Cryptography in Cloud Computing Data Security

Lasal Sandeepa Hettiarachchi
Department of Computer Science and Software Engineering
Sri Lanka Institute of Information Technology
Sri Lanka
it19132310@my.sliit.lk

Senura Vihan Jayadeva
Department of Computer Science and Software Engineering
Sri Lanka Institute of Information Technology
Sri Lanka
it19139036@my.sliit.lk

Rusiru Abhisheak Vikum Bandara
Department of Computer Science and Software Engineering
Sri Lanka Institute of Information Technology
Sri Lanka
it19104218@my.sliit.lk

Dilmi Palliyaguruge
Department of Computer Science and Software Engineering
Sri Lanka Institute of Information Technology
Sri Lanka
it19120980@my.sliit.lk

***Abstract*— The cloud computing infrastructure supports the use of adaptable, ever-expanding capabilities and creating potential without investing in additional hardware, software, or staff. Moreover, cloud computing was first conceived as a business strategy and then expanded into a successful information technology. Providing an ecosystem that prioritizes cloud data and application security is crucial. For this reason, networks must be protocols that employ robust algorithms. To secure the security of data in the cloud, the focus of this work will be on evaluating and understanding cloud security challenges, and then presenting cryptographic algorithms and effective approaches to address these issues. In addition, we'll highlight certain privacy concerns of the present cloud computing environment to provide some additional context for some cryptographic security concerns.**

Keywords—Cloud Computing, Cryptography, AES, DES, Blowfish algorith, Load prediction, Machine Learning, Containerization

I. INTRODUCTION

Audience may learn a lot about it through the language and ideas that surround it. Somehow, the true meaning of cloud computing has gotten lost in all the writing about it. The phrase "cloud computing," however, has its roots in network topology, where several organizations fulfill their service requirements. In this context, "cloud computing" means using the Internet to run useful programs or services. There was no sudden explosion of "the cloud," as the concept can be traced back to the early days of computing systems with remotely time-shared computing resources and practical applications. The wide range of cloud-sourced applications and services has been the source of some worry. The tools and software utilized to provide these services often don't do anything particularly remarkable. The cloud is utilized by a diverse variety of commercial organizations. Companies using cloud computing services in 2010 resulted in the following. The Microsoft® SharePoint® online service is a cloud-based platform for storing and sharing documents, websites, and other files; it also provides access to a variety of business intelligence and enterprise resource planning applications. Google's cloud storage offers a plethora of options for enterprises and other large I.T. service providers [2]. Additionally, Salesforce.com built its own cloud services [3] for their clientele. In the most recent years, Vmforce and a number of other premium cloud services have arisen as a subsequent development [4]. Who is in charge of ensuring the security and confidentiality of cloud platforms? In the sections that will follow, an attempt will be made to define many aspects of cloud computing, including its deployment models, features, installation procedures, benefits, and encryption features. Cloud Computing Features

The most crucial aspects of cloud computing are as follows:

1. Cloud computing's virtualized software architecture, networking capabilities, and (perhaps) shared physical services are all examples of its distributed infrastructure. Also, data storage is another viable use case for cloud computing. Irrespective of the delivery model, the cloud infrastructure always scales the amount of exposed infrastructure in proportion to the known user population.
2. Second, with dynamic provisioning, software can be set up to automatically approve services based on real need. Services can be elaborated and condensed as needed. To meet these needs for dynamic scalability, while still ensuring high levels of safety and dependability, is a primary goal.
3. Thirdly, you'll need network access to take advantage of the standard-based API representatives set up on HTTP, which will allow you to provide service to a wide variety of devices. Cloud service deployments range from commonplace business software to cutting-edge mobile utilities.
4. Finally, "managed meter" which refers to a specific type of meter that is employed in the cloud computing environment. Its key goals are service optimization, regulatory oversight, and data collection for billing and reporting purposes. With cloud computing, users may have access to a plethora of shared and scalable services at any time and from practically

anywhere. Costs in this case would be based on how long a customer actually used the service.

A. *Service Model*

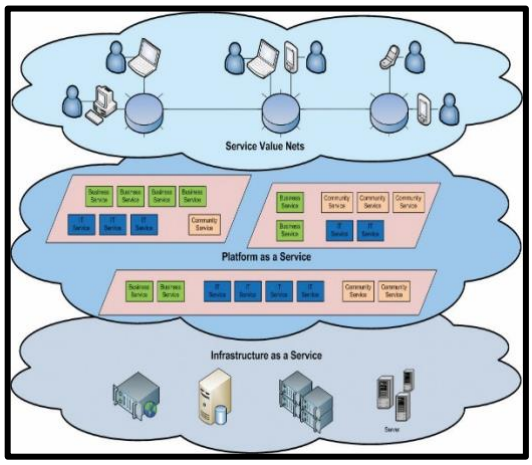

Fig.2. Service model

As can be seen in Fig. 2, cloud computing's original deployment was in very demanding corporate settings. The following are some typical examples of services:

Customers pay for the right to use a cloud-based service or program and get access to it via a subscription model known as "Software as a Service" [5]. Microsoft's efforts in this arena are expanding. Office volume license clients and Office Web App subscribers can use Microsoft's cloud-based web services to gain access to the Office Web Apps as a component of the cloud computing alternative for Microsoft Office 2010.

Platform as a Service (PaaS): Users pay for the use of pre-built infrastructure to bring their own applications and programs online [6]. Users have little control over the underlying operating system or the availability of the underlying network, and the deployment options available to them in terms of apps may be limited.

With Infrastructure as a Service (IaaS), customers are responsible for managing and monitoring their own cloud's operations, applications, storage, and network connectivity [7], rather than just the cloud itself. In addition, different categories of cloud models within a certain market or industry are identified.

One classification method for separating hosted IP telephony services is to use the term "communications as a service" (CaaS). Because to CaaS, there has been a proliferation of Session Initiation Protocol (SIP) trunks and an increase in IP-based communication. Installing Internet Protocol (IP) and Session Initiation Protocol (SIP) paves the way for PBX systems to be moved onto the cloud [9]. CaaS fits inside the umbrella of SaaS deployment models.

B. *Configuration Types for Deploying in the Cloud*

It is important to define the challenges associated with cloud computing's requirements, as well as the four deployment strategies that can be used to overcome them.

As the first step, a private cloud is set up, monitored, and used exclusively in a limited region. On the other hand, it will take place internationally via the internet. A private branch, nevertheless.

When it comes to cloud computing, the two main types are public and private. The consumer is able to build and deploy a service on the cloud with relatively minimal financial input when using public cloud computing in comparison to the capital that is generally needed by other cloud computing services.

Third, the hybrid cloud is based on the fact that all cloud infrastructures consist of several smaller clouds. Only in the clouds may one obtain knowledge, or at least the pieces of knowledge necessary to go between clouds. In order to meet the needs of storing data and providing services in the cloud, businesses might combine private and public clouds.

The fourth type of cloud is called the "Community Cloud," and it's used for large-scale infrastructure as when multiple government agencies share data by uploading it to a single cloud or when a university's server links together its cloud computing community.

Figure 3 also demonstrates that 35% of IT users avoid using cloud servers due to safety concerns. These customers should be aware that certain cloud providers don't bother with security at all. The expensive cost of servers based on hardware, software, and the skill necessary to install all of these components has led to a steady rise in the number of individuals using private clouds over the past several years. Only around one-seventh of all cloud servers are hosted in a public cloud. Public cloud servers are made available for free by several of the leading cloud service providers, including Google, Yahoo, and Microsoft. Hybrid clouds are gradually becoming one of the most promising contenders for the title of most cutting-edge service in the world because to the comparatively inexpensive expenses involved.

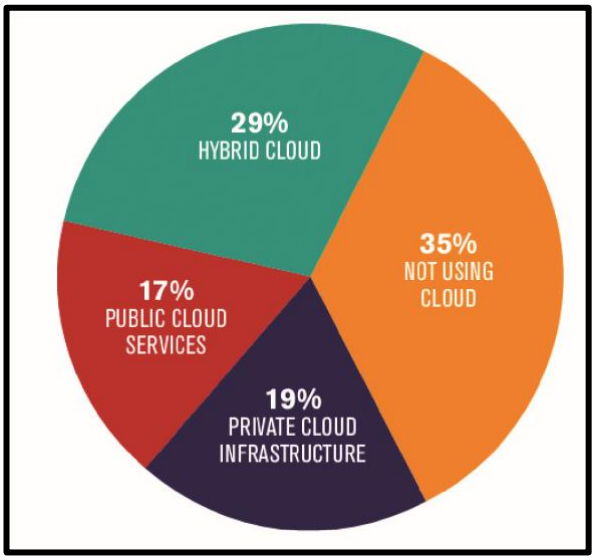

Fig.3. Cloud computing usage

II. RELATED WORK

In this paper the authors explore and cover the basics of cloud computing and cryptography. It involves a comprehensive analysis of existing cryptographic solutions in cloud computing for data security with examples. The authors also highlight the challenges, gaps, and implementations that can be used to enhance and uplift the protection mechanisms with the help of latest additions to the cryptographic world leveraging them to eventually improve the security of data in cloud computing.

C. Cryptography in Cloud Computing

A new service model is made possible by cloud computing, which reallocates resources and makes them available to users as needed. Additionally, it is crucial in Cyber-Physical and Social Computing as well as the next generation of mobile networks and services known as 5G. (CPSC). One of the most crucial cloud services, cloud storage allows users to drastically minimize their storage burden while also providing them with the comfort of easy access to their data.

The effectiveness of cloud computing depends on the safety of its data, thus privacy and trust in the cloud are major concerns that could slow down the evolution of 5G and CPSC. To begin, there is a higher chance of data breach and illegal access when using cloud storage. Second, attacks and breaches against cloud data centers are a growing concern for the safety of cloud-stored information.

Data storage, migration, deletion, update, search, query, and access on the cloud are all examples of data management processes that might not be completely trusted by the data's owners. If possible, those in possession of data should conduct an audit of the reliability of data management. All potential entry points and attack vectors must be identified and neutralized. A major security problem is posed by the aforementioned needs, especially in the realm of big data storage and management. Cloud-based data processing and calculation can expose the protection of data owners or associated companies to unauthorized parties, which is the fourth risk. Authorization of cloud data processing and protection of data processing outcome is another important and intriguing area of study. Security, privacy, and trust in the cloud are rapidly becoming critical issues that can make or break the widespread use of cloud services.

Data security, privacy, and trust in the cloud rely heavily on cryptography's use. But the state-of-the-art options are too cumbersome because of their ineffectiveness and flaws to be implemented in real life. When data is encrypted and stored in the cloud, the risk of privacy leakage is considerably decreased; nevertheless, auditing data management becomes more difficult. Managing keys for the purposes of access restriction and cancellation requires more processing and data transfer time. In addition, the high compute complexity and inefficiency of operations like fusion, aggregation, and mining on encrypted data make their deployment impracticable. Numerous unique solutions are possible with cryptography in cloud computing, but there are also many obstacles that have yet to be overcome.

D. Application of Cryptography in Cloud computing

A rise in the number of privacy-focused businesses is one way in which cryptography can facilitate the widespread adoption of Cloud Computing.

Protecting sensitive data during storage is when cryptography most benefits Cloud computing. The field of study known as cryptography focuses on making unintelligible representations of data for the sake of secure message storage [7]. These days, it's common practice to divide cryptography into three distinct algorithms. Both symmetric and asymmetric key algorithms, as well as hashing techniques, are included here [6]. Data encryption, backup data encryption, network traffic encryption, file storage system encryption, and host security are just a few of the cloud computing security issues that may be alleviated by using encryption alone. The extent to which each of these issues may be resolved varies greatly from case to case. Secure HTTP, encrypted VPNs, Transport Layer Security (TLS), and Secure Shell are just a few examples of encryption technologies that should be used when transporting data between the guest domain and the host domain, as well as between hosts and management systems. If you do this, you may be certain that your information is safe.

We may avoid vulnerabilities like man-in-the-middle attacks, faked assaults, and session hijacking by using encryption. To store and access information and programs, cloud computing makes use of shared server space. While it's easy to see why cloud computing would be beneficial, the fact that cloud operators are expected to change data on clients' behalf without being guaranteed full confidence poses additional security issues. To this end, we will strive to build cryptographic primitives and protocols that are suited to the environment of cloud computing, balancing security, efficiency, and utility. It is more likely that sensitive information will be compromised if it is stored in the cloud and only authorized individuals would have access to it. Owners of data must be wary about putting all of their faith in cloud services. To parties that do not have unlawful access, the processing and computing of data in the cloud could compromise the privacy of users, the data's owners, or associated companies. For these reasons and more, encryption has become more important in cloud computing to protect sensitive information, maintain user anonymity, and build user confidence.

E. Symmetric key Algorithms

The process of encrypting and decrypting data using symmetric algorithms only requires the use of a single key. Users who are accessing the network using symmetrical systems have access to a dual-channel configuration. It's a failsafe for identifying and authorizing users. Algorithms with a symmetric key employ the same key for both sides. Discretion is exercised with regard to the key. One of the benefits of symmetric algorithms is that they are fast and efficient at encrypting data while also requiring little in the way of computational resources. Block ciphers and stream ciphers are the two main categories of symmetric-key algorithms. The input to a bock cipher is a block of plaintext, the size of which is predetermined by the symmetric encryption technique being used. The input block is then encrypted using a key of the same fixed size, and the resulting

output block is also of the same size as the input block. To use a stream cipher, you must encrypt one bit at a time.

The symmetric-key encryption techniques Data Encryption Standard (DES), Triple DES, and Advanced Encryption Standard are all commonly used in cloud computing (AES).

a) Advanced Encryption Standard(AES)

The Advanced Encryption Standard is an example of a popular symmetric-key cryptographic method (AES). The 128-bit block size is standard across all ciphers, with keys ranging from 128 to 256 bits in length. We may rest easy knowing the hash code is safe because of the AES, the Advanced Encryption Standard. AES employs 128-bit blocks for its encryption [3]. The algorithm it employs looks like this: Adding more keys to a keyboard is done in stages, with the first being the addition of round keys. In Rounds, Sub Bytes, each byte is randomly changed with another byte determined by a table. The next phase follows Rounds, Sub Digits. When doing a transposition of rows, each line of the state is rotated by a predetermined amount. Because of this, the rows are switched around. Each column in the state is mixed with the others to create a whole new column, with all four bytes from each column appended together. A round key is used to combine each byte in that state; round keys are produced from the encryption key using a key schedule.

Insert a Round Key into the Keyboard. In 1998, a piece of equipment that cost perhaps in the neighborhood of $250,000 was able to break the DES encryption. As a result of the fact that the DES algorithm was developed for hardware in the middle of the 1970s, it did not create dependable and efficient software code. As a result, triple DES proved to be too sluggish for efficiency purposes. The Triple DES algorithm is obviously more time-consuming than the DES algorithm since it contains of three times as many rounds as DES does.

b) Data Encryption Standard(DES)

Block cipher DES (Data Encryption Standard) encrypts data using a symmetric key. discovered in January 1977 by NIST (National Institute of Standards and Technology). A 64-bit plaintext can be encrypted using the same 56-bit cipher key that decrypts it, and a 64-bit cipher text may be decrypted with the same plaintext. This cipher uses a total of sixteen Fiestel rounds and two permutations (P-boxes), or "beginning permutation" and "final permutation." Each each round of the encryption uses a different 48-bit round key calculated using the original cipher key according to a predetermined algorithm.

c) Blowfish Algorithm

Blowfish is another symmetric block encryption that can be used in place of DES. The fact that it accepts keys of varying lengths—anywhere from 32 bits to 448 bits—makes it a more versatile and powerful tool for both domestic and international applications. Blowfish is a quick, open-source alternative to other encryption algorithms developed by Bruce Schneier in 1993. It has since undergone extensive verification, and its reputation as a robust encryption scheme is growing. Because it is not protected by intellectual property law, Blowfish can be used by anyone for no cost.

F. Asymmetric Key Algorithms

In contrast to symmetric cryptosystems, it is a more recent invention. Encryption and decryption both make use of unique keys. This feature distinguishes the system from symmetric encryption in one important respect. A decryption key, often known as a private key, is something that each recipient has access to. An encryption key, or public key, must be created by the recipient. It is common for this form of cryptosystem to rely on an independent, verifiable authority to issue a public key's "signature," or official declaration of ownership.

a) RSA Cryptosystem

This asymmetric cryptosystem is one of the earliest and most fundamental of its kind. This cryptosystem is still widely used and widely deployed. The RSA cryptosystem gets its name from its creators, cryptography experts Ron Rivest, Adi Shamir, and Len Adleman.

For the avoidance of doubt, this algorithm is only used for public-key cryptography and not private-key cryptography. To this day, it remains the most popular asymmetric algorithm in use. A pair of keys—a public one and a private one—are required. There is no secrecy when using the public key for encryption because it is accessible to the general public. It is only possible to decrypt a message encrypted using a public key by utilizing its corresponding private key. The server employs public-key authentication here by digitally signing a one-of-a-kind message with its private key. Once the signature is completed, it is sent back to the customer. The server's public key is then used for verification.

b) Diffie-Hellman Key Exchange

Using the discrete logarithm issue, Whitfield Diffie and Martin Hellman proposed a key exchange system in 1976. Sender and receiver will use an untrusted channel to exchange keys for their symmetric key scheme. Alice selects a random number aE[1; n] and computes ga, whereas Bob selects a random integer bE[1; n] and computes gb, both of which are sent to Alice to establish a key. The shared secret is a value called gab, which is calculated by Alice using the formula (gb)a and by Bob using the formula (gb)b. Diffie-Hellman Protocol security relies heavily on key ideas like DDH, DHP, DLP, etc.

Given the nature of the concept, both symmetric and asymmetric algorithms have their own advantages involving security in cloud.

G. Hybrid Vigenere Ceacer cipher Encryption

HVVCE is a 3-phase solution that is focused on prevention of attacks is proposed in [16]. As discussed in the paper, security in cloud has 3 components. Prevention,detection and correction. Thus, in this paper a hybrid cryptographic algorithm is applied to maintain data integrity.The proposed

algorithm Caesar cipher is used on the plain text in the initial stage. The encrypted text from the first phase is applied using the Vigenere Cipher and the keyword in the second phase, according to the Vigenere Square value. This HVCCE hybrid encryption process is elaborated in Figure 4.

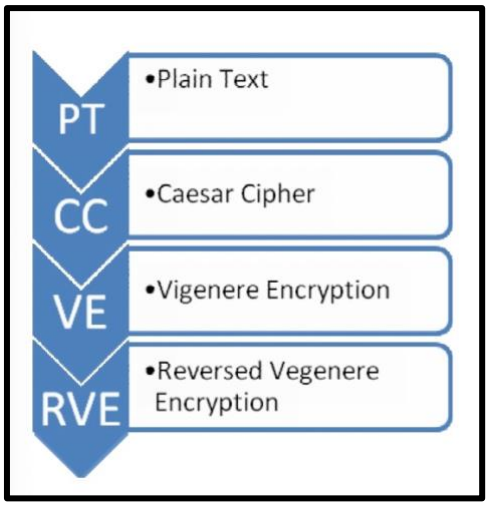

Fig.4. Three-phase encryption in HVCCE

Similarly decryption is also to be carried out in three stages. The reverse Vigenere Cipher must be used in the initial stages of decryption on the encrypted cipher text. The decrypted cipher text obtained from the first phase of decryption needs to be applied to the reverse Vigenere Cipher with the forward keyword in the second phase of decryption. The cipher text obtained in the second step of decryption must be put to the reverse Caesar cipher in the third phase. Figure 2 depicts these three decryption steps.

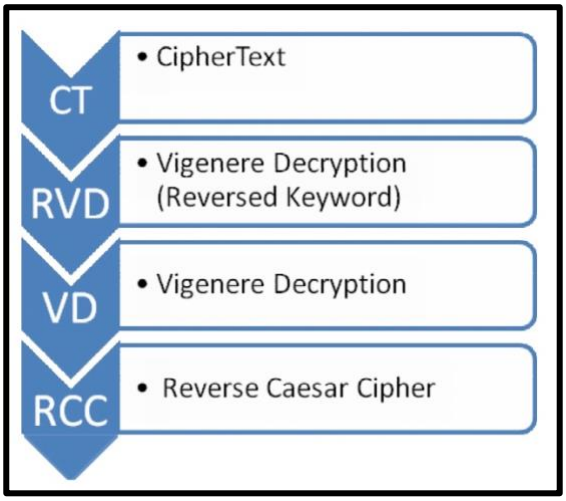

Fig.4. decryption in HVCCE

This hybrid encryption algorithm has been apllied to encrypt plain text which is tedious compared to ciphred text. But, using the proposed algorithm process the computation time can be drastically reduced

III. LITERATURE REVIEW

Numerous crucial cloud security research have analyzed private and trustworthy cryptographic protocols for protecting sensitive information.

A keyword-attribute-based data system that protects users' privacy In their paper titled "Privacy-Preserving Attribute-Keyword Based Data Publish-Subscribe Service on Cloud Platforms," Yang et al. offer the Publish-Subscribe (AKPS) method, which ensures the protection of both users and producers [10]. They were capable of keeping the published data secure by employing Attribute-Based Encryption and outsourcing out the decryption process. Additionally, they developed a new encryption scheme so that customers could pick whatever information they wanted to access.

On the other hand, Sanyal and Iyer [11] looked at cloud security using public key values. They talked about a safe and effective algorithm built on top of the AES (Advanced Encryption Standard) multi-key encryption method, which uses cipher keys with lengths of 128 bits, 192 bits, or 256 bits to encode and decrypt data. The results demonstrated that, in comparison to RSA, AES provides a higher level of security for cloud computing. However, AES is suitable for usage in both public and private clouds and virtual machines.

The careless use of intelligence and distributed power by hypervisors was highlighted as a major issue for secure network virtualization by Mao [12]. Information boxes are explored in the study as a means for hypervisors to exert control. Therefore, he recommended leveraging cutting-edge technology to create a virtual network, which has many practical uses, such as providing a safe environment for multiple cloud tenants to operate together. The use of cryptography has far-reaching effects on administration.

Cloud computing security has been explored by Rauber [13], and without it the whole system would be doomed to fail. In reality, Rauber debated whether cloud computing will transform the computer experience and claimed that the cloud's core components should be protected. Similarly, the researcher looked into how SaaS, homomorphic encryption, and functional encryption all work together to keep data safe. All of these issues were explored at length, and some good outcomes were reached as a result.

Zaheng [14] created an improved security-mobile cloud to address the one-of-a-kind problem of security. When using the public key cryptography that Zaheng defined, a sender does not need the recipient's help to decipher a cipher text that has been saved to the cloud. Keeping private data safe is a major concern when using cloud services.

In contrast, the Share button on Facebook allows users to distribute their information to other social media platforms like Twitter and LinkedIn. Zaheng, however, has noticed that there is still a major vulnerability in using mobile cloud computing servers to access social networks.

Kerchbaun [15] identified numerous insurmountable cloud security challenges, such as infrequent queries, security vs speed query optimization, and access control, and

constructed a high-performance prototype that is suitable for general usage. His work was published in the journal Science.

The importance of algebra in cryptography for the protection of cloud computing was brought to light by Ustimenko and Wroblewska [16], who devised a brilliant proposal for homomorphic encryption and multivariate key cryptography by making use of algebra. [They] emphasized the role that algebra plays in ensuring the security of cloud computing.

To create a homomorphic encryption system, Chakrborty et al. [17] proposed using elliptic curve cryptography. The initial implementation resulted in a data-driven self-control system. The application ensured the correctness of the retrieval strategy, allowing the user to question the safety of the data. Chakrborty et alhighly .'s secure third-party auditor approach relies on the importance of ideas in cryptography. On the client's side, however, the idea was put to use checking and updating encrypted path data. The writers reasoned that a Merkle hash tree would be the best way to store and retrieve data from the server, as it would provide the highest level of security while also being the fastest to access.

While various studies have raised concerns about the expense of elliptic curve encryption for use in PKI, these concerns can be addressed by improving the ECC algorithm [18]. Using RSA, Jangar and Bala built a privacy-aware security algorithm for the cloud, which they found to be effective, secure, and private.

H. Secure Cloud data storage

The problem of using hierarchical key assignment schemes for data access control in the cloud was addressed by Castiglione et al. in their article "Supporting Dynamic Updates in Storage Clouds with the Akl-Taylor Scheme," which made use of the inherent scalability of cloud services to circumvent the problem. By taking into account numerous key allocation techniques and showing that the suggested systems are reliable with regard to the idea of key retrieval, they arrived at new findings on the Akl-Taylor scheme. In their paper titled "Secure Independent-update Concise-expression Access Control for Video on Demand in Cloud," He et al. recommended a SICAC model based on Essential element Encryption inside the cloud as a way to promote adaptive and effective identification and authorisation for VoD operations. The strategy that has been proposed is intended to overcome the challenges that are caused by the regular subscribing and unsubscribing tendencies of a significant amount of cloud customers as well as the abundance of different kinds of movies that are stored in the cloud. Both an independent-update Key Policy ABE (KP-ABE) algorithm that enables users to independently keep updating their keys as well as a concise-expression access structure that requires consumers to convey a variety of logic relationships in a manner that is both flexible and efficient were developed by the authors of the study.

Because the currently available methods for the secure transfer of file formats in both mobile devices and the cloud possess limitations in terms of memory support, computational load, battery power, and data size, these methods are not suitable for use on mobile devices that are limited in their availability of these resources. The authors of the paper "Cryptography-Based Safe Data Storage and Sharing Using HEVC and Public Clouds" (Usman, Jan, and He), in an effort to find a solution to this issue, proposed a method that is not only safe but also compact, energy-efficient, and reliable. The proposed method uses High Performance Video Coding (HEVC) Intra encoded video streams in unsliced mode as a source for data hiding in order to make it possible for resource-constrained mobile devices to handle data in real time.

In their work "Intelligent Cryptography Approach for Secure Distributed Big Data Storage in Cloud Computing," Li et al. proposed an alternative technique for securing storage of cloud-based data. The authors introduced a sophisticated encryption method they called the Security-Aware Efficient Distributed Storage (SA-EDS) model, which makes it so cloud providers can't get their hands on partial data without going through a series of hoops. Data is successfully partitioned and stored separately across several cloud nodes.

I. Cloud data privacy protection

A privacy-preserving Attribute-Keyword based data Publish-Subscribe (AKPS) scheme is proposed by Yang et al. in their work "Privacy-Preserving Attribute-Keyword Based Data Publish-Subscribe Service on Cloud Platforms," which safeguards the interests of both publishers and readers. By using Attribute-Based Encryption and contracting out decryption, they were able to keep the publicized data safe, and also provided a new searchable encryption so that consumers could choose the information they wanted to see. The AKPS is novel and distinct from other approaches since it allows for more than one publisher and more than one subscriber, without the need for any of them to share secret keys. More than that, it prevents users from evading the access/subscription policy verification procedure by cleverly linking the two policies together with the use of two secrets.

Data privacy protection and simultaneous image maintenance present difficulties in the use of outsourcing the very computationally complex Compressive Sensing (CS) reconstruction process to the cloud. In their study "A Compressive Sensing Based Privacy Preserving Outsourcing of Image Storage and Identity Authentication Service in Cloud," Hu et al. developed a unique outsourced image reconstruction and identity authentication approach to overcome this difficulty. It combines signal processing methods from the CS realm with those of compute outsourcing. This ensures that the cloud can recreate images securely without exposing any private information. Additionally, the reconstruction service is delivered by using identity authentication.

In their study "Collaborative Trajectory Privacy Preserving Scheme on Location-based Services," Peng et al. think about how to solve the privacy problem that arises with LBS in the cloud. To conceal a user's true path from an LBS adversary, they developed a Collaborative Trajectory Privacy Preserving (CTPP) approach in which users would submit sham queries. Prior to this, it was suggested using a multihop caching-aware cloaking method to gain access to more relevant data. To protect users' anonymity while they move through space and time, a collaborative privacy preservation

querying technique was designed to send an LSP into a tailspin with a bogus inquiry.

The ability to provide cloud-based picture security services relies in large part on efficient and privacy-preserving content-based image retrieval. In their study "EPCBIR: An Efficient and Privacy-preserving Content-based Image Retrieval Scheme in Cloud Computing," Xia et al. suggested a cloud-based image retrieval system that uses encryption to protect users' privacy. The suggested system accomplishes CBIR over encrypted images without disclosing sensitive information to the cloud by means of image feature vector extraction, pre-filter table creation, and a secure k-Nearest Neighbor (kNN) algorithm, all while improving search efficiency.

In their study "Small-World: Secure Buddy Matching Over Physical World and Social Networks," Li et al. presented Small-World to ensure users' anonymity during the friend matching or recommendation process in social networks. It's meant to be a safe way of connecting people in the real world with those in virtual ones online at the same time. In order to accomplish this, the authors developed a set of modules, including a physical proximity module, a Katz score-based social strength proximity module, a solution based on the El Gamal cryptosystem, and an extension of that solution, to create a multi-hop social connection chain with a maximum of four hops, and a weight assigning function to fine-tune the contributions of individual modules.

J. Pros and Cons of Clod Security

Customers' data remains safe, cybercrime is reduced, and businesses are alerted immediately if an unauthorized person tries to make changes—all thanks to cloud cryptography. Cryptographic key holders are granted access. For security reasons, information is encrypted while being sent from one computer to another. In addition, in today's data-driven environment, cloud encryption enables businesses to take a proactive stance in protecting their data against infiltration and privacy concerns. If the data has been compromised, the recipient will be able to tell, and they will be able to take measures to fix the problem quickly. Data encryption methods that adhere to industry standards like HIPAA, FIPS, PCI/DSS, and FISMA [6] are among the most widely used.

However, there are other drawbacks to this topic, such as the fact that data in transit is only partially protected by cloud cryptography. Protecting encrypted information requires high-tech measures.

In addition, the systems need to be flexible enough to be updated, which adds to the costs, and too protective protections can make data recovery difficult for businesses. However, these difficulties can be readily conquered by strictly adhering to the established principles in encryption.

Businesses and organizations need to adopt a data-centric approach to data security to protect sensitive information from sophisticated assaults in the complex and ever-changing environments of virtualization, cloud services, and flexibility. Businesses should use cryptographic and encryption key management for cloud records and similar data fortification solutions. Access controls and key management capabilities that allow businesses to employ encryption to achieve security goals in the cloud should also be included in any comprehensive cloud security and encryption platform.

Currently with more and more migrations happening to cloud environments from on-premises environment the security is at high alert. Leading providers like AWS, Azure, and GCP are developing more tools and techniques to cope the requirements while preserving the CIA triad in security.

K. Data Storage Security in Cloud environments and auditing using cryptographic mechanisms

a) MAC-base auditing

The Message Authentication Code is a hash algorithm that ensures the authenticity of transmitted data. These procedures encrypt the file in increments of a predetermined size before sending it to the cloud. Finally, the MAC is determined for each encrypted data block. The system will then use these MACs to ensure nothing has been tampered with. Because the auditor needs access to the original data throughout the auditing process in MAC-based protocols, sensitive information may be compromised. A PoR model has been described in reference [8]. This system uses error-correcting and spot-checking codes to guarantee the safety and accessibility of data files kept in off-site service systems. If an audit exceeds the allowed number of times, the whole dataset must be downloaded from the server in order to construct new error correcting codes. This is because the number of times an auditor or data owner may do an audit is stated. A major issue is this.

To ensure the integrity of data stored online, [7] and [12] suggest a TPA. The material is encrypted, and then multiple symmetric-keyed hashes are sent to the auditor in advance. Data file integrity and the server's possession of a previously committed decryption key are checked by the auditor. This strategy will only function with encrypted files, it will need the auditor to keep track of the state, and it will have a finite consumption, which may result in an increased online strain for users after the keyed hashes have been depleted.

b) RSA-based auditing

RSA-Based homomorphic hash value based auditing

For added peace of mind, CSP uses an RSA-based homomorphic hash function to verify the authenticity of private information kept in the cloud. For this method, the data owner breaks up the file into blocks of a certain size, computes a hash value for each block, and then transmits the data to the CSP. After successfully transferring data to the CSP, the data owner only retains the hash values. The Data Owner chooses numbers at random and transmits them to the CSP for auditing purposes. Data integrity evidence is then calculated and provided to the owner by the CSP. The accuracy of the proof is then double checked by the Data Owner.

RSA-based homomorphic tag-based auditing

Instead of using hash values, the data is initially labeled with homomorphic tags calculated by Data Owner. In this scenario, the Data Owner transfers data to the CSP while keeping the data tag in his possession. The data owner issues

a challenge to the CSP, and the CSP returns a proof of data integrity, which the data owner subsequently verifies. The RSA-based homomorphic tag-based auditing is employed in the proven data possession (PDP) methodology [8].

This approach again does not ensure the secrecy of sensitive data because it may leak data during auditing.

In order to analyze the cryptographic threats provided by cloud computing platforms in line with the second scheme of threshold cryptography, a quantitative risk and impact assessment approach called QUIRC is introduced in the paper [14]. The term "risk" refers to the product of the chance of a security threat occurring and the severity of its consequences. These two components together make up what we call "risk." Using the procedure outlined in [15], the Data Owner generates a single key for decryption of the specific file and shares it with all of the data users in the group. Each set shares a common key. Because fewer keys are needed for file decryption, the system also decreases the administrative burden of keeping track of those keys. Only authorized users would have access to the cloud-stored information with the capability-based access control mechanism presented in [16].

IV. Results And Discussion

Challenges have arisen in the form of concerns over data ownership, the impact of software systems on natural resources, and the handing over of data access authority brought about by the rise of cloud computing. The above research led us to the following conclusions about cryptography's potential applications:

- Proofs of irretrievability
- Homomorphic encryption
- Private information retrieval
- Broadcast encryption
- Key Encryption Algorithms
- Auditing based on cryptographic mechanisms

This diagram illustrates how confidentiality, integrity, and availability (CIA) can be achieved with the use of cryptography. This involves a comprehensive analysis and an assessment of cryptographic terms and security logics to combine and provide a more clear and solid perspective to the audience. Because of this, cloud's advantages have permeated all the way up the infrastructure's backbone. However, security algorithms, encryption, and security policies are the meat and cheese that make cloud computing a viable option.

Confidentiality	Symmetric Encryption	Homomorphic Encryption	SSL
Integrity	MAC	Homomorphic Encryption	SSL
Availability	Redundancy	Redundancy	Redundancy

Fig.5. diagram of how CIA can be achieved using cryptography.

In addition, performance issues arise when many securities are implemented using multi-cloud. How to modify cryptographic encryption things with huge keys at little cost, with the clue not yet concluding.

V.Conclusion

It's obvious that data is what drives the modern world, which makes cyber security a major concern. The security of users and their data is crucial to the continued success of cloud computing. Hash functions, symmetric and asymmetric encryption algorithms, and other cloud cryptography methods are used to accomplish this. In principle, cloud cryptography protects private information while yet allowing for rapid data transmission. Using computers and mathematical procedures, the data is transformed into ciphertext, which serves as the only basis for the system. The two most common kinds of encryption used in the cloud are known as data-in-transit encryption and data-at-rest encryption. When it is effectively deployed, cloud cryptography has the potential to deliver several advantages to enterprises of any size. To prevent assaults, it is crucial to have a firm grasp of cloud cryptography.

VI.Acknowledgment

Lasal Hettiarachchi, Senura Jayadeva, Rusiru Bandara and Dilmi Palliyaguruge would like to thank the Sri Lanka Institute of Information Technology (SLIIT) and the Department of Software Engineering for providing the opportunity to create the review paper

References

[1] Cloud Cryptography and Data Security -Gourav Bansal, Kurukshetra University

[2] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3171727

[3] https://ieeexplore.ieee.org/abstract/document/8056952?casa_token=

[4] https://ieeexplore.ieee.org/abstract/document/7924403

[5] https://ieeexplore.ieee.org/abstract/document/8344738

[6] Cryptography and data security in cloud computing, Zheng YAN, Xidian University

[7] Sanjoli Singla, Jasmeet Singh ,"Cloud computing security
using encryption technique", IJARCET, vol.2, ISSUE 7.

[8] R. Bala Chandar, M. S. Kavitha , K. Seenivasan," A proficient model for high end security in cloud computing", International Journal of Emerging Research

in Management &Technology, Vol.5, Issue 10.

[9] Bokefode Jayant.D, Ubale Swapnaja A, Pingale Subhash V., Karane Kailash J. , Apate Sulabha S. ,"Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role bases Access Control Model", International Journal of Computer Applications, Volume 118-No.12, May2015

[10] Karun Handa, Uma Singh," Data Security in Cloud Computing using Encryption and Steganography", International Journal of Computer Science and Mobile Computing", Vol.4 Issue.5, May-2015, pg.786-791

[11]M.Vijayapriya,"security algorithm in cloud computing: overview", International Journal of Computer Science & Engineering Technology (IJCSET), Vol.4, ISSN: 2229-3345.

[12] Improving Data Storage Security in Cloud Environment Using Public Auditing and Threshold Cryptography Scheme
1.Reshma Suryawanshi, Sinhagad Academy of Engineering
2.Santosh Shelke, Sinhagad Academy of Engindeering

[13] Rashmi Nigoti, Manoj Jhuria, Dr. Shailendra Singh, "A survey of Cryptographic algorithms for cloud computing", International Journal of Emerging Technologies in Computational and Applied Sciences, March 2013, ISSN (online)-2279-0055.

[14] Douglas R. Stinson," Cryptography: Theory& Practice",
Chapman and Hall Publications.

[15] Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Stephen S. Yau, Efficient audit service outsourcing for data integrity in clouds, The Journal of Systems and Software 85 (2012) 1083 1095.

[16] N.Sengupta, J.Holmes, Designing of Cryptography Based Security System for Cloud Computing