CHAPTER - II
LITERATURE REVIEW

2.1 INTRODUCTION

Since the proposed research work aims to provide security solutions to the federated cloud environment, this section offers a comprehensive literature review about various cloud computing aspects such as distributed computing issues with respect to partitioning approaches, inclusion of broker in cloud architecture, security models in cloud, splitting of data in a typical cloud data centre, algorithmic approaches for enabling security constraints, pros and cons of different algorithms with appropriate outcomes are dealt.

2.2 DISTRIBUTED COMPUTING ISSUES

In distributed computing environment, there are few issues still existing. Through my literature survey I found six main areas[77][75][34]. They are,

2.2.1 Authentication

Authentication [77] is a core security in grid computing that requires mutual trust between parties. Common tools used for authentication in grid computing such as protocols and certificates are based on cryptographic algorithms. In general, authentication is achieved through the presentation of some token that cannot be forged. Biometrics can be used, especially as a mechanism by which a human can acquire a token that is later presented to a service for authentication purposes. For example a finger print scanner can be used to log in to a local machine. In general, authorization is based on authentication schemes. So far, most middleware such as globus, uncore, and legion rely on this concept. In there are two general approaches for authorization, which are identity-based or token based. Identity based approach is typically associated with access control lists, while token-based approach is also referred to as capability based authorization. A drawback of identity-based approach is that it cannot easily support delegation. On the other hand, a drawback of a token-based approach is it may be very difficult to dynamically revoke access rights.
2.2.2 Confidentiality

Important data or programs that are transmitted or transported between parties should be secured and protected. Furthermore, secure area should be established to prevent those from outside to be able to access the data or program. Although, cryptographic algorithms and policies are necessary to gain a high level of confidentiality, port monitoring of remote machines are also very important.

2.2.3 Integrity

Integrity is a “issue that concentrate on what prevent subversion of a system if someone did get it. It also deals with recovery from damage done either intentionally or unintentionally”. Based on this definition, there is a need to apply a physical security schemes in grid environment such as policies and tool which can save the data, applications, and any equipments from damage or loss. So far, the responsibility for integrity in grid computing relies on the individual organizations or user.

2.2.4 Non-repudiation

Non-repudiation [20] is the concept of ensuring that a party in a dispute cannot repudiate or refute the validity of the statement. In the receiver of the message checks the signature by calculating the hash of the clear text document and comparing the hash value with the value attached to the message itself. If the two matches, the receiver has strong evidence to believe that only the purported sender could have sent the message. Most popular algorithm in grid computing is digital signature algorithm (DSA) and time stamp authority (TSA) [14].

2.2.5 Management

Irrespective of the security schemes, the wide spread and variety of resources and the decentralization in grid computing made the management of grid very difficult. Therefore, certificates with its various types and policies are playing a core role in this field.
2.2.6 Denial of Service

Denial of Service (DoS) attack is one of the common attacks on distributed systems. These attack mainly target resources in such a manner that the resources are prevented from carrying out their legitimate operations. A method that uses services and markov chain to mitigate the effects on the DoS attack on a cluster based wireless sensor network has been presented in.

2.3 CLOUD SECURITY PROS AND CONS

2.3.1 Pros

- Access data anywhere on any smart device
- Frees up IT resources to focus on the core competency of the business
- Provides scale so that you can easily provision additional servers to meet computing needs
- Up to date – Lets you work with the most current hardware and Operating Systems. Some cloud providers manage the VMs, applying patches, and maintenance
- Reduce your IT costs using the PaaS model of cloud
- Provides a low cost, easy way to ensure backup and disaster recovery with offsite backups.
- Enhanced security from Internet services, by preventing loss due to fire, theft, or disaster.
- May keep costs low as you only have to pay for what you use, and don’t need to make significant upfront investments.
2.3.2 Cons

- Outages, while unlikely, can impact your business. Large files on STaaS require large amounts of network bandwidth to conduct storage utilization and internet-based services.

- Potential lock-in – Depending how you enable storage for your website. It may be challenging to move to another provider if you write provider-dependent code.

- Privacy – Governments (for example via the US Patriot Act) can potentially access your data. You may need to encrypt your data before storing it in the cloud, if this is a concern.

- Hard to predict costs. Because it’s so easy to get started with cloud services, and with such a low level of investment, if your business scales rapidly you may not have planned for these potential incremental costs.

So when thinking about cloud storage for your website, you most likely will want to consider the points above.

When it comes to cloud storage for your website, in general the pros outweigh the cons in my opinion. But also realize that how CMS vendors support cloud storage isn’t all the same. To avoid the potential costs and complexities of being locked into a specific platform, you most likely will want to choose a solution that will easily let you switch from Microsoft Azure to Amazon, or vice versa. You can find out more about the technical differences between Microsoft Azure and Amazon cloud storage in my previous post.

If you want to learn a little more about this increasing trend check out how Gartner Predicts Infrastructure Services Will Accelerate Cloud Computing Growth for a little more in depth analysis from a business perspective.
2.4 BROKER BASED CLOUD – THE NEED

The proportion of cloud services purchased through cloud brokers [14] is growing, and Gartner predicts [28] it will soon make up a substantial portion of cloud purchases. The appeal of a cloud broker is obvious: It allows the enterprise to leverage specialized expertise to provision expensive and complicated services. But what is a cloud services broker (CSB), and why do so many companies need one? What’s the impact of CSBs on IT, and should brokering the cloud be done externally or can it be as an internal IT function?

2.4.1 The Role of a Cloud Services Broker

As organizations continue to turn to cloud computing, the demand for specialized expertise to provision the optimal cloud offerings for enterprise business and technical requirements is rapidly increasing. This has led to the swift emergence of CSBs, who help the enterprise with all things cloud: from evaluating cloud service providers to negotiating contracts and documenting cloud vendor deliverables.

2.4.2 Internal Vs External Brokering

But is it worth paying the fees for an external firm, equipment vendor or consultant to serve as a broker [42], when instead IT staff could do it themselves? Today, many companies lack experience in analyzing cloud services and negotiating contracts with cloud vendors. Instead, they opt to use external CSBs to augment existing IT resources and accelerate institutional learning so the organization can broker cloud resources internally in the future or companies can opt to turn to trusted equipment vendors that have consulting practices to help them evaluate cloud requirements, identify shadow IT utilization of public cloud services that IT may not even be aware of, and make recommendations on cloud strategies.

But the use of external professional services can get expensive, and an internal CSB function is increasingly showing up within IT organizations. Organizations need a CSB function to secure cloud services, and the choice of
whether to select internal or external resources is being made largely based on existing staffing resources and skill sets within IT and the policies and procedures of each organization.

2.4.3 The Need for a Trusted Intermediary—Third party

A good CSB should know the cloud market well. And a trusted CSB can make it easier, more secure, and less costly to choose and manage cloud services, particularly in multi-cloud environments. Fast IT is transforming IT infrastructure, making it more flexible, automated, simple, and secure, and the enterprise is working with an ever-increasing number of cloud vendors. Whether the CSB is an internal or external resource, by acting as an intermediary between the enterprise and cloud service providers, a broker [45] should add value by helping the enterprise clearly define business and technical requirements while carefully evaluating the infrastructure capabilities, security policies, and unique differentiating features offered by each cloud service provider.

2.4.4 Aggregation, Integration and Customization of services

When Gartner [29][30] first introduced the concept of CSBs in 2011, the research firm laid out the three primary roles of a cloud services broker as aggregation, integration, and customization. With aggregation, a broker packages services from multiple cloud providers to ensure interoperability and security of enterprise data passing between systems.

A CSB [33] focused on integration will help an organization coordinate multiple cloud services, and CSBs focused on customization help IT find and tailor cloud services to meet their unique business and technical requirements. CSBs can also fulfill other important functions, such as helping the enterprise define and implement cloud governance policies and analyzing whether to migrate premises-based applications to the cloud.

Bringing the CSB role in-house as a specialty practice is an increasingly attractive proposition for many organizations, particularly as they learn from their early experiences with external CSBs and train IT staff in the many skills needed to broker cloud resources for the enterprise.
It takes time to develop and implement strategies for managing this function in-house because cloud brokers require skills ranging from negotiation to security to financial analysis, as well as domain expertise in multiple areas. For many companies, promoting internal senior IT professionals and investing in training them in a new model of IT to complement their existing skill sets with cloud-focused business and technical skills is a faster path to building in-house CSB capabilities than recruiting IT professionals that lack institutional knowledge.

It remains IT’s responsibility to make sure that cloud-based services used by the enterprise comply with enterprise governance, security, and compliance policies while minimizing enterprise risks, and efficiently brokering the right cloud services is increasingly essential in multi-cloud environments.

Smart enterprises are using multiple cloud computing providers and services to avoid vendor lock-in and stay diverse. But there’s a flip side to all these clouds: Public and private cloud services are hard to coordinate, and CIOs are finding that business divisions are using services outside those offered within their companies, creating governance problems.

Cloud service broker products solve most of these problems through an easy-to-use storefront that manages the use, performance and delivery of your cloud services. Here you can view a list of your services and select an option, such as moving an instance from your private cloud to the public cloud. Once you select your options, and are charged accordingly, you are notified that your instance is running and given a link to the reporting metrics for your service. You can also shop for services based on service-level guarantees, price points or performance. All of this is done via your selection in the CSB, and the hard work is automated in the background.

At its best, an in-house CSB product gives enterprises flexibility with internal and external cloud service providers and makes it unnecessary for a company to lock itself to a single vendor or type of cloud architecture.
Cloud service broker creates a governed and secure cloud management platform to simplify the delivery of complex cloud services to cloud service customers. They enable customers to realize the full potential that cloud provider has to offer. They enforce the correct IT policies and effectively handle service level agreements between cloud provider and cloud service consumer. Cloud Service Broker creates a trusted, governed and secured cloud management platform between cloud service provider and cloud service consumer. As such however, the term cloud service broker is a loosely defined one and is meant to stand for several different models.

2.5 APPROACHES FOR DATA PARTITIONING IN CLOUD DATA CENTRES

In this section we describe the data partitioning framework, focusing on the two core components: constructing the partition blocks and distributing them across multiple worker nodes. In order to provide partitioning models that are customizable to different processing needs, we devise three types of partition blocks based on the vertex structure and the vertex access pattern.

There are many nodes in a public cloud which are at different locations. The cloud has a Main Controller (MC) which chooses the suitable partitions for arriving jobs. The appropriate partition is selected by using best load balancing strategy. All the status information is gathered and analyzed by main controller and balancers. They also perform the load balancing operations. The system status then provides a basis for choosing the right load balancing strategy. In this paper we will use approximately 4 different servers, which are partitioned into small clouds called balancers (each balancer will have some servers). Cloud Service Provider (CSP) is used to handle a Main cloud (which is made up of small Clouds) called Main Controller or Controller main. Client interacts with cloud using a web application called client Site. When client uploads file it will be stored in the server. The cloud will take care that it will be loaded into the server which has minimum load.
To secure the cloud storage, five layers approach proposed by Bashir Alam et al [7]. There are five layers namely, the External Layer, Conceptual Middle Layer, Conceptual Layer, Physical Middleware Layer and Physical Layer. The main function of the service provider is to supervise and supply the services with full transparency and security. The conceptual level heterogeneity amongst dissimilar databases like SQL, DB2, Oracle etc. This coating represents the logical structure of the complete database and deals with the domestic processing on data. This layer provides the capability of defeat the heterogeneity across the dissimilar platforms like windows, Mac OS, Linux etc. This layer represents the physical representation of the data. In a cloud database service, the backend is creature overseen by a Physical layer that’s dependable for the continuous monitoring and configuring of the record to accomplish optimal scaling, high accessibility, and multi-tenancy and efficient reserve distribution in the cloud.

Xinyu Leit et al [67]. proposed Model which has some transformations on the Matrix Multiplication Computation (MMC) to get an encrypted MMC problem which is sent to the cloud and then transforming the outcome returned from the cloud to get the accurate result to the innovative MMC difficulty. Subsequently a randomized Monte Carlo confirmation algorithm with one-sided error is introduced to productively handle result authentication. In this paper they are suggesting protocol which ensures correct, secure and robust cheating resistant.

Security threats faced by cloud information storage can come beginning two different sources. On the one hand, a CSP can be self-interested, untrusted and probably malevolent. Not only does it yearning to move data that has not been or is infrequently accessed to a lesser tier of storage than decided for economic reasons, but it may also effort to hide a data loss occurrence due to organization errors, Byzantine failures and so on. On the other hand, there may also exist an reasonably aggravated opponent, who has the capability to compromise a number of cloud data storage servers in different time intervals and subsequently is able to modify or delete users’ data while remaining undetected by CSPs for a certain period. Two types of adversary proposed viz weak and strong. Weak Adversary: The challenger is concerned in corrupting the user’s data files stored on personality servers. Once
a server is comprised, an adversary can pollute the original data files by modifying or introducing its personal fraudulent data to thwart the unique data from being retrieved by the consumer. *Strong Adversary:* This is the nastiest case situation, in which we presume that the challenger can negotiation all the storage servers so that he can calculatedly adjust the data files as long as they are within dependable. In fact, this is correspondent to the case where all servers are colluding mutually to hide a data loss or altered form occurrence. To accomplish the storage accuracy, Fast localization of data error, energetic data support, dependability and light weight, there are three algorithms developed. Token pre computation, Correctness verification and Error Localization and Error Recovery algorithms are used to ensure the data security in the cloud.

For a security over cloud environment [68], this paper gives the idea, which followed by banking sector. Here, rules are framed and to be followed for the customer successful transactions. They are (i). All the cards only should be active through internet banking and transactions should be via the IP range of the company. (ii) Some accounts necessitate having a phone numeral to call and text message verification. If the substantiation is not received contained by a certain period of time, the contract will be cancelled; (iii) Transactions necessity be approved by a fax or an e-mail. Otherwise, after a confident period of time, the reverse operation is generated by the system and the first contract will be cancelled; (iv) transaction tracking codes will be sent throughout a channel. One or more receiver numbers can be used to substantiate the transactions. Based on these considerations, in the next segment a security explanation for card transactions is projected.

Mark D. Ryan [43] proposed three types security in cloud computing viz. (i) Homomorphism encryption- it is an encryption technique that allows a part that holds cipher texts to perform certain operations on the cipher texts, which mirror the corresponding operations on the plaintexts. In the case of simple homomorphism encryption, there is just one operation on the plain text that has a corresponding operation on the cipher text.(ii) Key translation in the browser- With this approach, data is encrypted before being uploaded to the cloud, and the data
owners retain the keys. However, dissimilar parts of the data may be encrypted with unusual keys and some of the clients participating in the service may execute “key translation” in order to agree to data items to be forwarded to planned recipients. (iii) Hardware-anchored Security – to achieve confidentiality from the cloud provider is based on special hardware on the cloud side. The idea is that the cloud provider is able to decrypt the data, but is able to offer guarantees about the circumstances in which it does that. Those guarantees will promise that the data owners that the data is handled in agreement with their policy.

Mehmet Yildiz et al [45] proposed a dynamic security model for cloud security. This model is based on eight aspects and includes four layers. Network, Storage, Servers and Application layers. It includes one enterprise level principles at the highest level and a system management aspect. It also includes two kinds of dynamic security types: horizontal and vertical. The horizontal type is specific to each layer end to end. Here, horizontal dynamic security policy for storage does only cover the security objects related to storage. The vertical type is designed to cover the interfaces between layers. Some security objects between servers and storage may be partially belonging to each layer. The vertical dynamic policies ensure that any common object or exception is covered.

The EU’s Data defense instruction (95/46/EC) gives consumers certain basic rights with reverence to their personal data while requiring “data controllers” to go behind rules and limitations with deference to their data dispensation operations. Consumers are permitted to notice of the characteristics of any data controller and the purposes for which their private data are being together and otherwise processed. This Directive requires data controllers to pursue eight core ideology of data isolation protection that define the individual rights of consumers and the responsibilities of data controllers that process personal data. These data processing rights and responsibilities concern to the dispensation of personal data by companies regardless of the context and should be implicit to apply to cloud-computing systems. In the EU, businesses may not assemble, store, use or disclose consumers’ private data unless they observe with the Data Protection Directive and any more thorough regulations that have been adopted in the associate States’ laws. This means private data may only be collected and processed for particular,
unambiguous and legitimate purposes and may not be processed unpredictably with those purposes (legitimacy and finality). The data question must be fully conversant on the details of the dispensation, counting who has access to the data, how it is stored and how the focus can review it (transparency). Personal data must be sufficient, relevant and not unnecessary in relation to the purposes for which it is composed and further processed (proportionality). Supplementary, businesses are required to provide enough security for consumers’ personal data to avoid unauthorized contact to the data.

Sandeep K. Sood [61] proposed construction has been structured to make available complete protection to the data throughout the complete process of cloud computing, be it in cloud or in transfer. Consequently multiple mechanisms and accessible techniques are applied to protect the critical information from unauthorized parties. The planned frame work is separated into two phases. First phase deals with procedure of transmitting and storing data securely addicted to the cloud. Second phase deals with the recovery of data from cloud and presentation the generation of requests for data contact, double confirmation, authentication of digital signature and reliability, thereby providing approved user with data on passing all security mechanisms.

Another secure model and protocol that will enable data sharing amongst a group of users specified by the data owner. These techniques implemented in health monitoring systems and are not limited in any way to medical applications and can be applied to other Cloud applications. For secure transmission of data ElGamal encryption and Proxy re-encryption.

An incorporated approach to secured clouds h to an integrated secure cloud platform to facilitate aims to embody all of the above ideology. The first step is to identify the threats and necessities of Critical Infrastructures. This infrastructure generally focus on Hacking attacks, DDoS attacks, Insider attacks, Equipment failures, End –to –end issues ,espionage and data loss or corruption.

Nancy et al.[51] gives the recommendations regarding the reform in EU and US regulations on customer sensitive data. The reforms include (i) expanding the legal definitions of sensitive data that deserve heightened data protection (ii) reducing regulatory constraints that currently limit EU and U.S businesses from taking full advantage of the benefits of cloud computing.
2.6 ALGORITHMS FOR CLOUD SECURITY MODELS - A REVIEW

To provide secure communication over the network, encryption algorithm plays a vital role. It is the fundamental tool for protecting the data. Encryption algorithm converts the data into scrambled form by using “the key” and only user have the key to decrypt the data. In Symmetric key encryption, only one key is used to encrypt and decrypt the data. Another technique is using asymmetric key encryption; two keys- private and public keys are used. Public key is used for encryption and private key is used for decryption. Figure Fig 2.1 shows some of the symmetric & asymmetric algorithms[52][37].

2.6.1 Symmetric Algorithms:

**DES:** This stands for Data Encryption Standard and it was developed in 1977. It was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). DES is 64 bits key size with 64 bits block size. Since that time, many attacks and methods have witnessed weaknesses of DES, which made it an insecure block cipher.

**BLOWFISH:** This was developed in 1993. It is one of the most common public algorithms provided by Bruce Schneier. Blowfish is a variable length key, 64-bit block cipher. No attack is known to be successful against this. Various experiments and research analysis proved the superiority of Blowfish algorithm over other algorithms in terms of the processing time. Blowfish is the better than other algorithms in throughput and power consumption.

**RC5:** It was developed in 1994. The key length if RC5 is MAX2040 bit with a block size of 32, 64 or 128. The use of this algorithm shows that it is Secure. The speed of this algorithm is slow.

**3DES:** This was developed in 1998 as an enhancement of DES. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level. But it is a known fact that 3DES is slower than other block cipher methods. This is an enhancement of DES and it is 64 bit block size with 192 bits key size. 3DES has low performance in terms of power consumption and throughput when compared with DES. It requires always more time than DES because of its triple phase encryption characteristics.
**AES:** (Advanced Encryption Standard), is the new encryption standard recommended by NIST to replace DES. Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption. Both AES and DES are block ciphers. It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications.

**2.6.2 Asymmetric Algorithms**

**RSA:** This is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption. Till now it is the only algorithm used for private and public key generation and encryption. It is a fast encryption

**DSA:** The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS) and adopted as FIPS 186 in 1993. Four revisions to the initial specification have been released: FIPS 186-1 in 1996, FIPS 186-2 in 2000, FIPS 186-3 in 2009, and FIPS 186-4 in 2013. With DSA, the entropy, secrecy, and uniqueness of the random signature value \( k \) is critical. It is so critical that violating any one of those three requirements can reveal the entire private key to an attacker. Using the same value twice (even while keeping \( k \) secret), using a predictable value, or leaking even a few bits of \( k \) in each of several signatures, is enough to break DSA

**Diffie-Hellman Key Exchange (D-H):** Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior
knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

**El Gamel:** In cryptography, the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. It was described by Taher Elgamal in 1984. ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The Digital Signature Algorithm is a variant of the ElGamal signature scheme, which should not be confused with ElGamal encryption. ElGamal encryption can be defined over any cyclic group. Its security depends upon the difficulty of a certain problem in related to computing discrete algorithms.

![Fig 2.1 Classification of Algorithms](image-url)
2.7 Conclusion

By surveying more number of papers, there are security algorithms available to protect the data. Studying the various algorithms using various parameters for my research we have chosen RSA and ECC algorithms. By combining these we can develop a new algorithm and implement in our cloud data storage. Through this literature survey, we can develop an algorithm using vertical partitioning in order to secured the cloud data.