Privacy Protection In Cloud Using ECC System:

A Comparative Analysis

# Dr.Manoranjini J1, Dr.S Sowjanya.C 2, Dr.Sengole Merlin

# *1, Professor, Department of CSE, Swamy Vivekananda Institute of Technology, Hyderabad, Telangana State, India*

# *,2Asst Professor, Department of CSE, Sreyas Institute of Engineering and Technology, Hyderabad, Telangana State, India*

# *3Cloud Consultant,Freelancer,Texas, USA*

1drmanoranjinicse@gmail.com,2soujikits@gmail.com,3sengolemerlin@gmail.com

# Abstract. The growing rapid mobile technology is wide and far using the cloud as the platform for data storage and retrieval. Cloud contains software’s and services which is accessible to users on- demand. This on-demand service availability puts risk to cloud users. The virtual cloud has enormous security breaches. So, we have proposed system for protection of private data of users using elliptic curve cryptography ECC.ECC includes mathematical operations which enables to provide more security and accurate results. We have analyzed and studied and compared the results by the performance by AES algorithm and the ECC.

# Keywords: Cloud, ECC, Hybrid Cloud, Encryption, Decryption, AES

# I.INTRODUCTION:

# Cloud computing is a term that refers to the amalgamation of cybernetics referred to as computing with Internet-based growth acknowledged as cloud. Cloud computing is huge web of processors placed in a single site (usually stated as a Cloud data processing center.) that can be acquired remotely by a user. It is enormously accessible and internationally obtainable on-demand, with significantly inferior principal expenditures than typical corporate application and service hosting centers. This enables users to install an application as required, and because it was built from the bottom up to be extremely mechanized, it will pay for itself in decreased running expenditures and redundant systems, eliminating the possibility of a single point of failure. Cloud computing refers to the delivery of all sorts of services through the Internet. Storage space, server, a database, applications, social networking, cognitive ability, and data analysis are all examples of cloud computing services. [1]

**II. What is Cloud Computing? :**

# Cloud computing refers to the supply of various services through the Internet, such as data storage, servers, databases, networking, and software. Cloud storage has increased in popularity among people who want more storage space and organizations looking for an effective off-site data backup option. A cloud refers to the services and software that run on Internet. Privacy in data in the cloud allows collection, storage, transfer and share of the data taking care of the privacy of personal data. The significant components are front end, back end and cloud based delivery components.



**Fig i) Architecture of Cloud Computing**

# Front End: A cloud computing business platform's front-end infrastructure is essentially anything with which the end-user interacts. The user interface is the result of the integration of different sub-components. This governs in what way the end-user links to cloud computing. It comprises of web browsers, graphics cards, local networks, web applications and operating systems that allow access to tailor-made programming from suppliers such as Microsoft & Google. In front end of architecture, cloud is used by client who contains client-side interfaces and applications required to access the cloud computing platforms. It includes web servers, thin & fat clients, tablets, mobile devices.

**Front-end modules:**

1. **UI:** The cloud delivers a streamlined atmosphere in which end users may execute activities deprived to launch any software on their native workstations. Users can interact with tablet android phone, computer, all of which require on an interface to function effectively. Google Docs, Gmail, and evernote are examples of popular interaction interfaces.
2. **Software:** The front end software architecture is what the user sees. It is made up mostly of client-side apps that are in charge of displaying records to consumers.
3. **Customer or network device:** Client-side device is the hardware on the end user's side. It may be any input device, such as your mouse, keyboard, or sound card, because it is a critical component of the frontend architecture. In cloud computing, the client-side device does not need to be very powerful to handle huge loads.

# Back End: In back end of architecture, cloud is used by service provider which manages all resources required to provide cloud computing services. It also includes huge amount of data storage, security mechanism, virtual machines, deploying models, servers and traffic control mechanisms. characteristics of cloud computing includes self-service provisioning, elasticity, pay per use, workload, resilience, migration flexibility, broad network access and multitenancy.The advantages of cloud computing includes data security, data backup and restore, low maintenance cost, infinite storage capacity, pay-per-use services and excellent accessibility. Cost savings, high-speed, backup and restore of data, unlimited storage capacity are some of the advantages of cloud. Security is the main concern for cloud. The cloud-based back-end architecture enables the front-end architecture. It is made up of hardware and storage that are housed on a distant server. This backend architecture is managed and controlled by the cloud service provider. Because it is entrusted with supporting the framework of a cloud-based system, seamless back-end cloud infrastructure is considered as a durable and persistent as promising.

**Back End Components:**

1. **Application:** A user interface used by clients is an important component of the application architecture. It provides backend services that allow clients to access their data. This layer handles their needs and requirements.
2. **Service:** Backend cloud computing is a fantastic range of investigation that provides usefulness to any cloud hosting structure. This facility enables the execution of any cloud-based job. Administration and solicitation programming, repository and web services are some prominent services that enable various activities to perform fast and competently on a cloud runtime atmosphere.
3. **Cloud Lifecycle Phase (Runtime) :** The phrase 'Cloud Runtime' is a catchword that alludes to the notion of easily available services. This is similar to a cloud operating system, which uses technologies such as virtualization to allow individuals to access a large number of networked servers at the same time. While these servers are backed by virtualization architecture, they function as independent storage devices. They operate independently of one another and comprise the primary server known as Hypervisors. Oracle VM for x86, Oracle Virtual Box, VMware Fusion etc are some of the examples.
4. **Storage:** Cloud storage refers to the location of data within a cloud application. This is usually done with a specific part of the cloud. SSDs, HDDs, Intel Optane DC Persistent Memory, and other technologies are examples. The majority of the storage in the system is provided by HDDs in server bays, with solid-state repositories accounting for a tiny portion.
5. **Substructure & Design:** Substructure is the mechanism that drives entire cloud software facilities. It is a wide phrase that encompasses a variety of skills like network cards, accelerator cards, Graphics Processing Unit (GPU) and so on. The workload of your clients influences the infrastructure model.
6. **Management:** software serves as ‘middleware' for a cloud computing structure. It ensures that if any organization has duties linked to several fronts, this type of software provides different resources to each activity and ensures that each task receives its fair share of attention.
7. **Security:** is both essential and crucial. The security structure of the design is built with one goal in mind: keeping track of debugging activities. Bugs are handled on a daily basis, if not on hourly basis. Periodic system backups are required since what is the use of having something if it cannot be recovered when needed? Because the cloud is not resistant to virtual intimidations, firewall software is required for the security infrastructure to function properly.

**iii) Cloud Based Delivery:**

A cloud-based solution is everything that can be accessed via search engine from any method with internet connection. Expertise behemoths combine a limited number of items and distribute it to customers in an easy-to-use style using the approaches as follows:

* **SaaS model Framework:** SaaS model is a software dispersal paradigm in which creators place their programmes on a cloud-based distribution scheme. Patrons gain admittance to such programmes over World Wide Web, often via an internet service provider. SaaS subscriptions may be particularly cost-effective because the customer does not need to invest in additional IT equipment.
* **PaaS model Framework:** This paradigm, which is typically managed by an organization, enables customers to successfully maintain apps on the cloud in addition to designing and running them there. In the PaaS model, a third-party company will offer technical resources such as hosting or development tools. Some examples are Google App Engine, Apache Stratos, Heroku, Force.com, and others.
* **IaaS model Framework:** This strategy provides the framework needed for businesses to function. It combines storage, data centre space, and both virtual and physical servers. Cloud computing, a subset of utility computing in which the service provider grants access to distributed systems and resources, is another service offered by IaaS. A few examples include Linode, Rackspace, Amazon Web Services (AWS), Microsoft Azure, and Google Compute Engine (GCE). There are three cloud deployment models in addition to the cloud delivery kinds already mentioned below:
1. **The public Cloud:** While the public cloud may give client companies and service providers with economies of scale, it lacks control over the location and security of confidential data housed in an infrastructure-as-a-service environment. Without complete control over their data encryption systems, many large firms and government agencies are no longer able to outsource their IT operations. Because of this, private clouds are increasingly being viewed by company leaders as a viable option for protecting personal information, even if they may be more expensive to adopt for some organizations.
2. **The Private /Personal Cloud:** b. The Private /Personal Cloud: A private cloud is the greatest choice for organizations of all sizes and types since having a matching online presence is vital for attracting and retaining potential customers. A private cloud also gives more precise degrees of control and security, which is especially relevant for bigger organizations with highly stringent security or data protection expectations and requirements.
3. **Hybrid Cloud:** A hybrid cloud is formed by combining two clouds into one. On the one hand, it's comparable to the services offered by a conventional public cloud (such as Amazon Web Services or Google Cloud Platform) in that it provides clients with basic resources that may be used to host websites, applications, and even complex services on their computing platform. It is a private cloud, which is comparable to an internal data centre in that customers may use as much or as little bandwidth and storage space as they like, with everything running behind a firewall for ease and security. This design offers various benefits to those who want to combine the best of both worlds in order to host the most critical business-related applications without sacrificing performance or dependability.



 **Fig ii) Hybrid Cloud**

In Hybrid cloud, Non-critical operations are handled by the public cloud, whereas vital tasks are handled by the private cloud. A hybrid cloud is mostly employed in banking, healthcare, and universities. Amazon, Microsoft, Google, Cisco, and NetApp are the finest hybrid cloud providers. [2]

**III. PROS AND CONS OF CLOUD COMPUTING:**

It solely makes in a monetary sense, why cloud computing has grown so popular among businesses all over the world. Let's take a closer look at what this type of technology can accomplish for user may not be aware of all the advantages of cloud computing.

**1.** **Lower The Costs Of Infrastructure:**

Companies spend a lot of money on internal data storage. Both the upfront cost of buying each new server and the cost of deploying them are involved. Either you have to pay the vendor to handle the installation, or your IT team needs to take time out of their busy schedules to execute it. You save money since the cost of the infrastructure is covered by your plan and shared by all of the clients of the service provider. Businesses that use cloud computing services annually save more than 35% on operational expenses, according to a survey on the global cloud services market.

**2. The Effect on Personnel:**

The cost of keeping an internal IT team large enough to operate local servers may rise fast. The time and money spent on hiring and training are all done in the hopes of creating a committed and highly successful worker, but that isn't always the case. Some workers will perform below expectations, while others could choose to quit the company. IT industry turnover costs businesses 150 percent of an employee's compensation. Your internal team also includes the benefits that come with having an in-house staff come at an additional expense, which cloud services may help offset. Your in-house team may be refocused, or you can avoid the expense of future team expansion, while your service provider takes care of maintenance and backups.

**3. Data Consolidation:**

Data is dispersed throughout bicoastal data centers using cloud storage. Data can be linked and updated fast thanks to synchronization technology, however syncing is not required when data is stored in the cloud. You always know exactly where each piece of information is when it is all saved on the cloud.

**4. Prevent Catastrophes:**

Losing data may be disastrous for any size of business. Data breaches cost $3.86 million on average globally, and $7.91 million on average for businesses in the US. Operating a data centre on-site is far less secure than using cloud-based storage. When compared to companies that employ cloud storage, those who store their data on-site experience a 51 percent higher rate of security problems. Cloud storage services offer enterprise-level security that is significantly superior than what most small and medium-sized business enterprises (SMB) can afford on-site. There isn't a single point of abandonment, which is one benefit of using the cloud to store data. Your data is replicated across many servers so that even if one of them crashes, your organization's data is still safe and secure.

**5. Improve Uptime:**

Unplanned downtime has a significant financial impact that cannot be overstated. An average business loses $5,600 for every minute of unanticipated downtime brought on by a data centre failure. $300,000 was made in under one hour. The productivity lost during that period is money you won't be able to recover, even though employees may like the extra time spent in the break room. If unplanned downtime has a negative impact on clients, it can also seriously harm a company's brand.

**6. To Strengthen Collaborative Teamwork:**

It is now more common than ever for businesses to have staff working all over the world, making collaboration skills as indispensable. Using cloud computing, numerous employees may see and edit files and documents in real time, making it much easier for team members to work together on projects. Browsing documents in the cloud makes it easier to verify that everyone is using the most recent version of a document and to prevent the spread of outdated copies among local sources.

**7. Stay Adaptable:**

How might cloud computing help your business grow? One of the problems of growing is staying scalable.

Utilizing cloud computing keeps scalable. Or, cloud storage service provider a call and ask them to quickly raise company’s cloud capacity. Increasing cloud also has predictable costs, which removes the risk involved with making investments in new storage equipment. Your organisation will become more nimble and competitive regardless of your sector if you have a better ability to raise or reduce its storage capacity as necessary.

**8. Amplify Automation:**

Regular backups are an important part of sustaining internal data storage. The IT department must set out time to plan backups around everyday activities. These routine backups may be greatly automated using cloud computing services, allowing your employees to get back to work.

**9. Conserve Space:**

In-house system expansion frequently necessitates careful planning to acquire the appropriate amount of space due to the substantial square footage required by servers and all of its accompanying equipment. Larger firms may have more room to expand into, but smaller businesses sometimes struggle to make the most of every available square inch. By removing the need to prepare for future equipment growth, cloud computing can free up space in your workplace for additional amenities or workstations.

**10. Improve Compliance:**

The many rules that apply to various forms of data are difficult to comprehend, time-consuming to implement, and labor-intensive to maintain. Why not delegate the labor-intensive aspects of compliance to a cloud storage service provider? A trustworthy provider adheres to all regulations.

Let us elaborate the drawbacks of the cloud storage have:

**1. Consciousness of the Expenses:**

Although moving to the cloud might help cut expenses in some areas, it is crucial to make sure that the move is justified. A proper strategy must be implemented, and all organizational systems must be examined. The secret is to analyze the systems and divide them into two groups. Systems that ought to be migrated to the cloud and those that ought to stay on-premises fall under these two groups. You may then decide on a budget for the project after this has been decided.

**2. Transition from on-Premises to the Cloud:**

A company may often experience a transition from on-premises servers to cloud data centers without much difficulty. Switching to a different cloud provider or going back to an on-site server is not as simple. The costs associated with this procedure might really add up, and the conditions frequently favour the cloud provider. Make sure to inquire about and comprehend the procedure for relocating workloads out of the cloud supplier's data centre before selecting whether or not to sign into a contract with them. Covering the deadlines, penalties, and procedure is essential.

**3. Restrictive Control:**

Businesses may be concerned that they won't have adequate control over the service because the service provider owns and manages the cloud infrastructure. The end-user license agreement (EULA) of the supplier may be able to assist you in this situation. It details the restrictions the provider may impose. It describes the restrictions the supplier may impose on how you utilize the deployment. Even if they don't let user to make any changes to the architecture, all reputable cloud computing companies let business exercise control over its apps and data. Make sure to comprehend every term of the service level agreement (SLA) that the supplier gives. This will enable to confirm what is permitted and prohibited using the service.

**4. Lock-In Of Vendor:**

Vendor mismatches may represent one of the drawbacks of cloud computing. When transferring services to a different vendor with a different platform, organisations may experience difficulties. It's possible for data to be exposed to needless vulnerabilities if this procedure isn't managed properly.

**5. Slower Restores and Backups:**

Due to the high communication delay involved in sending data to the cloud, backups may wind up taking longer than they would with an internal system. This often isn't a problem, not even for bigger, full backups. The initial, larger backups take longer, but they may operate in the background without interfering with networks. It can take longer if you have to restore the entire server. However, certain files and folders probably won't be affected. If you choose the correct provider, speed differences are barely noticeable.

**6. Internet Dependence:**

The fact that cloud computing is totally dependent on the internet is a slight disadvantage. For the length of the outage, you won't be able to access data saved in the cloud if your internet connection drops. An internet outage won't jeopardize or erase your cloud-stored data, though. Cloud computing is essentially the same as any other web-based technology because practically every operation of your organisation requires the internet.

**7. Use of the Internet:**

Large backups to the cloud have the potential to cause congestion and degrade your internet speed if they are being done during business hours when internet usage is high. Small companies who lack the funds to invest in the fastest internet bandwidth and speeds are the ones most impacted by this problem. To avoid this problem, a professional service will cooperate with you on scheduling or other matters.

**IV.SECURITY BREACHES IN CLOUD COMPUTING:**

Any uncovered danger or weakness in any system that might be exploited by hackers to compromise systems or data is a security concern. The computers and software used to link your company to clients, as well as your business's personnel and operations, are all vulnerable.

To a varied degree, almost every organisation has incorporated cloud computing into their operations. In such organization's cloud security plan must be prepared to defend against the main risks to cloud security issues, to utilize services of cloud.

Some of the security breaches in cloud computing are:

1. **Misconfiguration:**

A major factor in cloud data breaches are incorrect configurations in cloud security backgrounds. The strategies utilized by many organisations are to maintain their cloud safety measures are inadequate for protecting their cloud-based organization. This is influenced so many number of factors. Because cloud infrastructure is intended to be simple to use and facilitate quick data exchange, organisations find it challenging to guarantee that data is only available to authorized persons. As a result, organisations utilizing cloud-based infrastructure must rely on security measures offered by their cloud service provider to setup and safeguard their cloud installations. Additionally, organisations using cloud-based infrastructure also lack total visibility and control over their infrastructure. It is simple for a Misconfiguration or safety omissions to leave an organization’s cloud-based possessions exposed to assailants because many organizations are unaccustomed to protecting cloud infrastructure and frequently have multi-cloud organizations, each with a dissimilar set of vendor-provided safety controls.

1. **Inappropriate Access:**

In contrast to an organization's on-site infrastructure, its cloud-based deployments are external to the network perimeter and open to the general public. Although this makes the infrastructure more accessible to users and customers, it also makes it simpler for an attacker to access a company's cloud-based services without authorization. An attacker may be able to acquire direct access with the use of improperly configured security or compromised credentials, sometimes without the organization's awareness.

1. **Unsecure APIs and Interfaces:**

Application programming interfaces (APIs) and interfaces are frequently provided by CSPs to their clients. In an effort to make these interfaces simple for a CSP's clients to use, they are often well-documented.

However, if a client has not adequately protected the interfaces for their cloud-based infrastructure, this might present problems. A cybercriminal may also utilize the customer-designed documentation to find and leverage possible access and exfiltration techniques.

1. **Hijacking  Credentials:**

Password reuse and the usage of weak passwords are two common examples of poor password security practices. Because of this issue, phishing scams and data breaches are made to be even more damaging because a single stolen password may be used on several accounts. As organisations increasingly rely on cloud-based infrastructure and apps for critical business processes, account hijacking is one of the most significant cloud security challenges. While compromised client credentials allow complete control over their online account, an attacker with access to an employee's credentials can access important data or functionality. Additionally, organisations frequently struggle to recognize and counteract these risks in the cloud in the same way they do for on-premises equipment.

1. **Lack of Visibility:**

The infrastructure used by a company's cloud-based resources is not part of the corporate network and is placed outside of it. As a result, many conventional methods for attaining network visibility are ineffective in cloud systems, and some businesses lack security technologies that are specifically geared towards cloud environments. This may make it more difficult for an organisation to keep an eye on and defend against attacks on its cloud-based resources.

1. **External Data Sharing:**

Data sharing is made simple with the help of the cloud. Many clouds provide users the choice of sending an explicit email invitation to a collaborator or sending a link to a shared resource that anybody with the URL may access. Although this simple data exchange is a benefit, it can also pose a serious threat to cloud security. Controlling access to shared resources is challenging when link-based sharing is used, a common choice because it is simpler than individually inviting each intended collaborator. A cybercriminal may guess the shared link, give it to another person, or steal it as part of a cyber attack, giving them access to the shared resource without authorization. Furthermore, link-based sharing prevents access from being revoked for only one recipient of the shared link.

1. **Malicious  Insiders:**

For every organisation, insider threats are a serious security concern. An organization's network and some of the sensitive materials it holds are already accessible to a malevolent insider. Most attackers are discovered by their target during attempts to achieve this degree of access, making it challenging for an unprepared organisation to identify a dishonest insider. Finding a malevolent insider on the cloud is much more challenging. Because of the absence of control over the underlying infrastructure that comes with cloud deployments, many standard security solutions are ineffective. This makes it considerably more challenging to identify hostile insiders, especially with the fact that cloud-based infrastructure is readily accessible from the public Internet and frequently has security setup issues.

1. **Cyber attacks:**

Cybercriminals choose their targets based on the likelihood that their attacks will be profitable since cybercrime is a business. The public Internet may immediately access cloud-based infrastructure, which is frequently insecure and houses a lot of confidential and personal data. A successful assault may probably be performed many times with a high likelihood of success because the cloud is utilized by a wide variety of businesses. As a result, cloud installations within organisations are frequently the target of cyber attacks.

1. **Attacks on a Denial of Service:**

The capacity of many organisations to conduct business depends on the cloud. Business-critical data is stored there, and they use the cloud to operate crucial internal and client-facing apps.As a result, several firms are likely to be significantly impacted by a successful Denial of Service (DoS) assault against cloud infrastructure. DoS assaults that involve a ransom demand to end the attack thereby constitute a serious risk to an organization's cloud-based resources.

1. **Loss/Leakage of Data:**

Data saved in cloud-based systems may be shared easily. These settings allow for easy data exchange with third parties by direct email invites or by disseminating a public link to the data, and they are immediately accessible from the open Internet. Although a valuable asset and essential to cloud collaboration, the simplicity of data sharing raises substantial issues about data loss or leakage.

1. **Data Confidentiality and Privacy:**

For many organisations, data privacy and confidentiality are top priorities. The security of client data is mandated by data protection laws such as the EU's General Data security Regulation (GDPR), the Health Insurance Portability and Accessibility Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), and many more. Organisations also own a significant quantity of internal data that is crucial to preserving a competitive edge. Although moving this data to the cloud offers benefits, 66% of organisations have serious security concerns. Many businesses have embraced cloud computing, but many lack the skills to make sure that it is being used securely by both themselves and their staff. Sensitive data is therefore at danger of disclosure, as seen by the enormous number of cloud data breaches. [3]

**V. CLOUD CRYPTOGRAPHY:**

# Cryptography is the study and practice of techniques for secure communication in adverse conditions. It constructs and analyzes the protocols to prevent third parties or public from accessing secure messages. In cryptography, a plain text containing ordinary information is converted into cipher text containing secret information.

Cloud cryptography is the encryption used to protect data stored in the cloud. Several mechanisms are being used in cloud cryptography to add a high layer of security to secure data in order to prevent it from being infiltrated, hacked, or impacted by malware. Cloud encryption is a method of using codes to safeguard data and communication. Cloud data encryption may protect sensitive data and ensure asset transfer without slowing data transmission. To balance efficiency and security, several digital behemoths, like Google and Amazon, create cryptographic algorithms for cloud computing. Companies utilize many types of cryptographic keys for cloud security. Three algorithms are used to encrypt cloud data:

* Symmetric-key Algorithm
* Asymmetric key Algorithm

 &

* Hashing Algorithm
1. **Symmetric-Key Algorithm:** It employs a single key for both encryption and decoding. It requires little computer resources and performs exceedingly well in encryption. To ensure verification and approval, symmetrical algorithms use two-way keys. Except when the client possesses the key, the encoded data is stored in the Cloud and cannot be decrypted. Data encryption standard (DES), Blowfish, Advanced encryption standard, Triple DES, and other well-known symmetric algorithms are employed in cloud computing methods.
	* **Advanced Encryption Standard (AES)** - This standard is used to encrypt digital data in industries such as telecommunications, finance, and government. The same key is utilized for both encryption and decryption in AES. It is a block of cipher text that repeatedly repeats itself after each stated step. It features a block size of 128 bits and key sizes of 128, 192, and 256 bits. It is both software and hardware efficient.
	* **Data Encryption Standard (DES)** - It uses a 64-bit secret key, 56 bits of which are generated at random and the remaining 8 bits are utilized for error detection. DES is implemented in hardware and is mostly used for single-user encryption, such as encrypted contents saved on a hard disc.
2. **Asymmetric-Key Algorithm:** It employs many keys for encryption and decoding. Every beneficiary in this case requires a decoding key. This is known as the recipient's private key. The encryption key in this case belongs to a specific person or business. This type of method is said to be the most secure since it requires both keys to access a piece of explicit data.
	* **RSA Rivest Shamir Adleman Algorithm** - It is a de facto encryption standard that is utilized on a number of platforms. It employed distinct keys for encryption and decryption.
	* **Elliptic Curve encryption (ECC)** - ECC is a contemporary public-key encryption that generates a small key using number theory and mathematical elliptic curves. Because to its short key size, ECC is favoured by security experts.
3. **Hashing**: It is a critical component of block chain security. Data is stored in blocks on the blockchain and is linked together using cryptographic standards such as a string or chain. When an information block is added to the chain, a unique code or hash is issued to it. Hashing is primarily used to arrange and retrieve items in a data collection. It also employs two separate keys for encrypting and decoding messages. It also allows for faster information retrieval.

# The security of cloud data contains securing an organization’s data in a cloud environment where the data is located. Most organizations contain massive amounts of data ranging from confidential information to organization’s own information shared among employees. Also, lot of data is moved to the cloud and stored in multiple places. Securing cloud data will secure applications and data across multiple platforms, identify and mitigate risks and prevents data loss and disruption. In this paper, data privacy protection is discussed using ecc.ecc is more secured as it has shorter key lengths with optimal security.ECC stands for Elliptic Curve Cryptography.ECC are based on algebraic structure of elliptic curves. It allows smaller key to provide security. An elliptic curve is plane curve. Elliptic curves are applicable for [key agreement](https://en.wikipedia.org/wiki/Key_agreement), [digital signatures](https://en.wikipedia.org/wiki/Digital_signature), [pseudo-random generators](https://en.wikipedia.org/wiki/Cryptographically_secure_pseudorandom_number_generator) ECC creates faster, smaller and efficient cryptographic keys.

The reason behind using ECC is that:

1. It provides security using fewer bits.
2. It requires smaller chip size, less power consumption and increase in speed.[4]

**VI. APPLICATIONS OF ECC ALGORITHM IN CLOUD:**

There is lot of Cryptographic Algorithms to perform Asymmetric Key Generation for Encryption and Decryption.ECC provides Tighter Encryption Technique.ECC algorithm has four-step procedure to provide cloud security. It includes generation of connection, creation of account, authentication and exchange of data.



**Fig iii) A Four Step Procedure in Elliptic Curve Cryptography Algorithm**

ECC is an asymmetric key cryptosystem in which each user has one pair of private and public keys. For every prime number q or integer that can be written in terms of 2ˆn, let Equation (a, b) be the elliptic curve with parameters a, b, and q. G is an elliptic curve point that is satisfied for a big value of n. Figure iii) depicts the processes involved in the ECC algorithm in a four step procedure. [5]

# VII. RELATED WORK:

# In investigation on cloud computing system providers is implemented for security and privacy issues. So, adoption of released acts for new scenarios in cloud will make new users to switch to cloud environment. Privacy protection of cloud and data security in cloud is reviewed and analyzed systematically in the proposed model. A framework of privacy protection is proposed and basic ABE, KP-ABE and CP-ABE encryptions are also proposed. Lastly, privacy protection laws are proposed for technical deficiencies. A model based on ECC is projected to provide efficient data security in the proposed framework. [6]

# VIII. THE PROPOSED METHODOLOGY:



**Fig iv) The Proposed Methodology**

* 1. **Proposed System:** The cloud computing is a virtual world which enables exchange of confidential data. Therefore, several data storage security breaches are possible. Since it is a part of virtual cloud the users will not be able to identify the location of the data to even secure it. However it is a challenge to address the virtualcloud.ECC offers faster speed of execution. It generally uses small keys. Elliptic curves keys can be defined over real values, prime numbers or over GF. We have considered the proposed ECC into three parts which involves [7]
* Key Generation
* Encryption Algorithm
* Decryption Algorithm

# Key generation:

For any effective cryptographic algorithms the most effective part is the generation of keys. ECC system has effective key generation mechanism. Generally every cryptographic algorithm generates a public and private key. The user A which sends the data should encrypt its data with one of the keys and the user B receiving the data should decrypt using the agreed key. It is therefore necessary to note that even before the data is encrypted, Key generation should be done. This process can be implemented between the Cloud service provider and the user for effective cryptographic key generation. Elliptic curve generates smaller keys and this provides saving of energy wide and large in a cloud system. To generate a key ECC uses either one of these,[8]

* Using real values
* Using prime numbers
* Using finite field values.

These keys are generally smaller in size and hence the computational process and power are quite easy to operate.ECC also exhibits the group properties.ECC curves also forms abelian group under addition which helps in generating smaller keys.

# Elliptic curves over real values

Cubic equations are formed using the real values. For example, Let us consider z2=a3+xa+y. This equation can be used to generate keys using cryptographic calculations. Consider z=−$\frac{-b\pm \sqrt{b^{2}-4ac}}{2a}$ and z gives positive and negative values which are produced by z. ECC follows certain addition rules like if there is a given Elliptic curve and if three points are joined by straight line then their sum will be zero.

Zero acts as an identity element. If p is a point the p+0=p. Suppose if p is a point then p=(Ax, By) and negative point will be -p(ax,by). Let us consider two points g & h which has different x coordinates and we can calculate the intersection of those two points to get the third point.[9]

* + - 1. **Elliptic Curves over prime numbers**

These curves are also called as prime curve. In the prime method cubic curves have all values from 0 to p-1. The equation to be obtained would be a2modp=$(\frac{-b\pm \sqrt{b^{2}-4ac}}{2a}$)modp. Ifp+0=p which follows identity rules then we assume that p=(Ax,By)for the same a coordinate. And we get -p(Ax,By) where p+(-p) will be equated to zero.[10]

# Elliptic Curves Over Finite Field (GF)

# These curves are also called as GF curves or finite field curves and the calculations obtained are a2+bc=b3+xb2+b. If p+0=p identity rule is implemented then p=(ax,by) and -p=(ax,ax+by).[11]

# Encryption Algorithm:

**Step 1:** Suppose Cloud user X wants to send data to Y.

**Step2:** X takes plain text message and encodes it onto a point, p using any one of the keys from the elliptic group.

**Step 3:** X computes the following, Cm= {N M,Pk+NPy} Where, N is a random integer of user choice, M is a point on the curve (one of the curves), P is the point, NPy is the key used by x from y.

**Step 4:** The cipher text is thus obtained.

**Step 5:** Send cipher text Cmto cloud Y.

* + 1. **Decryption Algorithm:**

 **Step 1:** Cloud Y will take the following steps to decrypt the cipher text.

#  Step 2: Y will compute the following:

#  Pk = Pk + NPy - Ay \* N \* M

#  Pk = N (Ay \* M) – Ay \* N \* G which gives the pk.

#  Step 3: B cloud then decodes pk to get the original message.

**IX .RESULTS & DISCUSSION:**

To implement the ECC system in Cloud environment we need a minimum requirement of system with a configuration appropriately like Windows 7 operating system with 4 GB RAM and 2.6 GHz processor and for better efficiency we require a windows 10 OS. The following table shows the efficiency of the elliptic curve cryptographic system. [12]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Key Size** | **File Size(KB)** | **File Mode** | **Key generation time (s)** | **Encryption Time (s)** | **Decryption Time (s)** |
| 489 | 100 | Jpeg | 0.1 | 0.7 | 0.25 |
| 584 | 200 | Pdf | 0.3 | 1.3 | 0.7 |
| 697 | 300 | Gif | 0.55 | 2.7 | 2 |
| 874 | 400 | png | 1.1 | 5 | 3 |
| 489 | 500 | png | 0.1 | 0.7 | 0.25 |

 **Table 1: ECC Performance**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Key Size** | **File Size(KB)** | **File Mode** | **Key generation time (s)** | **Encryption Time (s)** | **Decryption Time (s)** |
| 165 | 100 | Jpeg | 0.06 | 1.5 | 0.3 |
| 230 | 200 | Pdf | 0.20 | 2 | 0.5 |
| 270 | 300 | Gif | 0.30 | 4.1 | 1.2 |
| 400 | 400 | Png | 0.60 | 5.2 | 2 |
| 489 | 500 | png | 1.1 | 6 | 2.1 |

 **Table 2: AES Performance**

In this graph, ECC and AES cryptographic algorithms are compared for Key Generation Time which is measured in seconds. In case of ECC, the key generation time is increasing slowly. The curve is linear from the key size of 165 KB to 230 KB from key generation time of 0 second to 0.2 second. Then, the curve increases slowly from key size of 230 KB to 270 KB. [13][14]The curve takes a sharp increase after 270 KB to 400 KB of key size which increases key generation time to 0.4 second. This increase in curve continues till 400 KB of key size. The curve keeps on increasing as the key size increases further which increases key generation time. In case of AES, the curve makes steady increase initially. The curve takes sudden increase from 697 KB key size which increases key generation time.[15]

****

**Fig v) Encryption Algorithm**

ECC and AES cryptographic algorithms are compared with respect to Encryption Algorithm with the help of graph. In case of ECC, the curve is increasing slowly in linear fashion from key size 165 KB to 230 KB. With the increase in key size, encryption will take longer time to encrypt data. The curve remains con constant for key size from 230 KB to 270 KB. After 270 KB, the curve starts increasing steadily which increases encryption time also. In case of AES, initially the curve increases steadily from 489 KB to 584 KB of key size and takes sharp increase from key size of 584 KB to 697 KB. Further, the curve increases from 697 KB of key size rapidly.[16]

****

**Fig vi) Decryption Algorithm**

Here, ECC and AES encryption algorithms are compared with respect to decryption algorithm. In case of ECC, the curve is increasing slowly from key size of 165 KB to 489 KB. So, decryption is slower with increase in key size. In case of AES, the curve starts increasing from key size of 489 KB to 584 KB. Suddenly, the curve takes steep increase in the graph. It shows that with the increase in key sizes the decryption time is more in AES than in ECC.[17][18]

**X. CONCLUSION:**

No matter how tech-savvy the user is, IT-related services like cloud computing offer effective services. Regardless of the user's location, data can be easily saved, maintained, upgraded, and retrieved through a cloud interface offered by independent cloud service providers via the Internet. Numerous features are available to users of cloud services. According to the type of cloud service, users are those who use the services. In addition to being advantageous for so many customers to access their data from wherever, services are offered at minimal cost. Since you don't need to bring your device with you, cloud services can be made available on any system. The low data security of cloud services, meanwhile, is a disadvantage that can be overcome and must be protected. ECC is utilized to simplify the activities, specifically for the production of the key. ECC's enhancement is substantially superior than other cryptographic methods because to its small key size. The optimization and security of the data can be greatly improved when AES is used in conjunction with ECC. In this paper, cloud data is protected using ECC which is highly secured to protect the data. Also, ECC is compared with AES algorithm in terms of Key Generation, Encryption and Decryption which is better than AES.

**XI. FUTURE SCOPE:**

In order to develop the idea of cloud computing through cryptographic methods in the future, much security is still required. Future research can be strengthened by enhancing the hybrid approach's security. To increase the system's effectiveness and productivity, multiple security levels might be introduced. This paper will be further implemented to secure real time data. Also, a stronger algorithm will be implemented to provide more security to data.

**XII. REFERENCES:**

[1] https://www.interviewbit.com/blog/cloud-computing-architecture/

[2] https://www.javatpoint.com/hybrid-cloud

[3]https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/

[4] https://peoplactive.com/blog/cryptography-in-cloud-computing/

[5] Purna Chandra Sethi, Neelima Sahu,Prafulla Kumar Behera, Group security using ECC, Bharati Vidyapeeth’s Institute of Computer Applications and Management 2021,PP 955-963,Springer Publications. DOI: 10.1007/s41870-021-00613-1.

[6] Dr. M. Gobi, Karthik Sundararaj, A Secured Cloud Using Elliptic Curve Cryptography, Proceedings of the

UGC Sponsored National Conference on Advanced Networking and Applications, 27th March 2015,pp.141-144.

[7] PAN JUN SUN, Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and

Solutions, Volume 7, 2019, National Development and Reform Commission, Information Security Special

Project, Development and Reform Office.

[8] [Minqi Zhou](https://ieeexplore.ieee.org/author/37592164100), [Rong Zhang](https://ieeexplore.ieee.org/author/37069921600), [Wei Xie](https://ieeexplore.ieee.org/author/37591633400), [Weining Qian](https://ieeexplore.ieee.org/author/37416694800), [Aoying Zhou](https://ieeexplore.ieee.org/author/37266730700), Security and Privacy in Cloud Computing: A Survey, Software Engineering Institute, East China Jiao Tong University, Shanghai, China, 2010.

[9] G Prasanna , Dr.K.Ramesh Reddy, Y. Sreevaishnavi, Secure Privacy Preserving Schema Using ECC By

Holomorphic Algorithm for BAN and Data Storage in Cloud, European Journal of Molecular & Clinical

Medicine, 2020.

[10] Ashima Narang, Gupta Deepali, Comparative Analysis of Various Cloud Security Frameworks, ICCS, 2018.

 [11] R.Sridevi, R.Rahini priyadharshini, Cloud security using Searching of Cloud data using KNN, IJARSET, 2016.

[12] Saba Rehman, Nida T. Bajwa, AES-ECC Model Security of Data over Cloud Storage Electronics, 2021.

[13] A.Priya, Implementation of hybrid cryptographic schemes in a cloud environment for enhanced medical

data security, IJNAA,2021.

[14] J.Athena,V.Sumathy, Survey on Public Key Cryptography Scheme for Securing Data in Cloud Computing, Circuits and Systems,2017.

[15] S.Hendry Leo Kanickam,L.Jayasimman, Comparative Analysis of Hash Authentication Algorithms and ECC Based Security Algorithms in Cloud Data,2019.

[16] Orobosade,Thompson Aderonke Favour-Bethy,Alese Boniface Kayode,Arome J. Gabriel,Cloud Application Security using Hybrid Encryption CAE,2020.

[17] Ijaz Ahmad Awan, Muhammad Shiraz, Muhammad Usman Hashmi,Qaisar Rizwan Akhtar,Allah Ditta, Secure Framework Enhancing AES Algorithm in Cloud Computing, Hindawi Security and Communication

Networks,2020.

[18] Sanjeev Kumar,[Haider Banka](https://onlinelibrary.wiley.com/action/doSearch?ContribAuthorRaw=Banka%2C+Haider),[BaijnathKaushik](https://onlinelibrary.wiley.com/action/doSearch?ContribAuthorRaw=Kaushik%2C+Baijnath),[Surbhi Sharma](https://onlinelibrary.wiley.com/action/doSearch?ContribAuthorRaw=Sharma%2C+Surbhi),A review and analysis of secure and lightweight ECC-based RFID authentication protocol for Internet of Vehicles, Emerging Telecommunications Technologies,2021.