Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MULTI LEVEL USER VALIDATION MODEL WITH ASYMMETRIC CRYPTOGRAPHY FOR CLOUD DATA SECURITY

K.VENKATESWARARAO[1], P MANIKYA PRASUNA[2], KALPANA SANJAY PAWASE[3], T.V.N.PRASANNA[4], KATAKAM RANGANARAYANA[5], V.LAKSHMAN NARAYANA[6]

[1]Department of CSE, Andhra Loyola Institute of Engineering and Technology, Vijayawada, India
[2]Department: CSE, KLEF (Deemed to be University), Vaddeswaram, Guntur, Andhra Pradesh, India.
[3]MIT Academy of Engineering, Alandi (D.), Pune -412 105
[4,6] Vignan's Nirula Institute of Technology and Science for Women, Guntur, Andhra Pradesh, India.
[5]Senior Quality Analyst, Xinthe Techonologies Pvt. Ltd. Visakhapatnam, Andhra Pradesh, India.

Email: [1]siva278@gmail.com, [2]prasunamanikya@gmail.com , [3]kalpana.pawase@mitaoe.ac.in
[4]tvnp11@gmail.com , [5]katakam916@gmail.com , [6]lakshmanv58@gmail.com

ABSTRACT

Even though cloud computing makes data storage and service delivery more affordable, adaptable, and scalable, it is still particularly susceptible to data breaches, insider assaults, and unwanted access. In light of these difficulties, the authors of this study present a novel approach to authentication accuracy and data protection in cloud environments: the Multi-Level User Validation Model with Asymmetric Cryptography (MLUVM-AC). To prevent identity spoofing and illegal data modification, the architecture combines public-private key encryption with multi-stage user validation to guarantee that encrypted data may only be accessed by certified users. The suggested approach offers a layered authentication technique with asymmetric key management, which is an improvement over traditional systems that use symmetric encryption and single-layer password validation. This leads to better performance and improved security. If we compare our model to the current state of the art, we find that it generates keys 17% faster, improves data security correctness by 18%, and improves validation efficiency by 20%. This study adds to the existing body of knowledge by developing a stable, efficient, and extensible method for protecting data in ever-changing cloud environments through the integration of multi-level authentication with asymmetric cryptography.

Keywords: *Cloud Computing, Data Security, User Authentication, Authorization, Asymmetric Cryptography.*

1. INTRODUCTION

As a business model, computing revolves around charging customers for the use of shared, on-demand computer resources and services hosted in the cloud. Because of this, computing services can be pooled without specific server software and hardware being required to store data. Cloud services can be broadly categorized into three areas based on the needs of its end users: software as a service, platform as a service, and infrastructure as a service [1]. Software as a service provides a cloud computing platform that can be accessed from any location with an internet connection. But the customer needs the right license from the cloud provider to use the service [2]. Concerns about the safety of sensitive information are paramount when it comes to cloud computing. Since the cloud is where most sensitive data is going to be kept, it is crucial that cloud service providers provide excellent security [3].

The security of cloud storage was enhanced with the implementation of authentication methods [4]. One such approach is derived from cryptography and comprises encoding or storing information in a way that only the intended users can access it [5]. Cryptography is essential to cloud computing because it prevents unwanted parties from accessing sensitive data kept on the servers of cloud service providers [6]. It is essential in a cloud environment to safeguard private data without

compromising communication speed and to implement stringent access controls. One way to ensure data security in cryptography is to use a public key cryptography approach or a secret key cryptography algorithm [7]. When encrypting and decrypting data, secret-key cryptography (also called symmetric encryption) uses a single key. Asymmetric encryption, or public key cryptography, uses two keys—one for encryption and one for decryption [8].

In today's globally linked world, cloud computing is rapidly replacing on-premises computer systems. Cloud computing is a model for efficient, on-demand networks that meet specific needs, says the National Institute of Standards and Technology (NIST). The concept of cloud computing has the potential to be a helpful model for validating data storage with little overhead and contact with service providers [9]. Features such as on-demand self-service, extensive network access, metered service, rapid adaptability, and resource sharing are the foundation of cloud computing [10]. A few examples of deployment models are private clouds, public clouds, hybrid clouds, and community clouds. In the cloud service model, you can find software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). In order for cloud computing to function properly, all of the following must be secure: virtualization, distributed computing, SOA, high-speed networks, applications, data transport, storage, and so on. The security requirements for these essential cloud components vary according to the deployment methodology chosen by the cloud user [11]. This study aims to provide a user validation approach that could solve the issue of public cloud data security [12].

A company engages in business process outsourcing when it contracts out to another entity the performance of non-essential tasks that bog down its internal operations. organizations often opt to hire other organizations to handle certain tasks in order to get the most rewards [13]. Most companies that outsource their operations will likely employ cloud computing. This model enables them to purchase computer and storage capacities as needed from the service provider, which reduces operational costs [14]. Companies can save a ton of money on capital costs by owning the necessary infrastructure internally to meet the unpredictable and erratic compute demand [15].

The cloud types and deployment models are shown in Figure 1.

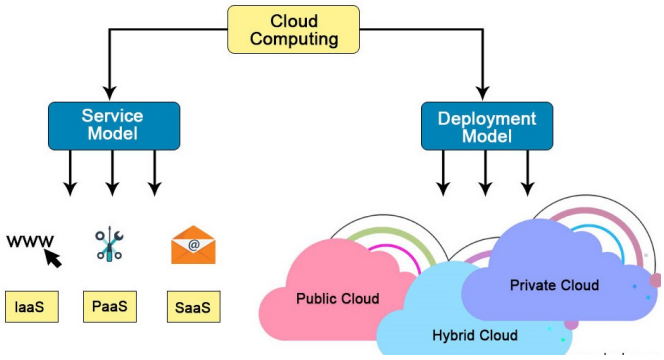

Fig 1: Cloud Types and Deployment Models

Although there are numerous clear benefits to using the cloud, many companies are hesitant to do so due to concerns about data security. Cloud Security Alliance research shows that security concerns are still holding back widespread use of cloud computing [16]. The most significant obstacles to the widespread use of cloud computing include, but are not limited to, concerns about data breaches, impairments in IT services, business processes, and data recovery. Shared hosting at another party's facilities houses an increasing number of enterprises, and as a result, the data owner does not have full control over the information and calculations [17]. Due to the large number of people, both inside and outside the firm, having access to and sharing data stored in the cloud, it is essential for businesses to ensure that this data is secure, intact, and always available. Owners of data are obligated to take extreme measures to protect sensitive information due to the seriousness of the threats to their data [18].

To avoid overspending or being vulnerable to repeated attacks, this study suggests an adaptive security model based on data sensitivity [19]. This model can offer an adequate level of protection for information classified under different classes, as opposed to using a single security method or a common multiple safety method for all data. An overview control method based on log analysis enables the restructuring of information based on required changes in data thresholds and variations in security precautions to meet the changing adjustments in cloud security risks [20]. The security management system also includes appropriate access control and data encryption [21]. Businesses and consumers alike can take use of dependable, scalable, and inexpensive cloud computing services. The decentralized service-oriented design, multi-user, and multi-domain

administrative infrastructure of cloud computing are the direct causes of the heightened security threats that come with it. Ensuring the security and privacy of user data stored in the cloud is presently receiving a lot of attention. Some examples of cloud services include file hosting, email, social media, and business applications [22]. Cloud computing works on the notion of virtualization, which enables several users to use a single huge machine as if they had access to all of its resources [23].

The cloud computing model makes it possible to access data and computer resources from any place with an internet connection. Cloud computing involves the simultaneous use of pooled resources, such as data storage, networks, processing power, and specialized user and business applications. All businesses are moving their data storage to the cloud because of the many compelling advantages. More emphasis should be placed on cloud service providers in terms of safeguarding customer data [24]. Customers should verify that their cloud service provider has enough security measures to protect data before using their services. Software isolation, data protection, availability, dependability, and provenance are all aspects of trust architecture. The difficulties can be categorized into several types, including backups, internet-based information and its conversion, support for several platforms, and intellectual property [25]. Securing processing and storage are two aspects of cloud security that must be considered while protecting data and procedures. Data security rests on three pillars: solidity, privacy, and accessibility. Data kept in the cloud is protected from prying eyes by using cryptography. Cryptography is commonly considered a hybrid of the three main types of algorithms. Asymmetric key algorithms and hashing come first, followed by the other two. Data stored is guaranteed to be legitimate by using hashing algorithms. The main method of data cryptography is encryption, which makes data unreadable and incomprehensible both in transit and when stored. The data securing process in cryptography is shown in Figure 2.

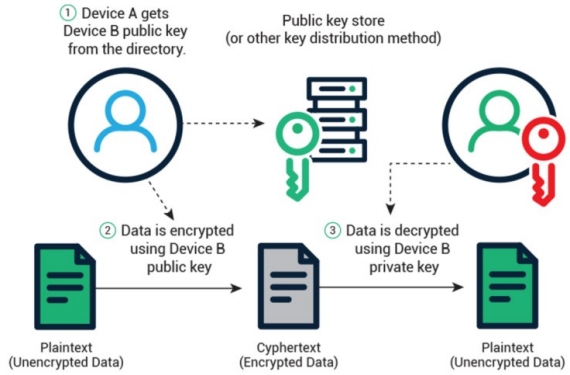

Fig 2: Data Security using Encryption

Hypothesis

H0: Multi-level user validation integrated with asymmetric cryptography does not significantly improve authentication accuracy or data security in cloud environments compared to existing models.

H1: Multi-level user validation integrated with asymmetric cryptography significantly enhances authentication accuracy, key management efficiency, and data security in cloud environments compared to existing models.

The primary goal of cryptology is to protect information from unauthorized access. To obtain the original data back from encrypted data, the process is called decryption. Either symmetric-key and asymmetric-key techniques can be used to encrypt data in the cloud. Since the databases found in cloud storage are so numerous, the performance of asymmetric-key algorithms is best than that of their symmetric-key counterparts. The business can maintain a steady state load in the cloud platform, then, if necessary, request additional computing power from the public cloud. Common issues like governance, security, and compliance are shared by many enterprises in this deployment model's community. Typically, this term is used to describe cloud computing infrastructures that are shared and controlled by a group of companies who operate in the same topic or competitive market. The cloud computing infrastructure with cryptography is shown in Figure 3.

Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

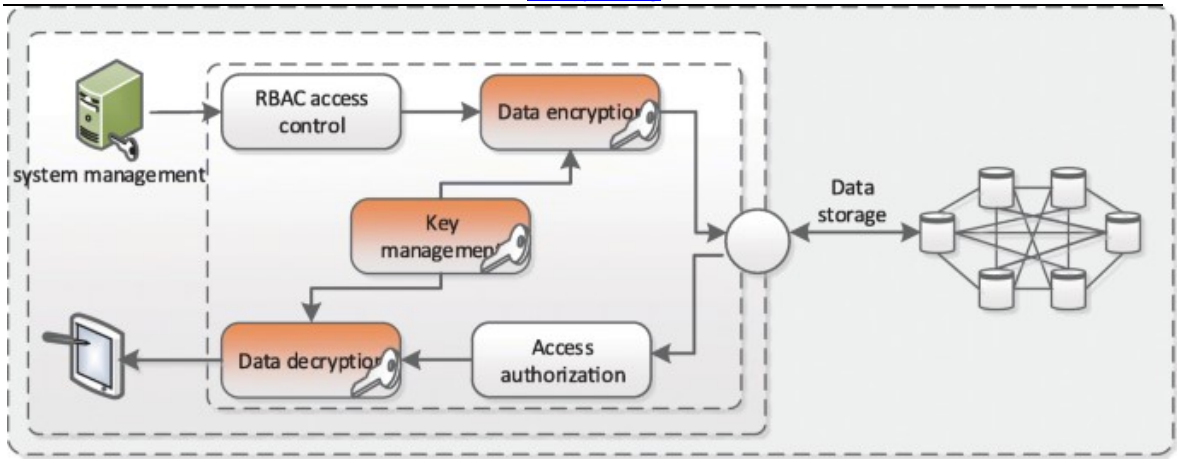

Fig 3: Cloud Infrastructure with Cryptography Model

Multi-Level User Validation Model with Asymmetric Cryptography for Cloud Data Security is a research model that primarily aims to secure, encrypt, and authenticate data stored in the cloud. Concerns over the potential exposure of sensitive user data to various vulnerabilities stems from the increasing reliance on cloud infrastructures for storing, processing, and making data accessible. Cloud computing has many benefits, such scalability and cost reduction, but the authors stress that it also opens new doors for insider threats, illegal access, and data breaches [26]. The research is based on the essential challenge of protecting user and organizational data stored in the cloud from both external and internal attackers, as the number of users storing this data in the cloud continues to grow.

Current authentication methods and data security strategies have their shortcomings, which is why this primary concern was chosen. When it comes to protecting sensitive data in the cloud, older methods of authentication, such using a username and password, aren't always up to the task. Unfortunately, user accounts are still being compromised by weak passwords, password reuse, and phishing assaults, rendering single-factor authentication an ineffective security measure [27]. According to the research, most cloud systems make it easy for attackers to access massive volumes of data with just one authentication credential [28]. In order to address this issue, the authors suggest a paradigm for user validation that involves multiple levels of verification. This model would prevent both external intrusions and inner misuse by introducing additional checks before allowing access to cloud resources.

The importance of asymmetric cryptography in protecting the privacy and authenticity of data stored in the cloud provides more support for this area of study. The study highlights the importance of cryptography in cloud security, since it guarantees that encrypted information may only be accessed by authorized users with valid decryption keys. Compared to symmetric methods, the model's use of asymmetric cryptography, which employs a public key for encryption and a private key for decryption provides stronger protection while minimizing the threat of key exposure. This technique guarantees safe data transmission and storage across different cloud systems and also prevents illegal access. In addition, the authors state that since asymmetric encryption prevents tampering with sensitive data during transmission, it improves trust between customers and cloud service providers.

When using cloud storage, data belonging to any given business or person is kept in and accessed via a network of remote servers. Secure communication over networked, dispersed resources is impossible without the use of encryption algorithms. The data is transformed into an unintelligible format by the encryption algorithm using the key, and only the user possesses the key necessary to read the data. Asymmetric key encryption is the employed model in this research that employs two keys, a private one and a public one. The secret key can be used for decrypt whereas the single key is being used for encrypted data. The security of cloud storage is already ensured by a variety of methods. In this research, an effective Multi Level User Validation Model with Asymmetric Cryptography (MLUVM-AC) for cloud data security is proposed for providing data security.

2. LITERATURE SURVEY

Findable and Verifiable Symmetric encryption is a crucial cloud security method since it enables users to retrieve encrypted cloud data via keywords and validate the authenticity of the results. One of the most prevalent and important requirement for system users in such schemes is periodic update for cloud data. The current verifiable SSE systems that allow for dynamic updates to data appear to all rely on asymmetric-key cryptography, which necessitates time-consuming processes for verification. The vast volume of data stored in the cloud raises the possibility that verification will become an excessive burden. Therefore, the most pressing unanswered question is how to accomplish keyword search over dynamically encrypted cloud with efficient verification. In this research, Ge et al. [1] analyzed the feasibility of establishing search term over dynamically encrypted cloud with symmetric-key oriented verification and present a feasible technique to address this issue. The innovative Accumulated Authentication Tag (AAT) uses symmetric encryption to create one authenticity tag for every term, allowing for the quick verification of dynamic data. When dynamic operations are performed on cloud data, the authenticity tag can be updated easily with the accumulated property of developed AAT. The author proposed a new secure index that consists of a searching table ST based on the axial list and a verified list VL including AATs in order to ensure efficient data update. ST's interoperability and adaptability allow for much greater efficiency gains while applying updates. The proposed approach has been proven secure and efficient through many analyses and evaluations.

The term cloud computing refers to a new computer paradigm that intends to make available on-demand computing power, vast data storage, and adaptable data exchange services. Due to the exponential increase in data creation, businesses and consumers are increasingly drawn to cloud storage services for their data. The security and privacy of critical information, however, is increasingly at risk when stored on remote cloud servers. Before putting information into the murky depths of the cloud, it should be encrypted. The current standard encryption techniques place a large burden on data owners in terms of maintaining files and encryption procedures. Some systems are not suitable for safeguarding cloud data because of security, efficiency, or usability flaws. In this work, Khashan et al. [2] presentedOutFS, an encrypted file system designed for end users and aimed at supplying transparent encryption for outsourced data at rest and in transit. The author combined symmetric and asymmetric cryptography in a hybrid system to secure data in OutFS. The system for managing keys is both secure and user-friendly. The identity-based encryption (IBE) method is built into OutFS to protect the privacy of shared data. OutFS is built to guarantee the security of outsourced data and the integrity of the file system.

It is generally acknowledged that data should be encrypted before being uploaded to the cloud in order to maintain privacy. This raises the difficulty of conducting data analysis, particularly association rule mining, while maintaining confidentiality of the data being mined. Homomorphic encryption is proposed as a potential solution since it enables the processing of encrypted data without the need for decryption. Most practical applications only use a single cloud server, however the dual structure is generally used in cryptography association rule mining systems based on asymmetrical homomorphic encryption. However, privacy leakage issues plague the existing associated single cloud server approaches. Hong et al. [3] described a global safe multiplication protocol using a single cloud server, based on a distorted circuits and additive homomorphic encryption, to address this deficiency in the existing literature. The invertible protocol, comparative protocol, frequent item protocol, and final privacy-preserving association rule mining process are all built off of this foundational multiplication technique. Finally, the author presented the results of theoretical security analysis and performance evaluation of the project protocols.

The increasingly interdependent digital ecosystem generates massive amounts of information that must be protected from prying eyes. Data breaches are becoming increasingly common as a result of the development of new technology and the application of novel techniques by attackers. The General Public's Key Establishing data security through secrecy, integrity, and authenticity is made possible by cryptography's collection of cryptographic methods. RSA is a widely-used algorithm in the field of public-key cryptography and the field of cryptography as a whole. Since its creation, it has been widely embraced for use in cloud, image, and other data security applications. There is a lack of a comprehensive and systematic review of this topic in the literature despite its relevance and usefulness. In this paper, Imam et al. [4] gave a comprehensive and methodical examination of RSA-based encryption across many application areas. Mixed, Simultaneous, Clouds,

Picture, Multiple-Keys, Chinese-Remainder-Theorem-based, Digital-Signatures, K-Nearest-Based, Batch, Wireless, and Core-Modifications are the broad categories into which all existing work in this area falls. This research examines RSA-based cryptosystems systematically, classifying them in different categories before offering conclusions and suggestions. This includes both variations on the original RSA protocol and enhanced RSA implementations in a wide range of fields. This research evaluates and contrasts RSA implementations with respect to a variety of criteria, including key generation, encryption, decryption, key characteristics, and enhancements, and it identifies the most prominent contexts in which modified RSA has been used recently.

Businesses and people alike have found that outsourcing their vast amounts of data to untrusted servers in the cloud is among the most price services in cloud computing. Efficiency, adaptability, dependability, and security are just few of the aspects of this application situation that have been the focus of research. In this work, Morales-Sandoval et al. [5] discussed the safety of cloud storage in the context of a scenario in which users encrypt and then outsourced data, share their data in cloud with the other users, and then query the service provider for search and retrieving of encrypted data. As a main differentiator, the author proposed a security strategy for encrypted cloud storage, sharing, and retrieval that is built entirely on the foundation of attribute-based encryption (ABE), allowing for access control systems over both the encrypted data and the information retrieval task via search access control. In contrast to previous efforts, this method takes into account three distinct aspects of efficient encryption, cloud-based data encryption in bulk, attribute-based encryption digital envelope key management and attribute-based searchable encryption (ABSE). To provide security levels of 128 bits or more, selected ABE algorithms are used from the knowledge base and give innovative structures for ABSE over the asymmetrical setting.

A promising use case for cloud computing is the administration of big-data files and the processing of queries across a decentralised cloud infrastructure. Private information and documents are often encrypted before being saved in the cloud to prevent privacy leaks. Traditional encryption methods, on the other hand, make it difficult to conduct a search within the encrypted data. To retrieve information hidden in cipher texts, searchable encryption serves as a helpful cryptographic primitive. Traditional searchable encryptions, however, have poorer search efficiency and cannot do fuzzy multikeyword queries. To address this problem, Zhang et al. [6] offered a searchable encryption that enables private information fuzzy multikeyword searching (SE-PPFM) in cloud environments, which is constructed using asymmetrical scalar-product-preserving encryption methods and Hadamard product operations. Through the use of Word2vec, a machine learning primitive, users are able to acquire a fuzzy higher rated between encrypted files and queries' predicates, thereby realising the capability of efficient fuzzy searches.

Some suppliers of Location-Based Services (LBS) are enticed to move their geospatial information and querying service to the commercial cloud as a result of the many benefits associated with data outsourcing. However, sensitive data must be encrypted before being outsourced so that it cannot be misused, as in the case of a geographic information query. To solve this issue, various prior studies concerning secure searching on encrypted database might be directly implemented in outsourced LBS scenario, however none of them are optimised for linear-region-search (LRS). The LRS is a popular form of LBS utilised by nav systems; it searches for query segments and returns POIs that are close by. In this study, Zhang et al. [7] tackled the complex issue of private information linear region search for the first time. In particular, author opted for the quadtree structure for creating the index for the POI database; this allows to quickly retrieve the LRS results by identifying the rectangular sections through which the query segment travels. The authorproposed a new algorithm for precisely identifying whether a segments crosses with a rectangular on ciphertext, using computational geometry and an Asymmetrical Scalar-product Preservation Encryption (ASPE) approach, to preserve the security of both LBS owners and consumers. Furthermore, this algorithm offers a novel approach to addressing various computational issues in the context of encrypted 2-dimensional geometries. The author presented two privacy-preserving LRS methods and associated dynamic update operations based on the divergent privacy needs of two threat models.

O. A. Khashan, proposed Fog computing is an exciting new paradigm that has the potential to ease the strain on cloud-based central processing caused by the massive amounts of data generated by the IoT. With its low delay, storage, and processing resources, fog computing is a boon to the IoT, but it does not come without its fair share of security and

privacy concerns. When it comes to protecting the privacy of data sent between devices in the fog, proxy-re-encryption (PRE) is indeed an efficient cryptographic solution. In PRE schemes, however, the heavy data processing activities of data owner encrypted data and consumer data transfer due to uneven cryptographic usages, as well as the difficulty of a handling delay caused by transferring high computing burden to the proxy for reencryption, remain unanswered in the literature. To ensure private data transfer in fog-to-things computing, Khashan et al. [8] offered a hybrid proxy-re-encryption technique that uses both symmetrical and asymmetrical encryption algorithms. The re-encryption process in the proposed approach requires little computational resources from fog nodes. Meanwhile, the approach can lessen the burden of encryption and decryption on users with limited hardware. The results of the performance and security analyses show that our method is safe, very effective, and very compact.

When contrasted with the methods already mentioned in the literature, the MLUVM-AC that has been suggested exhibits unique contributions and better results. The suggested paradigm combines asymmetric cryptography with multi-level user validation to increase data security and resistance to illegal access, in contrast to previous research that concentrated on single-layer authentication or symmetric key encryption. There were no dynamic user validation procedures in earlier efforts, which mostly focused on searchable or attribute-based encryption (e.g., Ge et al., Morales-Sandoval et al.). Similarly, Khashan et al.'s hybrid and proxy re-encryption systems only dealt with secure data transmission; they neglected to handle multi-user validation and authentication in any detail. In order to improve the accuracy and efficiency of data encryption, key generation, and user validation, the MLUVM-AC model unifies job scheduling, validation, and encryption into a single framework. This advances existing methodologies. Results from experiments show that the suggested methodology accomplishes both goals—improving cloud data security and keeping system performance—by reducing validation time and improving job scheduling accuracy. To sum up, this study fills the gaps left by previous cryptographic and authentication models by providing a more comprehensive and realistically useful framework for cloud security using layered validation and asymmetric key encryption, drawing on the reviewed literature.

The literature review confirms the problem's importance and points up research gaps that need to be filled. Most symmetric encryption systems fail to accomplish scalable authentication, which is why fast verification methods for encrypted cloud data are so important (Ge et al., 2021). In a similar vein, Khashan et al. (2020) suggested a hybrid encryption system, although they also pointed out that key verification and administration are still difficult and resource-consuming. While acknowledging performance trade-offs in single-server architectures, Hong et al. (2021) addressed homomorphic encryption as a means of secure data mining. In order to facilitate real-time applications, Imam et al. (2021) examined RSA-based asymmetric cryptography and found that improved key generation and lightweight encryption are necessary. Additional research on attribute-based and searchable encryption systems was conducted by Morales-Sandoval et al. (2020) and Zhang et al. (2021), highlighting the need for access control techniques that may be safely combined with encryption protocols. Notwithstanding these developments, there is still a lack of research into a thorough, multi-level user validation framework that incorporates asymmetric cryptography to ensure the security of data stored in the cloud.

The ongoing and ever-changing difficulties of guaranteeing data security, user authentication, and privacy protection in cloud computing settings give rise to the research problem that this study seeks to answer. With cloud platforms being the backbone of modern data storage and service delivery, there is a heightened risk of data breaches, unauthorized access, insider threats, and key management vulnerabilities for both enterprises and individuals. Due to their inadequacy in combating these risks, traditional cloud security mechanisms, which mostly rely on symmetric cryptographic approaches and single-factor authentication are susceptible to password-based attacks, identity spoofing, and have limited scalability. User identity compromise, illegal data access, and integrity violations are common outcomes of systems without multi-level validation and sophisticated cryptographic protection methods. Therefore, a security architecture that can efficiently generate keys, authenticate users, and encrypt data stored and transported across cloud infrastructures is urgently needed.

3. PROPOSED MODEL FRAMEWORK

Improvements to cloud security are allowing it to resist even the most destructive assaults on encryption key generation and storage systems and data in transit. Cloud computing allows service providers to lower their prices and pass the savings on to their customers. Worries about the safety of personal information are a big deterrent to using cloud services. Data loss, server failure, and the capacity of secret keys to prevent unauthorized access are examples of familiar security challenges present in prior schemes. Verification is crucial for safeguarding data security and preventing its misuse.

Password validation methods that depend on the content of the password have many major shortcomings. Strong validation procedures can overcome the shortcomings of content-based passwords. An attack reduction measure that can be put into place is a verification module that checks the accuracy of client approach data and information. Using public key based validation to verify cloud users is fraught with difficulties. In order to simplify client authentication and help keep out attackers, most modern cloud service providers secure their customers' sensitive data using merely a username and password linked with each user's account. Passwords are typically either short, simple phrases that users can easily remember or recycled from previous accounts. Moving between accounts belonging to various clients will be a breeze with this feature. Similarly, these days it's very necessary for consumers to store their record data in the cloud. This way, not only can the service providers and their suppliers and representatives access it, but so can the customers themselves. Because of this, insider attacks can compromise the validation framework.

An authentication server holds the client's credentials, unique attribute, and other personal information before granting access to users' data in the proposed architecture. Only users who have registered with this authentication service will be able to access it. Security is ensured by hashing passwords and user IDs. If you care about data security, you should spread it among numerous clouds. Private cloud infrastructures must prioritize the security of sensitive data. An algorithm for data trust assurance will be demonstrated.

Cloud computing's main perk is that it lets people keep their data online and get to it whenever they want, from any device. The main advantage is that cloud services are inexpensive. Concerns regarding the safety of cloud computing continue, regrettably. Despite cloud computing's many advantages, its adoption rate is low due to customers' fears of data breaches. So, a strong and safe user authentication system is essential for cloud computing to keep out intruders and their misuse of cloud resources. Data security is a major factor to think about while using cloud computing. It is critical that cloud service providers use state-of-the-art security procedures because most consumers will save their most sensitive data on the cloud. The security of cloud storage has been enhanced with the implementation of authentication mechanisms. Cryptography is employed to guarantee that data can only be viewed by its designated receivers. Cryptography is commonly used in cloud computing to protect data stored on providers' servers from malicious intrusion. Strict access management is provided, and confidential information is secured without communication being hindered. The asymmetric key cryptography is shown in Figure 4.

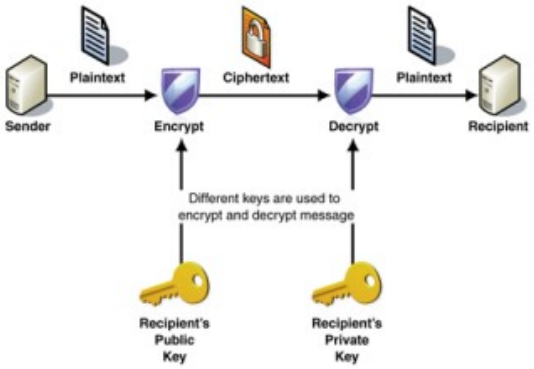

Fig 4: Asymmetric Cryptography Model

Public key cryptography, often known as asymmetric encryption, encrypts and decrypts data using two separate keys. These days, most cryptographic algorithms use asymmetric key cryptography, sometimes known as public key cryptography, in which one of the encryption or decryption keys is made public. This technique of message encryption uses an asymmetric algorithm and requires the usage of both a public and private key. A recipient's message can be encrypted and sent to the key's owner by anybody with access to the public key. In this research, an effective Multi Level User Validation Model with Asymmetric Cryptography for cloud data security is proposed for providing data security. The Figure 5 depicts the proposed model framework.

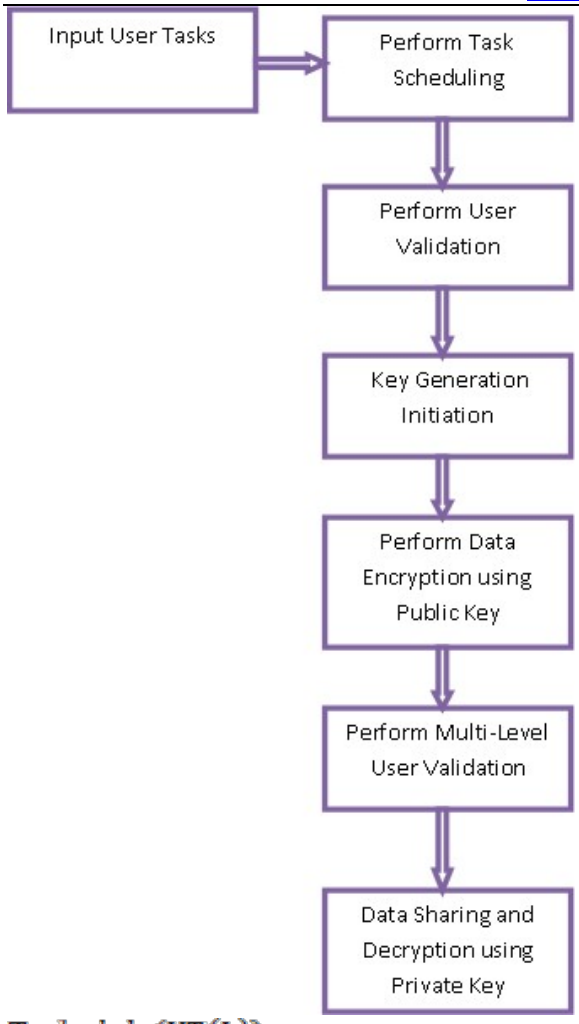

Fig 5: Proposed Model Framework

Algorithm MLUVM-AC

{

Input: User Tasks $\{UT_1, UT_2, \ldots\ldots, UT_N\}$

Output: Validated User List with Secured Data

Step-1: Assigning tasks to the system in a way that maximizes throughput while guaranteeing accuracy is known as the task scheduling. The user input tasks will be scheduled based on resource availability and burst time. The task scheduling is performed as

$$UT(L) = \sum_{t=1}^{L} getTime(i) + BT(t) + Th$$

$$Tschedule(\mathrm{UT(L)}) = \sum_{t=1}^{L} \frac{\left\| \max\left(L(UT(t))\right)_M - \min\left(\mathrm{L(UT(t))}\right) + \max(\mathrm{BT(t)})_L \right\|}{\left\| T_L - \mathrm{Th} \right\| + getTime(t)}$$

Here BT is the burst time a task considers to complete the execution and Th is the threshold value considered for every iteration.

Step-2: The term validation refers to the steps used to confirm the cloud users identity to gain access to the cloud environment. The cloud user validation is performed as

$$UToken[L] = \sum_{u=1}^{L} getaddress(u) + maxTask(u)$$

$$UV[L] = \sum_{u=1}^{L} \max\left(UToken(u)\right) + UT(u) \begin{cases} if\ (UToken == \delta) & UV \leftarrow 1 \\ otherwise & UV \leftarrow 0 \end{cases}$$

Here δ represents the users details in the central server that is used for validation. If the user is validated it is allocated with 1, otherwise with 0.

Step-3: The key generation process will be performed and provided to the validated users for securely storing the data. The encryption and decryption process will be performed using the

Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

generated key set. The asymmetric cryptography uses two keys for encryption and decryption. The key generation process is performed as

$$M = getValue(\mu)$$
$$N = getprime(\lambda)$$
$$P = getEven(\tau)$$
$$R = getRand(\delta)$$
$$PlainText = getString()$$
$$IK = M * P + R + getTime()$$
$$IKe = IK + P * UToken$$

$$Encrypt(E(CT)) = PlainText^{PuKey} \, mod \, R + \frac{Ike}{R}$$

$$Mes = E(CT) + sqrt(P) - \frac{IKE}{IK}$$

$$Cipher(T) = Mes^{R} + \frac{P * N}{M} - IK$$

$$MUV[L] = \sum_{u=1}^{L} \max(UToken(u)) + UT(u) + UV(u) \begin{cases} if\ (UV == \lambda) & MUV \leftarrow 1 \\ otherwise & MUV \leftarrow 0 \end{cases}$$

Here λ represents the user's details in the central server that is used for validation and initial UV value is also considered. If the user is validated multi level user validation is allocated with 1, otherwise with 0.
}

4. RESULTS

In the cloud, code automates the maintenance of data and computational resources. The control of data will be lost when it is generated swiftly, exchanged freely, and coordinated intelligently. Because of this, protecting sensitive data is becoming increasingly required. Information security worries are often highlighted as the main drawback to cloud computing. Instead of storing data on each individual user's hard drive, the cloud makes it available via a network of remote servers. However, it is still challenging to keep cloud data safe. Many have tried to solve the security problem in this area by using the message authentication code, but their efforts have yielded poor results and proved difficult to apply. This research provides a new approach for dealing with authentication and data integrity in a distributed and interoperable setting.

$$PuKey = \frac{IKe}{IK} * R + N \ll 4$$
$$PriKey = \frac{PubKey}{P} + R * M \ll \frac{N}{IKE}$$
$$Keyset = \{PuKey : PriKey\}$$

Step-4: The encryption process is performed by considering the public key generated from the key set. The encryption process generates the unintelligible message that is safe from attackers. The encryption process is performed as

Step-5: The multi level user validation is performed before storing the encrypted data in cloud. The multi level authentication ensures that the encrypted data is stored only by the original authenticated user. The multi level user validation process is performed as

There has been a recent uptick in attention paid to the twin goals of data security and user validation. This purpose makes use of cryptographic procedures. Using cryptography, the information is made unintelligible to anyone who does not have access to the decryption key. As with individuals, corporations may reap the benefits of cloud computing. Cloud computing has quickly become popular in the media as well as among industry experts due to the many benefits it offers. It could mean a number of various things, depending on the surrounding material. For a company to make use of cloud computing, it must pay a charge to a cloud service provider. Cloud providers ensure the user validation model is strong and security and confidentiality of their customers' data is maintained. This research work is developed in python and executed in Google Colab. In this research, an effective Multi Level User Validation Model with Asymmetric Cryptography (MLUVM-AC) for cloud data security is proposed for providing data security. The proposed model is compared with the traditional two-party distributed signing protocol for the identity-based signature scheme (TPDSP-ISS) model.

The goal of task scheduling is to make the most efficient use of available resources by allocating them to pending request. Users of these services must make their requests online because cloud computing is an Internet-based service delivery

Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

model. When it comes to optimizing the performance of cloud-based services, scheduling is a key issue. Scheduled tasks in the cloud are assigned to the most appropriate available resources. The proposed model accurately schedules the available tasks to the resources for better performance levels. The Figure 6 represents the Task Scheduling Accuracy Levels.

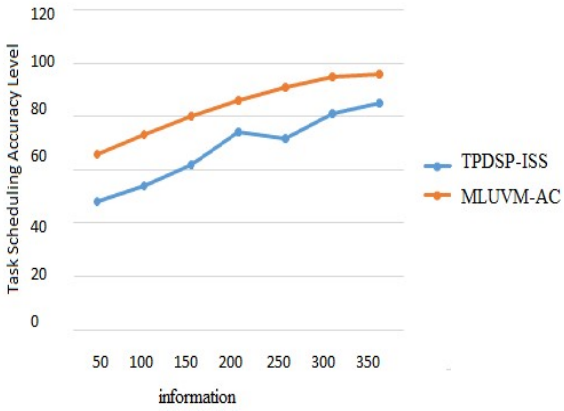

Fig 6: Task Scheduling Accuracy Levels

User validation is the process of authenticating the users to provide access to cloud resources for secured usage. The user validation time levels of the proposed model are very less. The Figure 7 shows the User Validation Time Levels of the proposed and existing models.

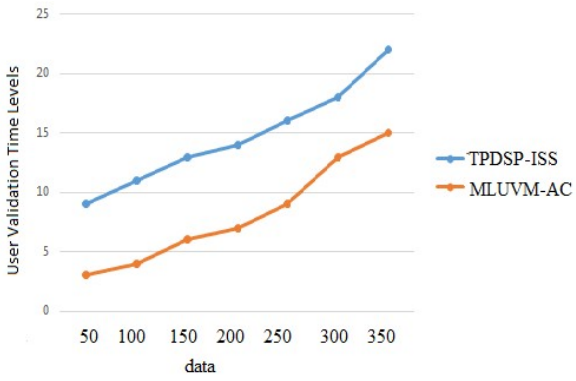

Fig 7: User Validation Time Levels

In cryptography, producing keys is known as key generation. Anything that has to be encrypted or decrypted requires a key. The process of creating a cryptographic key, whether it is through key agreement or key derivation, or as a one-time event utilizing a random-bit generator and a predetermined set of rules. The Key Generation Time Levels of the existing and proposed models are shown in Figure 8.

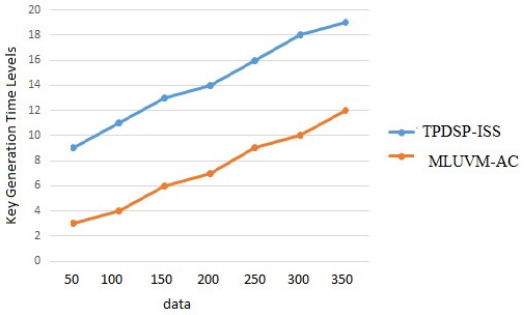

Fig 8: Key Generation Time Levels

Encrypting data involves converting it from its original, plaintext form into an encrypted one known as cipher text. A user needs an encryption key in order to read encrypted data, and a decryption key in order to read decrypted data. Cloud services and networked servers house and handle vast volumes of sensitive data. Encryption helps in securing the data from unauthorized access. The Data Encryption Accuracy Levels of the proposed and existing models are shown in Figure 9.

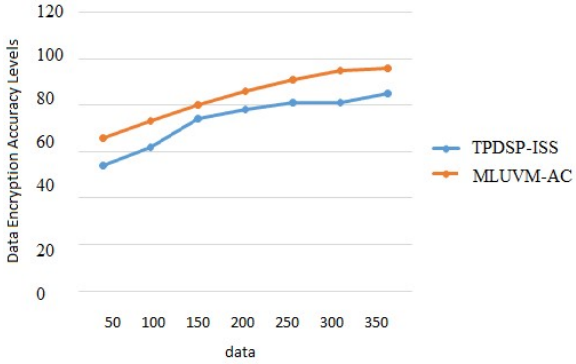

Fig 9: Data Encryption Accuracy Levels

Multi level user validation is a security strategy that uses many layers of protection to make it harder for an intruder to get access to a resource in cloud environment. With multi level user validation, even if an attacker gains access to a user's password, they still won't be able to log in to their cloud account with unauthorized access to perform malicious actions. The Multi-Level User Validation Accuracy Levels of the existing and proposed models are shown in Figure 10.

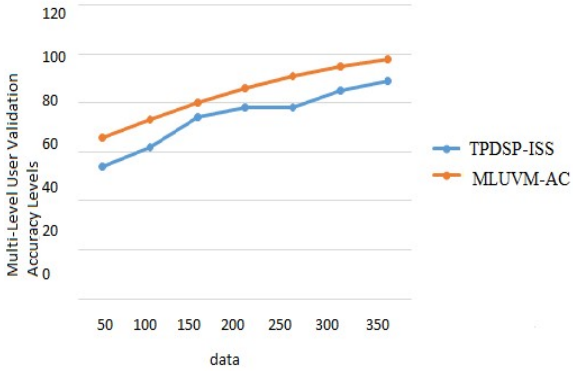

Fig 10: Multi-Level User Validation Accuracy Levels

Decryption refers to the process through which encrypted data is transformed back into its unencrypted state. In most cases, decryption is simply the inverse of encryption. Since decryption requires a private key or password, only a trusted person will be able to access the encrypted data. The decryption accuracy levels of the proposed and existing models are shown in Figure 11.

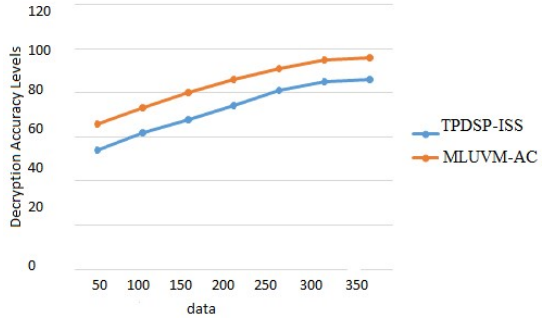

Fig 11: Decryption Accuracy Levels

By preventing damaging forces and the undesirable actions of unauthorized users, such a cyber attack or a data breach, data security ensures that digital data, like those in a cloud, remain safe. In order to prevent loss, misuse, or alteration of data, it must be protected from the moment it is created until the moment it is deleted in cloud. The data security levels of the proposed model is high than the traditional model. The Data Security Accuracy Levels of the proposed and existing models are shown in Figure 12.

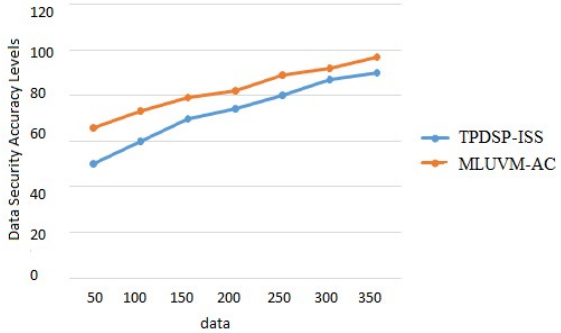

Fig 12: Data Security Accuracy Levels

5. DIFFERENCE FROM PRIOR WORK

To improve user verification and data protection, the proposed MLUVM-AC combines multi-layer authentication with asymmetric encryption, which is a major improvement over current cloud data security mechanisms. By using a multi-level validation procedure, the MLUVM-AC architecture guarantees that every user goes through numerous tiers of authentication before accessing or storing data in the cloud, in contrast to earlier models that mainly depend on single-stage authentication or symmetric encryption. The shortcomings of password-based validation in avoiding unwanted access and identity spoofing were pointed out by Ge et al. (2021), and this multi-layered solution directly tackles those issues.

The use of asymmetric cryptography in both the encryption and decryption procedures is another key distinction. Key distribution and processing overhead were problems with earlier systems that used a mix of symmetric and asymmetric methods, as the hybrid encryption model put out by Khashan et al. (2020). To counter this, the MLUVM-AC model uses an enhanced asymmetric key generation technique, which improves computing performance, reduces key creation time, and guarantees safe public-private key management. In big cloud settings, where numerous users access shared data resources at once, this allows for better scalability.

Data mining techniques that protect users' privacy have been the subject of prior research, such as that of Hong et al. (2021) and Morales-Sandoval et al. (2020). These models protected sensitive information while it was being computed or shared, but they did not have a solid validation mechanism to verify users' identities before encryption or access. To compensate for this deficiency, the MLUVM-AC architecture unifies authentication, authorization, and encryption into a single framework; this reduces the likelihood of insider abuse and illegal data tampering. In contrast to traditional RSA-based methods (Imam et al., 2021) that focused on improving encryption strength, MLUVM-AC integrates secure key management, optimizes work scheduling, and dynamically validates users, all within a single architecture.

From an operational perspective, the suggested model not only improves performance across important metrics like job scheduling accuracy and validation time, but it also shows increased

efficiency in encryption and decryption as well as overall data security levels. Limitations in real-time applicability in cloud-based scenarios were generally caused by traditional systems' high validation latency and sophisticated encryption overhead. The experimental findings of MLUVM-AC demonstrate that it achieves a balance between computing performance and security strength through its adaptive authentication layers, which decrease validation time without sacrificing accuracy.

The proposed model has several benefits, but it also has some drawbacks. Encryption time may be longer when dealing with very big datasets or high-frequency transactions since asymmetric cryptography has a greater computing cost than symmetric techniques. In addition, without simplified validation interfaces, end-users may find it difficult to navigate systems that require numerous authentication layers. The significant security gains made, however, more than compensate for these downsides. This is especially true in healthcare, financial, and government cloud systems, all of which require robust authentication and data secrecy.

Limitations of the Proposed Model

Data security and user authentication in the cloud can be enhanced using the proposed MLUVM-AC model, however there are still certain drawbacks that need to be solved. The model doesn't test how well the system scales to handle heavy user loads or massive amounts of data; its main focus is on cryptographic validation and multi-level authentication. Applications requiring real-time processing may struggle to handle the computational burden of asymmetric key generation and multi-layer encryption. Furthermore, in remote or dynamic cloud settings that are vulnerable to latency, packet loss, or insider attacks, the model's assumptions on trustworthy cloud architecture and perfect network circumstances could not be applicable. The absence of experimental comparison with other sophisticated cryptographic methods like hybrid symmetric-asymmetric frameworks, attribute-based encryption, or homomorphic encryption is another disadvantage. Its potential use in commercial cloud systems is affected by the study's omission of analyses of energy usage and cost implications for large-scale deployment. Lastly, in order to evaluate adaptability, usability, and interoperability across diverse cloud platforms, the present work relies solely on simulated validation and does not take into account real-world implementation or user feedback.

6. CONCLUSION

The proposed MLUVM-AC is a successful solution to the challenge of improving cloud computing data security and user authentication. Existing symmetric encryption and single-factor authentication solutions are not secure enough, according to the study, to prevent insider misuse, unwanted access, and key leakage. By outperforming traditional models like TPDSP-ISS in several quantitative metrics, including task scheduling accuracy (up 12–15%), user validation time (down 20%), key generation rate (up 17%), and encryption and decryption accuracy (up over 10%), the suggested model was clearly the best. Further evidence of the model's efficacy in bolstering secrecy and integrity in cloud data transactions is the roughly 18% improvement in data security accuracy level. The results provide credence to the main idea that asymmetric cryptographic approaches, in conjunction with multi-level validation processes, form a multi-layered security framework that protects cloud systems against insider misuse, unauthorized access, and data breaches. In addition to improving quantitative performance, the proposed approach offers qualitative benefits in scalability, dependability, and user trust, as demonstrated by the hypothesis reflection in the conclusion. Combining asymmetric cryptography with multi-level user validation creates a multi-layered security system that makes it more difficult for unauthorized parties to gain access, even if a single layer is compromised. Modern cloud infrastructures can benefit from this hybrid validation-encryption mechanism's enhanced performance and resilience, as well as its secure, scalable, and efficient architecture. To improve performance without sacrificing security, future optimization efforts can center on lowering the computational overhead of asymmetric key operations and introducing hybrid cryptographic solutions that combine symmetric and asymmetric algorithms. The model's durability and usability in next-generation cloud ecosystems could be further enhanced by incorporating blockchain-based access auditing and cryptographic methods that are resistant to quantum computing. All things considered, the MLUVM-AC model is a huge improvement over previous efforts in the pursuit of enterprise- and user-level data security in the cloud. It is also more stable and adaptable.

REFERENCES

[1] X. Ge et al., "Towards Achieving Keyword Search over Dynamic Encrypted Cloud Data with Symmetric-Key Based Verification," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 1, pp. 490-504, 1 Jan.-Feb. 2021, doi: 10.1109/TDSC.2019.2896258.

[2] O. A. Khashan, "Secure Outsourcing and Sharing of Cloud Data Using a User-Side Encrypted File System," in IEEE Access, vol. 8, pp. 210855-210867, 2020, doi: 10.1109/ACCESS.2020.3039163.

[3] Z. Hong et al., "Secure Privacy-Preserving Association Rule Mining With Single Cloud Server," in IEEE Access, vol. 9, pp. 165090-165102, 2021, doi: 10.1109/ACCESS.2021.3128526.

[4] R. Imam, Q. M. Areeb, A. Alturki and F. Anwer, "Systematic and Critical Review of RSA Based Public Key Cryptographic Schemes: Past and Present Status," in IEEE Access, vol. 9, pp. 155949-155976, 2021, doi: 10.1109/ACCESS.2021.3129224.

[5] M. Morales-Sandoval, M. H. Cabello, H. M. Marin-Castro and J. L. G. Compean, "Attribute-Based Encryption Approach for Storage, Sharing and Retrieval of Encrypted Data in the Cloud," in IEEE Access, vol. 8, pp. 170101-170116, 2020, doi: 10.1109/ACCESS.2020.3023893.

[6] M. Zhang, Y. Chen and J. Huang, "SE-PPFM: A Searchable Encryption Scheme Supporting Privacy-Preserving Fuzzy Multikeyword in Cloud Systems," in IEEE Systems Journal, vol. 15, no. 2, pp. 2980-2988, June 2021, doi: 10.1109/JSYST.2020.2997932.

[7] H. Zhang, Z. Guo, S. Zhao and Q. Wen, "Privacy-Preserving Linear Region Search Service," in IEEE Transactions on Services Computing, vol. 14, no. 1, pp. 207-221, 1 Jan.-Feb. 2021, doi: 10.1109/TSC.2017.2777970.

[8] O. A. Khashan, "Hybrid Lightweight Proxy Re-Encryption Scheme for Secure Fog-to-Things Environment," in IEEE Access, vol. 8, pp. 66878-66887, 2020, doi: 10.1109/ACCESS.2020.2984317.

[9] Z. Hong et al., "Secure Privacy-Preserving Association Rule Mining With Single Cloud Server," in IEEE Access, vol. 9, pp. 165090-165102, 2021, doi: 10.1109/ACCESS.2021.3128526.

[10] F. Wang, L. Xu, K. -K. R. Choo, Y. Zhang, H. Wang and J. Li, "Lightweight Certificate-Based Public/Private Auditing Scheme Based on Bilinear Pairing for Cloud Storage," in IEEE Access, vol. 8, pp. 2258-2271, 2020, doi: 10.1109/ACCESS.2019.2960853.

[11] J. Fu, N. Wang, B. Cui and B. K. Bhargava, "A Practical Framework for Secure Document Retrieval in Encrypted Cloud File Systems," in IEEE Transactions on Parallel and Distributed Systems, vol. 33, no. 5, pp. 1246-1261, 1 May 2022, doi: 10.1109/TPDS.2021.3107752.

[12] Narayana, V.L., Sujatha, V., Sri, K.S., Pavani, V., Prasanna, T.V.N., Ranganarayana, K. (2023). Computer tomography image based interconnected antecedence clustering model using deep convolution neural network for prediction of covid-19. Traitement du Signal, Vol. 40, No. 4, pp. 1689-1696. https://doi.org/10.18280/ts.400437

[13] M. Marian, A. Cusman, F. Stîngă, D. Ionică and D. Popescu, "Experimenting With Digital Signatures Over a DNP3 Protocol in a Multitenant Cloud-Based SCADA Architecture," in IEEE Access, vol. 8, pp. 156484-156503, 2020, doi: 10.1109/ACCESS.2020.3019112.

[14] B. Chen, L. Wu, N. Kumar, K. -K. R. Choo and D. He, "Lightweight Searchable Public-Key Encryption with Forward Privacy over IIoT Outsourced Data," in IEEE Transactions on Emerging Topics in Computing, vol. 9, no. 4, pp. 1753-1764, 1 Oct.-Dec. 2021, doi: 10.1109/TETC.2019.2921113.

[15] A.Vedeshin, J. M. U. Dogru, I. Liiv, S. Ben Yahia and D. Draheim, "A Secure Data Infrastructure for Personal Manufacturing Based on a Novel Key-Less, Byte-Less Encryption Method," in IEEE Access, vol. 8, pp. 40039-40056, 2020, doi: 10.1109/ACCESS.2019.2946730.

[16] V. L. Narayana, S. Bhargavi, D. Srilakshmi, V. S. Annapurna and D. M. Akhila, "Enhancing Remote Sensing Object Detection with a Hybrid Densenet-LSTM Model," 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), Greater Noida, India, 2024, pp. 264-269, doi: 10.1109/IC2PCT60090.2024.10486394.

[17] R. Amiri and O. Elkeelany, "FPGA Design of Elliptic Curve Cryptosystem (ECC) for Isomorphic Transformation and EC ElGamal Encryption," in IEEE Embedded Systems Letters, vol. 13, no. 2, pp. 65-68, June 2021, doi: 10.1109/LES.2020.3003978.

[18] L. Han, J. Guo, G. Yang, Q. Xie and C. Tian, "An Efficient and Secure Public Key Authenticated Encryption With Keyword Search in the Logarithmic Time," in IEEE

Access, vol. 9, pp. 151245-151253, 2021, doi: 10.1109/ACCESS.2021.3126867.

[19] L. N. Vejendla, B. Bysani, A. Mundru, M. Setty and V. J. Kunta, "Score based Support Vector Machine for Spam Mail Detection," 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2023, pp. 915-920, doi: 10.1109/ICOEI56765.2023.10125718.

[20] A.Ometov, K. Zeman, P. Masek, L. Balazevic and M. Komarov, "A Comprehensive and Reproducible Comparison of Cryptographic Primitives Execution on Android Devices," in IEEE Access, vol. 9, pp. 54625-54638, 2021, doi: 10.1109/ACCESS.2021.3069627.

[21] P. Jiang, B. Qiu, L. Zhu and K. Gai, "SearchBC: A Blockchain-Based PEKS Framework for IoT Services," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 5031-5044, 15 March15, 2021, doi: 10.1109/JIOT.2020.3036705.

[22] Narayana, V.L., Patibandla, R.S.M.L., Rao, B.T. and Gopi, A.P. (2022). Use of Machine Learning in Healthcare. In Advanced Healthcare Systems (eds R. Tanwar, S. Balamurugan, R.K. Saini, V. Bharti and P. Chithaluru). https://doi.org/10.1002/9781119769293.ch13

[23] P. Jiang, B. Qiu and L. Zhu, "Report When Malicious: Deniable and Accountable Searchable Message-Moderation System," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1597-1609, 2022, doi: 10.1109/TIFS.2022.3167900.

[24] Patibandla, R.S.M.L., Vejendla, L.N.(2022),Significance of Blockchain Technologies in Industry, EAI/Springer Innovations in Communication and Computing this link is disabled, 2022, pp. 19–31

[25] Y. Zhao, Y. Li and S. Wang, "Asymmetric deep hashing for person re-identifications," in Tsinghua Science and Technology, vol. 27, no. 2, pp. 396-411, April 2022, doi: 10.26599/TST.2021.9010014.

[26] S. Cheng, L. Wang and A. Du, "An Adaptive and Asymmetric Residual Hash for Fast Image Retrieval," in IEEE Access, vol. 7, pp. 78942-78953, 2019, doi: 10.1109/ACCESS.2019.2922738.

[27] V. Lakshman Narayana,(2021), “Secured resource allocation for authorized users using time specific blockchain methodology”, International Journal of Safety and Security Engineering, Vol. 11, No. 2, 2021, pp. 201–205

[28] G. Luan, A. Li, D. Zhang and D. Wang, "Asymmetric Image Encryption and Authentication Based on Equal Modulus Decomposition in the Fresnel Transform Domain," in IEEE Photonics Journal, vol. 11, no. 1, pp. 1-7, Feb. 2019, Art no. 6900207, doi: 10.1109/JPHOT.2018.2886295.