYSTEM USING AUTHENTICATION AUDITING AND STORAGE TECHNIQUES

The multi-layer architecture of internet-based educational information system (IEIS) using authentication auditing and storage techniques as shown in Fig.1.

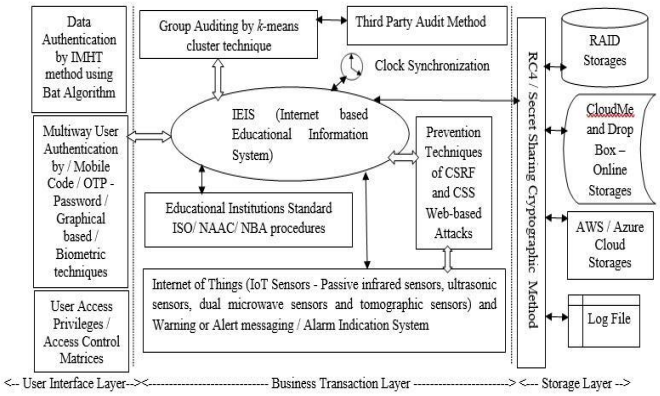

Fig-1. Multi-layer Architecture of Internet-Based Educational Information System (IEIS)

Most of the educational institutions followed accreditation policies and rules which has been enforced in this internet-based educational information system. This system provides private-accreditation experts details which able to assists some educational institutions follow standard operating procedures and levels of accreditation of various international and national accreditation bodies like NAAC, IAO, NBA, ISO and so on with respect to the institutional and specific programme accreditation based on the need of educational institutions. Different types of clients or end-users used this internet-based educational information system, so there is possibility of malicious users or attackers also entered to access the system, so in order to avoid the various categories of clients or different types of hackers or malicious insiders, this system enforced several multi-way user authentication techniques.

In this system as per the institutions requirement large number of authentication techniques are used such as steganographic authentication, one time password, smart code or mobile code, finger-print based biometric authentication, user name login password, email-based passcode, user authenticated quick response code and so on [12,13,20,21]. The user access privileges and access control matrix provides various access permissions like read, write, modify, erase or delete options to various users depends on their privileges given by the system [25]. This IEIS provides user access privileges and access control matrix for different users on various confidential files maintained by all educational institutions as shown in Table 1.

Table-1. User Access Privileges and Access Control Matrix

Access Control Matrix	**Access Control List**

		Object Type (format)	Object Type (format)
Subject (User Types)		***File1<video>***	***File2< Document>***
	Client 1	Read, Write	Read only
	End User 2	Read, Print	Read, Write
	Customer 3	Read only	Execute only

In IEIS the maintaining user roles and permissions for any type of educational institutions are mentioned with respect to institutions, various users or client, roles assigned to users or client and permissions as depicted in Fig.2.

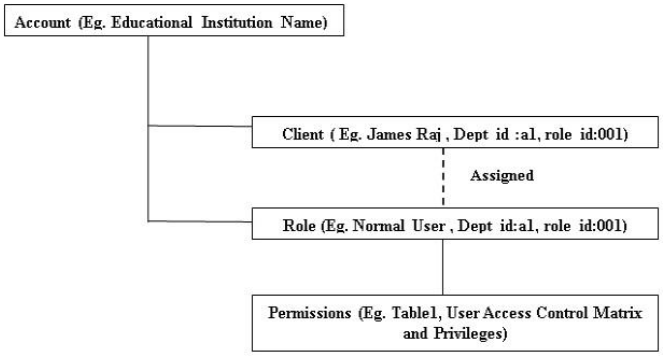

Fig-2. Supervision of User Roles and Permissions

In this IEIS customer access permission control mechanism has been assigned to several users or clients which able to access various manipulations of internet-based educational information system in terms of role-based mechanism with various several policies and attribute-based access models [25].This well-secured incorporated structure of the IEIS enforced multi-layer architecture as user interface, business transaction and storage layers. This IEIS achieved data integrity through improved merkle hash tree mechanism using bat technique which safeguards appropriate user data authentication admittance as shown in Fig. 3.

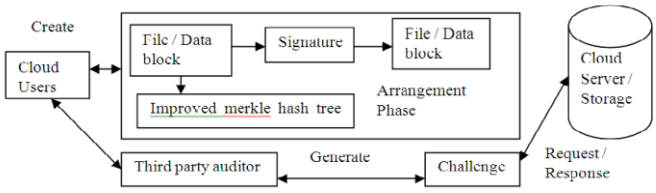

Fig-3. Improved Merkle Hash Tree process block

The purpose of third-party auditing explored public auditability which guarantees security and privacy through private key of the client for cloud environment [18]. The client data integrity and public auditability can be obtained through optimize the process of improved merkle hash tree using bat mechanism. The confidential secret key kept in the root of improved merkle hash tree which maintains the data in the components unchanged. For every node of tree, authentic value and hash value h(.) of data has enforced in hash tree that can be applied in merkle tree to authenticate data blocks. The purpose of hash function which verified each entries which means data block of the file as depicted in Fig. 4. The purpose of Bat technique [26] is to select optimal private key of the user with assistance of adapting pulse frequency, refresh fitness evaluation through seeking the best values.

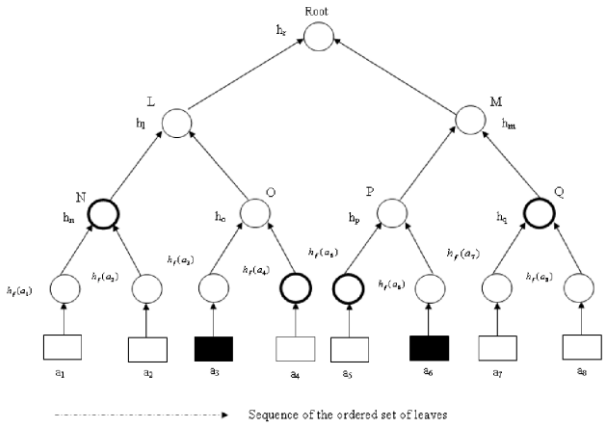

Fig-4. The Structure of Improved Merkle Hash Tree

Steps of Bat technique [18,26] is represented in below:

1: Prepare the bat population by the setting the initial values

2: State pulse frequency and velocity

3: Fix the rate of pulse and loudness

4: Evaluate the fitness by exact matched data which should be maximum.

5 Find and make new original solution by fine-tuning of Frequency and keep on changing the velocity

6: Select the best result and make local solution which is near to the best result or solution based the condition which should be random number is less than pulse rate else go to step 7

7: Assess fitness value

8: Get new result or solution by rapidly increasing value of the pulse rate and decreasing the value of loudness if new solution or value is healthier than existing old value then proceed to step 9 else goto step 2

9: Seek the best solution or location.

This improved merkle hash tree has arrangement and dynamic data integrity stages [18,26] . The arrangement stage creates signature for data block which is in file, make tag for auditing, transmitting the confidential secret key in the root of merkle tree to server. The dynamic data integrity stage perform validation on data by the auditing tag and Genproof(.) and the appeal from third party auditor by computing the constraints or parameters σ and γ [18,26] using (Eqn.1 and Eqn.2).

$$\gamma = \sum_{i=d_1}^{d_c} u_i \, a_i \in Z_p \qquad \ldots\ldots (1)$$

$$\sigma = \prod_{i=d_1}^{d_c} \delta_i^{u_d} \in G \qquad \ldots\ldots (2)$$

The main node or root of enhanced merkle hash tree should be authenticated by signature set e(σ,g) [18,26] generated using (Eqn.3).

$$e(\sigma,g) = e\left(\prod_{i=d_1}^{d_c} h_f(ai)^{ui}, s^{\gamma}, u\right) \ldots\ldots (3)$$

The dynamic data integrity stage attained user data integrity and public auditability [18,26]. It has several data operations such as insertion, deletion and updating of cloud providers storage. The enhanced merkle hash tree updation under data block in a file modification [18,26] as shown in Fig. 5.

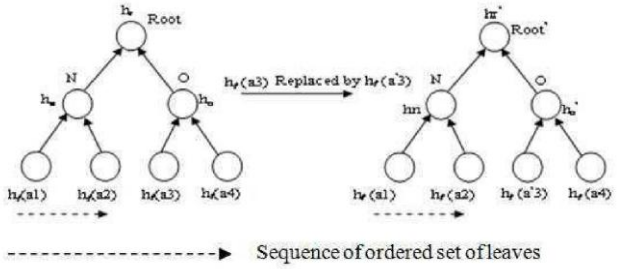

Fig-5. Updation of Improved Merkle Hash Tree Data Block

The IEIS achieved group auditing on different types of various formatted resources such as text files, different categories of image files, document files etc... through *k*-means cluster technique [11]. The group auditing can be processed by same types of resources on various batches make it a group through *k*-means clustering the data blocks or files (Eqn.4) on different batches [11] as shown in Fig. 6.

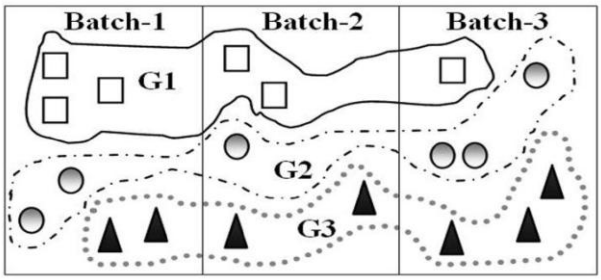

Fig-6. The Group Auditing by *k*-means Cluster Technique

$$\sum_{j=1}^{k} \sum_{i=1}^{n} \| x_i^{(j)} - c_j \|^2 \quad \cdots\cdots\cdots\cdots \quad (4)$$

Where || xi(j) - cj||2 mentioned the distance between the position of the resource and the cluster's centroid of batch auditing of various resources on cloud or offline storages.

The process for *k*-means-algorithm for *k*-means group auditing as shown in below:

i : Select *k* points as prime centroid in each batch of auditing

ii : Repetition (Repeat)

iii : Make *k* clusters by assembling all points to the adjacent centroid of group

iv : Estimate centroid of each cluster in multiple group batch auditing until the centroid don't change in group auditing

To maintain the flawless group auditing on various resources of various clients which require various segments like preliminary set-up, tag-signature-creation and auditing phase [11]. In preliminary set-up phase, the confidential key is assigned to resources of every user and stored at server. The tags-signature are created by secret key along with resources in tag-signature-creation phase. The auditing phase authenticated meta-data and its resources by signature and retrieved the resources in server [11]. All the non-academic and academic activities of IEIS are stored in both offline and online storages through cryptographic algorithm. The Internet-of-Things (IoT) sensors with alarm-

indication messaging system monitoring the whole IEIS indicates that if any data blocks on file or any other resources which has been corrupted or any other immoral occurrences or unauthorised user access has been involved then IoT Sensors with alarm-indication messaging system produce alarm indication or voice messages or SMS and send alert messages to respective in-charges of the concerned dept in IEIS. All the activities and process of IEIS are controlled by various sensor through IoT components. There is a distinct both online and offline log has been maintained to record all activities or all occurrences in IEIS. This cohesive IEIS which integrates both offline and online cloud service provider storages with IoT based IEIS alarm-indication messaging system is internet and mobile based supporting various operating system like android, windows phone and iOS. This IEIS provides capable solution for different types of clients to store their secret resources or files in various both offline and online cloud providers storages in form of encryption process with assistance of RC4 cryptographic algorithm is symmetric key based with initialization and operation phases [24] or secret sharing algorithm through file or resource split and combine mechanism as depicted in Fig. 7.

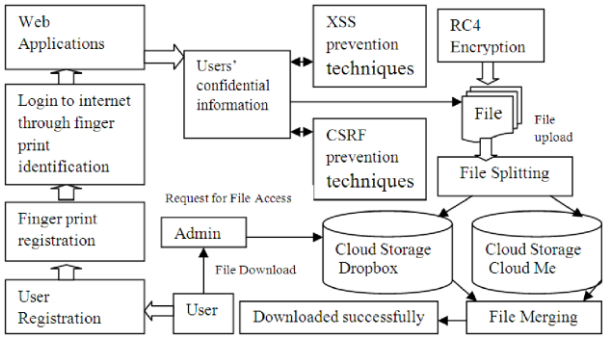

Fig-7. Resource Split and Merging mechanism and Prevention of resources in storages

In IEIS proposed one of the best authentication technique is biometric-based finger print mechanism [24,27] which assists to prevention of internet-based attacks such as cross site scripting (XSS), cross site request forgery (CSRF) and so on [24,27]. Nowadays all Indian citizens have Aadhaar card which bar code or quick response code which has been incorporated in all finger-print detection based electronic devices otherwise new user has to register their finger-print in the IEIS. Therefore, any type of client can verify their credentials, store and retrieve their confidential secret of all IEIS details through either in-built sensor of any system or biometric based finger-print electronic devices. The verification and validation of any categories of users can measured through finger-print verification method using minutiae map technique as shown in Fig. 8.

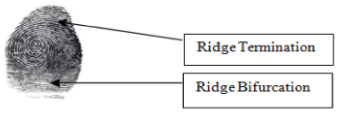

Fig-8. Biometric-based Client Finger-Print Verification using Minutiae Map Technique

In biometric-based finger-print mechanism, the ridge termination [24,27] and bifurcation is measured in the (Eqn.5) and (Eqn.6) as shown in below:

$$\sum_{i=1}^{m} N_i = 1 \quad \ldots\ldots (5)$$

$$\sum_{i=1}^{m} N_i > 2 \quad \ldots\ldots (6)$$

Where m=1 to 8 and Ni specifies finger prints.

In IEIS, any user finger-print characteristics and matching is done by minutiae map technique. The separation on any user finger-print provides a unique signature for every person. The procedure for identification of Minutiae map points extraction is depicted in below:

i) Select the any user finger-print copy of the image

ii) Calculate orientation field

iii) Process the finger-print through Gabor filter method

iv) Recognize and verify the minutiae point through template filtering technique.

The IEIS seeks and detects CSRF and XSS attacks on uniform resource location (URL) in different browsers of various systems. Cross site scripting is one of the internet-based cyber-attack which altered the script or code of any unsecured application at the end user's terminal. The susceptible vulnerable script is purposely injected into the unsecured uniform resource location of any website and the dangerous vulnerable script activated on URL and it performs the specified action assigned by attackers. By integrating confidential secret cookie is placed in the uniform resource location writing or web-application firewalls which leads to this type of web-based attacks cannot be permissible by treasured internet-based any type of website preventive methods such as http- request, securing or top-safeguarding cookie preference diminish, secret validation of client information [27].

The different users of IEIS are stored their academic and non-academic details in the form of RC4 cryptographic mechanism on cloud storage services such as CloudMe or AWS S3 storage or Google-drive or Dropbox or Microsoft Azure and other offline backup storages like log file or redundant array of independent disk [4,6,27]. This RC4 cryptographic algorithm has initialization and operation stages which encrypting all IEIS details and decrypt it in both offline storages and online storages.

The storing process of all IEIS details permits interleaved striping of dispersed identical parts of the redundant array of independent disk drive with parity enfolding details and achieved high level of redundancy due to partition striping and dispersed parity [27] mechanism as mentioned in Fig.9.

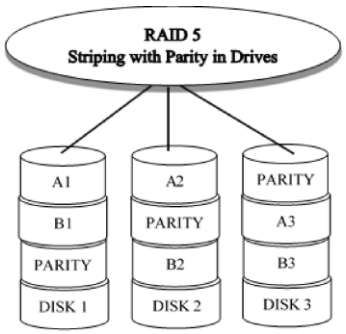

Fig-9. Redundant Array of Independent Disk Drive Interleaved Stripping with Parity Mechanism

4. RESULTS AND DISCUSSION

This Internet based Educational Information System (IEIS) using authentication auditing and storage techniques evaluates and accomplished effective utilization of bandwidth (bandwidth consumption) compared with CRUIS(Cost Reduction Usage of Infrastructure in Small scale sectors) method, HASSM (Homomorphism Authenticators using Sphere Shaped Marker) method and PPV (Probabilistic query and Periodic Verification) method. The performance evaluation for Internet based Educational Information System (IEIS) using authentication auditing and storage techniques has been compared the parameter of bandwidth utilization (bandwidth consumption) with file size among CRUIS, HASSM and PPV methods represented in Fig.10 which indicates that the IEIS method has bandwidth consumption (usage) can be calculated by once-a-month which has been compared with other methods like CRUIS, HASSM, PPV [28]. The bandwidth consumption is measured through confidential resources such as data

block of a file audit rate. The calculated value which indicates bandwidth consumption (Mb/sec) for the corresponding resources like data block on a size of file represented in (Gb). The utilization of bandwidth of the Internet based Educational Information System (IEIS) is increased by minimum 16.9 to maximum of 28.9% with Cost Reduction Usage of Infrastructure in Small scale sectors (CRUIS). Similarly, the competent utilization of bandwidth (consumption) of IEIS method is swiftly grown from 18.9 to 58.6% with Homomorphism Authenticators using Sphere Shaped Marker Method (HASSM). Likewise, the bandwidth consumption of IEIS method is escalation from 31 to 98.1% with Probabilistic query and Periodic Verification (PPV) method for various sizes of files.

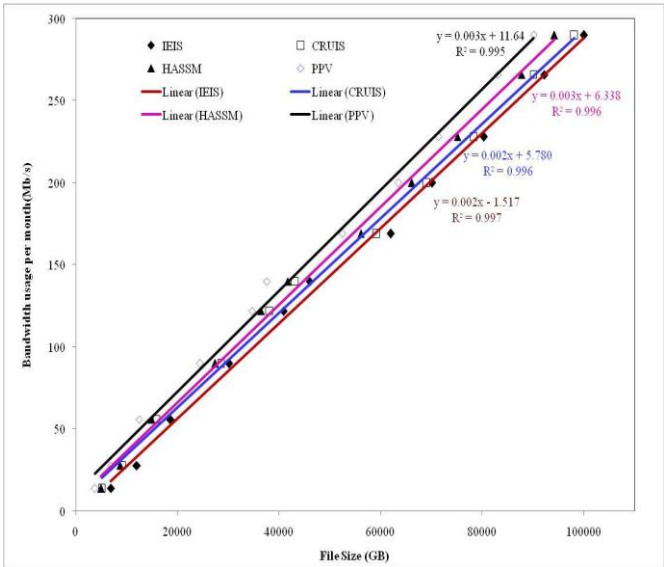

Fig-10. Comparison of Bandwidth Utilization of IEIS with HASSM, CRUIS, PPV method.

The IEIS using authentication auditing and storage mechanism evaluates computational and message transmission costs metrics or measurement ratio on different size of blocks of data on various files of academic and non-academic aspects has been depicted in Fig.11 which represents that computational and message transmission costs rapidly growing progressively with the request of various size of file and trial metrics or measurement ratio. The aim of this calculation is to diminish the computational and message transmission cost and maintains stability between efficient operational spending with average steady accuracy, which assist us to improve the better competence of authentication auditing and storage mechanism. Compute the competence or efficiency of internet based educational information system using authentication auditing and storage method file size *sz*, sample measurement ratio *w*, and data blocks on file. Our inspection indicates that the value of *s* should boost up with the growth of *sz* to fall the computational and message transmission costs. For sample example, the requested data block on files were preferred range 100 GB to 10000 GB, the sector numeral value or data block of file number were reformed from 89 to 1879 size of file, and the sample measure ratios were changed from 47 to 83 percent.

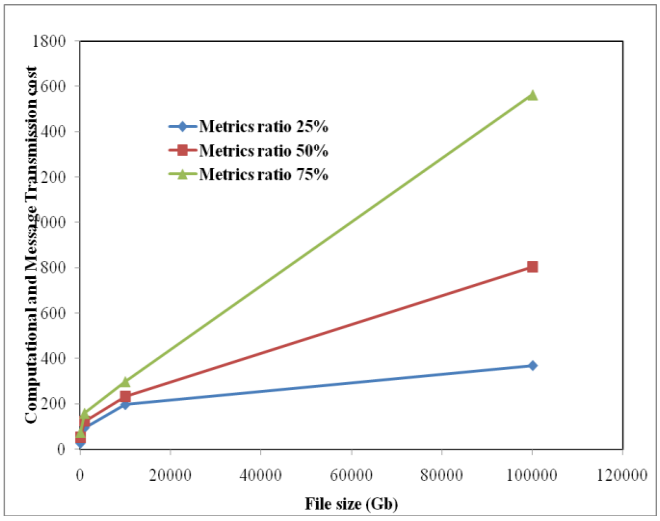

Fig-11. Computational and Message Transmission Cost for various Metric ratios Vs File Size

The Internet based Educational Information System (IEIS) assesses number of visits of client with respective to effective read operation efficiency compared with various methods such as HASSM and PPV method as represented in Fig.12.

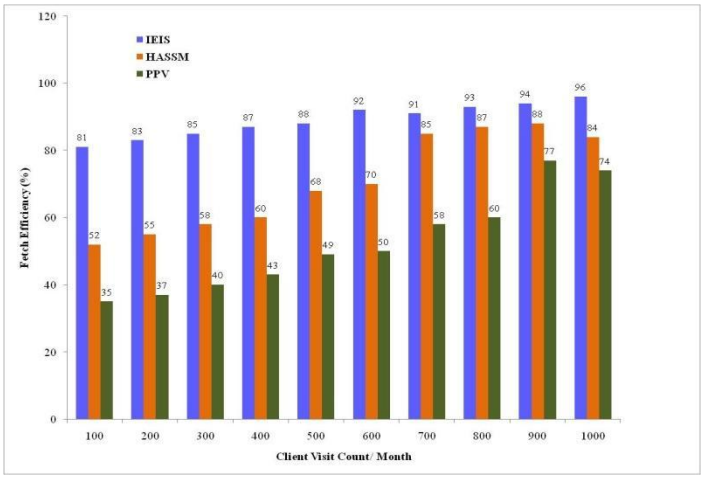

Fig-12. Comparison of Client Visit Count Vs Fetch Efficiency of IEIS with HASSM, PPV Method

The dynamic IEIS method achieved wide range of efficiency percentage of fetch operation with respect to different client visit count when compared with other methods such as HASSM and PPV [18,27,29] has been depicted in Fig.12.

The IEIS method make to approve the client and enhance read/write (fetch) operation percentage growing rapidly with user visit count and vice versa. The faultless efficient wide-ranging success rate of fetch operation of IEIS has range of 8% to 53% efficiency has been improved when compared with HASSM. Similarly fetch operation of IEIS has better result of 23% to 82% fetch efficiency has been improved compared to PPV method with respect to different client visit count. The faultless efficient fetch operation is one metric on IEIS files or resources or infrastructure based on various users call manipulation [18,27,29].

The one of the major feature of this paper is to manage and storing standard educational required functional and non-functional resources and NAAC, NBA, ISO documents in various online and offline storages which create strong relationship between various clients and cloud service storage providers. The secure IEIS storage method

retained good trade-off time, support better storage facilities with high-level various multi-security cryptographic mechanism as well as multi-authentication techniques. This paper compared the uploading time of various sizes of different format files and resources in various online as well as offline storages as represented Fig.13.

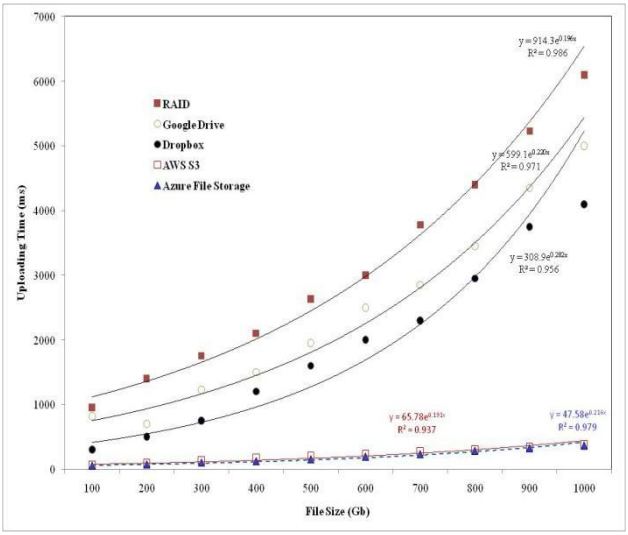

Fig-13. Comparison of File Size (Gb) Vs Uploading Time of files on On/Off line and Cloud Storages

Fig.13 indicates that the uploading time of cloud azure file storage and AWS S3 simple storage service which shows best reduction of uploading time (more than 92%) of various file sizes compare with other storages like Dropbox, GoogleDrive and offline storage like RAID. In future information-technology era, cloud service provider's storages is highly flexible, secured and trustable. The Dropbox is highly cloud-based file storage service which provides client-based cloud storages with small amount of storages provided to client with synchronization option. The uploading time of various size of files of Dropbox storage reduced 30-40% uploading time compare with offline storage RAID and 25-50% with Google Drive storage. The RAID offline storage produce less reduction of uploading time of various size of files compare with other storage method. The uploading loading time is calculated in terms of milliseconds and size of the file measured by Gigabyte for all types of storages. The comparison of user queried rate on number of files of different methods such as IEIS, CRUIS, HASSM and PPV methods are depicted Fig.14. In this IEIS system, client inquired rate indicates a quantity of optimistic, positive value in creating absolute outcomes to end users. The clients' files can be verified by IEIS method and magnifying the development of queried rate by 15% - 30% when compared with PPV method and similarly compared minimum of 8% and maximum of 10% is enlarged of client queried rate with HASSM and 2% to 3% with CRUIS. Therefore the IEIS achieved better client queried rate compared with other methods.

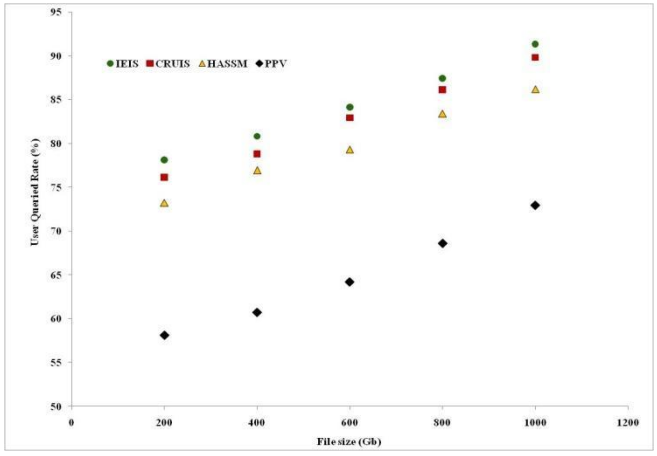

Fig-14. Comparison of File Size (Gb) Vs User Query Rate of various method.

The comparison of data verification (authentication) rate on user tasks of various methods such as IEIS, CRUIS, HASSM and PPV methods are represented in Table 2.

Table-2. Comparison of Data Authentication Rate on user tasks of various methods.

User Task Vs Data Authentication Rate					
No of User Tasks (Tasks - Read, Write, Modify, Execute on files)	**File Size (Gb)**	**Comparison of data authentication rate (% per tasks) of various methods**			
		IEIS	**CRUIS**	**HASSM**	**PPV**
1	200	93.2	92.7	90.5	80.6
2	400	94.9	93.5	91.3	81.7
3	600	96.2	95.8	93.6	82.5
4	800	97.9	96.9	94.1	84.8
5	1000	99.5	98.2	95.7	85.6

In IEIS, the data authentication has been achieved by improved merkle hash tree through bat mechanism and finger print mechanism. The number of user tasks can be categorized by tasks operation such as read, write, modify, execute or combination of one or operation and identification of user by finger print mechanism using Minutiae map method. From the Table 2, it has been observed that the IEIS data authentication rate is increased from 11% to 14% when compared with PPV, similarly 3 to 5% with HASSM and 1 to 2% with CRUIS. Therefore authentication rate in IEIS is linearly increased compare with other methods.

The comparison of computational cost on different sizes of files of various methods such as IEIS, CRUIS, HASSM and PPV methods are represented in Fig.15.

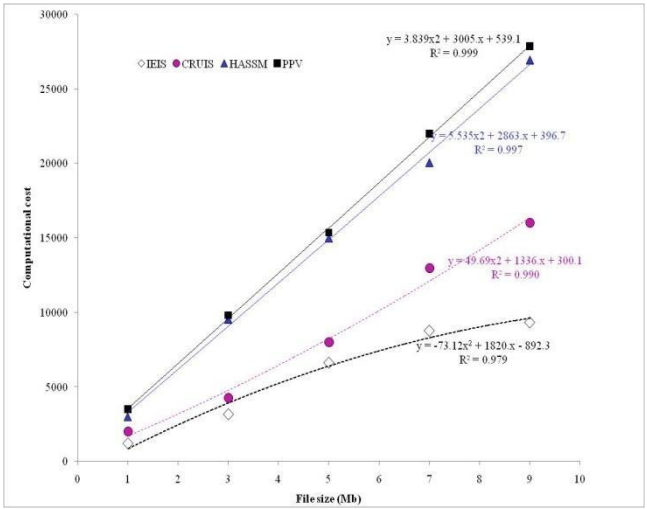

Fig-15. Comparison of File Size (Gb) Vs Computational Cost of various methods

Fig. 15 shows the computational cost of IEIS has been reduced from 40% to 65% compare with PPV and 30% to 60% with HASSM and 10% to 50% with CRUIS. It has been observed that the IEIS performed better computational cost compared with other methods.

Presently the more number of attacks, threats and vulnerable script has been found in world-wide IT based educational and other sectors. It has been observed that huge number of attacks has been available in global IT based commercial applications or web-portal as depicted in Table 3.

Table-3. Attacks, vulnerable scripts and other threats in global IT based commercial web portal.

Attacks / Vulnerable Script	**Percentage**
Cross-site scripting attacks	83%
Cross-site request forgery attacks	71%
Sql injection based scripts	14%
Phishing attacks	25%
Other threats or injection scripts	09%

The IEIS application highly reduced attacks, threats and vulnerable scripts, the Table 4 shows before and after implementation of prevention techniques of various web-portal-based attacks like Reflected and Stored XSS (cross site scripting) attacks found in IEIS application and it can be tested on ieees.online.com. After implementation of prevention techniques, many number of attacks found in vulnerable script and DIV and Span tag has been removed.

Table-4. Comparison of web-attacks before and after implementation on commercial web portal.

Attack Reflected XSS and Stored XSS Tested on www.ieees.online.com			
Reflected XSS	**Vulnerable script**	**DIV tag**	**Span tag**
Before Implementation	22	39	15
After Implementation	03	04	01
Stored XSS	**Vulnerable script**	**DIV tag**	**Span tag**
Before Implementation	20	40	16
After Implementation	02	05	02

Table 4 shows, In reflected XSS, huge number of attacks found on vulnerable script and tags like DIV and Span has been removed and similarly in stored XSS also very large of number of attacks found script and tag has been erased which had been tested on ieees.online.com.

5. CONCLUSION AND FUTURE ENHANCEMENT

In this information technology era, many educational institutions and other commercial organizations are scared due to unsecured web-based attacks, threats, security and privacy issues on confidential data while sharing their of details across the global world. Nowadays most of the educational institutions need continuous quality improvement-based institutional information system based on their accreditation bodies like NAAC, ISO, NBA requirements. Therefore more number of internal as well as external audits is required to maintain the confidential records in internet-based educational information system. Nowadays most of the organizations are frightened with respect to information stored in offline storages are insecure due to malicious insiders, hackers and attackers activities. In order to avoid this situation, we proposed internet-based educational information system (IEIS) using offline / online cloud storages along with authentication and auditing methods. This IEIS provides three dimensional architecture or layer which support different level of users or clients of educational information system. In this IEIS many clients stored their confidential details through Amazon and Azure cloud storages, other online storages such as dropbox, cloudme along with offline

storages like redundant array of independent disk storage and log files which keep track of user activities. The different categories of user's ranges from clerical to management advisory executive committee members used this internet based educational information system. This IEIS solved many issues like security, privacy, data integrity, user authentication, data authentication and availability of data when storing and sharing of confidential details among various users of any information technology-based organization. To guarantee the security on data has been stored in various storages through cryptographic RC4 encryption and decryption method. The improved merkle hash tree method using bat mechanism ensured data authentication. Storage utilization can be measured by internet of things-based sensors. The IoT based sensors generated sound warning system along with alert messages sent to user when user cross the limits of utilization of storage of this system. This system ensured user authentication through various bio-metric methods, Aadhaar card and multi-way authentication methods such one-time passcode, email messages and many more techniques has been enforced. Moreover all the administrative and academic related details are stored in online and offline and cloud storages through cryptographic RC4 algorithm which ensure data availability, information confidentiality, data security, data integrity and guaranteed the protection on resources from threat and attacks. This IEIS system accomplished and implemented the detection and prevention techniques of cross site script attacks enforced on web portal accessed by various clients like desktop users, laptop users and mobile users. This paper implements the priority based user access privileges and access control method to access the entire system for various clients of this internet-based educational information system. The proficient *k*-means cluster method mainly focused and achieved individual, group auditing mechanism. With respect to performance evaluation, this IEIS attained better outcome and compare with different methods like CRUIS, HASSM and PPV in terms of bandwidth consumption, user visit counts with fetch efficiency, data authentication rate, computational cost. This system evaluates computational and message transmission cost, comparison of stored and reflected cross scripting attacks before and after implementation on web portal. This paper adopts quality management system with multi-level security achieved better efficiency and reduced web-based attacks in this internet-based educational information system. Further in future the well-adopted and equipped hardware interfaces with supporting all types of operating system for wireless based devices has been enforced with this internet-based educational information system.

REFERENCES

1. DaojiangWanga et. al (2020), "A Novel Application of Educational Management Information System based on Micro Frontends",24th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, Published by Elsevier B.V. Science Direct Procedia Computer Science 176 1567–1576, 2020.
2. MuhammadFurqonet. al (2023), "The Impact of Learning Management System (LMS) Usage on Students" ,TEM Journal. Volume 12, Issue 2, pages 1082-1089, ISSN 2217-8309, DOI: 10.18421/TEM122-54, May 2023.
3. Nik Elyna Myeda et. al (2023), "Adopting quality management (QM) principles in managing facilities management service delivery", International Journal of Quality & Reliability Management, ISSN: 0265-671X, Emerald Publishing Limited, Vol. 40, Issue 10, pp. 2393 – 2419, 2023.
4. Serhii Petryk et. al (2023), "The effectiveness of quality management strategies in health care organizations: an analysis of quality standards implementation and clinical performance improvement", Amazonia Investiga, ISSN: 2322-6307, Volume 12, Issue 68, pp. 333-345, 2023.
5. Zheng Gu et. al (2023), "Elastic RAID: Implementing RAID over SSDs with Built-in Transparent Compression", SYSTOR '23: Proceedings of the 16th ACM International Conference on Systems and Storage, Haifa Israel, Association for Computing Machinery, New YorkNY United States, ISBN:978-1-4503-9962-3, pp.83-93, 2023.
6. Adnan Tahir et. al (2020),"A Systematic Review on Cloud Storage Mechanisms Concerning e-Healthcare Systems", MDPI Journals, 2020.
7. Dr.T.KamalaKannan et. al (2019), "Study on Cloud Storage and its Issues in Cloud Computing", International Journal of Management, Technology And Engineering, Volume 9, Issue 1, pp.976-981, 2019.
8. Durga Venkata Sowmya Kaja et. al(2019), "Data Integrity Attacks in Cloud Computing:A Review of Identifying and Protecting Techniques", International Journal of Research Publication and Reviews, Vol 3, no 2, pp 713-720, February 2022
9. Mohammed Aziz Al Kabir et. al (2023),"Securing IoT Devices Against Emerging Security Threats: Challenges and Mitigation Techniques", Journal of Cyber Security Technology, Volume 7, Issue 4, pp.199-223, 2023.
10. Yuchong Li et. al (2021),"A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments"Energy Reports Open Access" Science Direct Elsevier, Volume 7, pp. 8176-8186, 2021.

11. Srinivasan S et. al (2014), “Dynamic Group Audit Control Mechanism for Cloud Computing Using *k*-means Inter-Batch Cluster Method” International Journal of Applied Engineering Research, Volume 9, Number 22 (2014) pp. 16821-16835,2014.
12. Behnam Zahednejad et. al (2023), "A Lightweight, Secure Big Data-Based Authentication and Key-Agreement Scheme for IoT with Revocability", International Journal of Intelligent Systems (Hindawi), Volume 2023,Article ID 9731239, pp.1-19,2023.
13. Srinivasan. S and K.Raja (2018),“An Advanced Dynamic Authentic Security Method for Cloud Computing”,In: BokhariM., Agrawal N., Saini D. (eds) Cyber Security - Advances in Intelligent Systems and Computing(AISC) Book Series, Volume 729, (pp.143-152), Springer, Singapore, June 2018.
14. Mohammad Aldossary (2023), “Multi-Layer Fog-Cloud Architecture for Optimizing the Placement of IoT Applications in Smart Cities",Computers Materials & Continua, Vol.75 Issue 1, pp.633-649,2023.
15. Wenjun Luo,Die Lai and Zesen Dai (2023), ”Research on disturbing white-box cryptography algorithm based on local differential privacy" Security and Privacy, Wiley Publications, 2023.
16. A F Doni et. al (2019),“Implementation of RC4 Cryptography Algorithm for Data File Security”, Journal of Physics:Conference Series International Conference on Science and Technology, 1569 (2020) 022080, IOP Publishing, 2019.
17. Raghda Sattar Jabbar (2023), "Triple Encryption of Images based on RC4, Zigzag, and Elliptic Curve Algorithms for Enhanced Security”, International Journal of Scientific Research in Science, Engineering and Technology,Vol.10, Issue 2,pp.93-100, April 2023.
18. Srinivasan.S and Raja.K (2016), “Ensuring Cloud Security and Privacy Through Enhanced Merkle Hash Tree Method using Bat Mechanism" published in Australian Journal of Basic and Applied Sciences Volume 10(1) , pp.676- 684 ,2016.
19. Shayma Wail Nourildean et. al (2023), "IoT based Wireless Sensor Network Improvement Against Jammers Using Ad-Hoc Routing Protocols",International Journal of Interactive Mobile Technologies, Vol.17, Issue 07,pp.133-147, 2023.
20. Joseph Williamson and Kevin Curran (2021), "The Role of Multi-factor Authentication for Modern Day Security", Semiconductor Science and Information Devices, Volume 03, Issue 01, pp.16-23, April 2021.
21. Nassim Ammour et.al (2023), "Multimodal Approach for Enhancing Biometric Authentication", Journal of Imaging,Vol.9, Issue 68, pp.1-12, 2023.
22. Swapnil Sutar et.al (2023),"Implementation of a secret sharing-based masking scheme against side-channel attack for ultra-lightweight ciphers in IoT",International Journal of Information and Computer Security, Vol.21, Issue 3/4, 2023.
23. Shivendra Bhonsle et. al (2023), "Microsoft Azure vs Amazon Cloud Services: A Comparative Analysis", Iconic Research And Engineering Journals, Iconic Research And Engineering Journals, Vol.6, Issue 9, pp.1-6, March 2023.
24. Srinivasan.S and Raja.K (2016), "Preventing Cloud Attacks using Bio-Metric Authentication in Cloud Computing", Indian Journal of Science and Technology,Vol. 9, Issue 23,pp.1-9,June 2016.
25. Amardeep Kaur et. al (2023),"Adaptive Access Control Mechanism (AACM) for Enterprise Cloud Computing", Journal of Electrical and Computer Engineering, Vol.2023,Article ID 3922393,pp.1-30,July 2023.
26. Anand R et al (2014), “Solution of Unit Commitment Problem using Bat algorithm”, International Journal of Engineering and Technology Innovations, pp.15-19, Vol 1, Issue 2, May 2014.
27. Srinivasan S et. al (2021),"A Structured Protective Cohesive Health Care Information System using Security and Storage Mechanism In Cloud”, International Journal of Engineering Trends and Technology, ISSN :2231-5381, Vol.69, Issue 3,pp.29-33, 2021.
28. Srinivasan S et. al (2023), “Effective Cost Reduction of Usage of Infrastructure in Small Sectors using Cloud Storage and Internet of Things”, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN :2321-8169, Vol.11, Issue 9,pp.2441-2447, 2023.
29. Sathiya Moorthy Srinivasan, C. Chandrasekar, “Providing Dynamic Audit Services Using Homomorphism Authenticators in Cloud Infrastructure”, Journal of Theoretical and Applied Information Technology, Vol.67, No.3, pp.580-590, 2014.