JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

ENHANCED SECURITY USING ELLIPTIC CURVE CRYPTOGRAPHY IN CLOUD

[1]B.Sai Deepthi, [2]M. Sreenivasu, [3]P P S V V Yaswanth Siva Kumar, [4]Manda Jeevan, [5]Kantamaneni Vijay Kumar, [6]Nuka Ramesh

[1]Assistant Professor, [2]Associate Professor, [3]UG Student, [4]UG Student, [5]UG Student,[6]UG Student

Department of Information Technology,
GIET Engineering College, Rajamahendravaram, Andhra Pradesh,India

Abstract : **Cloud computing is one of today's hottest research areas due to its ability to reduce costs associated with computing while increasing scalability and flexibility for computing services. Cloud computing is Internet based computing due to shared resources, software and information are provided to consumers on demand dynamically. Cloud computing is one of the fastest growing technologies of the IT trade for business. Since cloud computing shares disseminated resources via the network in the open environment, hence it makes security problems vital for us to develop the cloud computing applications. Cloud computing security has become the leading cause of hampering its development. Cloud computing security has become a hot topic in industry and academic research. This paper will explore data security of the cloud in cloud computing by implementing encryption with elliptic curve cryptography.**

Keywords: Scalability, Flexibility, Internet-based computing, Shared resources, On-demand services, Fastest growing technology, IT trade, Security, Disseminated resources, Network.

1. INTRODUCTION

A cloud typically contains a virtualized significant pool of computing resources, which could be reallocated to different purposes within short time frames. The entire process of requesting and receiving resources is typically automated and is completed in minutes. The cloud in cloud computing is the set of hardware, software, networks, storage, services and interfaces that combine to deliver aspects of computing as a service. Share resources, software and information are provided to computers and other devices on demand. It allows people to do things they want to do on a computer without the need for them to buy and build an IT infrastructure or to understand the underlying technology. Through cloud computing clients can access standardized IT resources to deploy new applications, services or computing resources quickly without reengineering their entire infrastructure, hence making it dynamic. The core concept of cloud computing is reducing the processing burden on the user's terminal by constantly improving the handling ability of the cloud. All of this is available through a simple internet connection using a standard browser. However there still exist many problems in cloud computing today, a recent survey shows that data security and privacy risks have become the primary concern for people to shift to cloud computing.

2. Literature Survey

2.1 Research of Cloud Computing Data Security Technology

With cloud computing applications and research at home and abroad continuing to advance cloud computing platforms for users and data exchange between the greater the amount of user data transmission and storage a security threat, a cloud computing security is an important issue to be resolved. In this paper, all with state of encryption technology, presents cloud computing data security solutions, both to ensure safe transmission of data to ensure the security of static data.

2.2 An Efficient Method to Prevent Information Leakage in Cloud

Cloud Computing is storing and accessing data and programs over the Internet instead of personal computers. It is a computing paradigm shift where computing is moved away from personal computers or an individual server to a cloud of computers. Its flexibility, cost-effectiveness, and dynamically re-allocation of resources as per demand make it desirable. As desirable as it is, it has also created security challenges such as information leakage, account hijacking and denial of service. The proposed work is to develop a Software as a Service application to prevent information leakage by providing multi factor authentication, risk assessment, encryption using enhanced elliptic curve cryptography where a cryptographically secure random number generation is used to make the number unpredictable, data integrity, key management and secure disposal of information. The platform for deployment of the application is Google App Engine.

2.3 Enhancing Security of Cloud Computing using Elliptic Curve Cryptography

Cloud computing is a form of distributed computing environment. It provides an environment where thousands of computers work in parallel to perform a job in much less time than the traditional client server model. This parallelism happens because of low cost virtualization of hardware resources. Cloud computing abstracts the complexity of services provided to the user. In this article we have tried to explore various cloud computing models and how their security requirements differ from traditional computing models. We have analyzed various security risks associated with them, different ways to mitigate them and limitations of current cryptographic schemes. We have analyzed elliptic curve cryptographic schemes for cloud based applications in comparison to RSA based schemes. Here we have tried to give theoretical and experimental results to prove that elliptic curve based public key cryptography is far better than RSA based schemes. We have implemented ecdsa algorithm and compared its performance with RSA based algorithm in the cloud. It supports our conclusion from the survey of cloud based applications.

2.4 The Comprehensive Approach for Data Security in Cloud Computing

Survey Cloud Computing is becoming the next stage platform in the evolution of the internet. It provides the customer an enhanced and efficient way to store data in the cloud with different range of capabilities and applications. The data in the cloud is stored by the service provider. Service provider capable and having a technique to protect their client data to ensure security and to prevent the data from disclosure by unauthorized users. This paper will give a descriptive knowledge regarding cloud computing privacy and security issues provided by encryption and decryption services. If a cloud system is performing a task of storage of data and encryption and decryption of data on the same cloud then there are much more chances of getting access to the confidential data without authorization. This increases the risk factor in terms of security and privacy. This paper proposes a business model for cloud computing which focuses on separating the encryption and decryption service, from the storage service provided by the service provider. I mean that both encryption and decryption of the data can be performed at two distinct places. For studying this proposal are using a business model named as CRM (customer relationship model) for an example. For the evaluation of effective and efficient technique of data storage and retrieval we are providing three clouds separately such as including encryption and decryption services, secondly storage and a CRM application system. In this Research paper, we have tried to access separate encryption and decryption services using RSA algorithm and computing is a paradigm in which information is stored in servers on the internet. That information retrieved by the client as per usage. For this manner, we provide a solution for data security, confidentiality and privacy based on a concept of separate encryption and decryption service.

2.5 Enhanced Security Architecture for Cloud Data Security

Cloud computing offers a prominent service for data storage known as cloud storage. The flow and storage of data on the cloud environment in plain text format may be the main security threat. So, it is the responsibility of cloud service providers to ensure privacy and security of data on storage as well as network level. The following three parameters confidentiality, integrity and availability decide whether security and privacy of data stored on a cloud environment is maintained or not. The proposed work is to define cloud architecture with configured samba storage and cryptographic encryption techniques. The cloud architecture deployed with samba storage uses an operating system feature specifying permission values for three attributes (User/Owner, Group and Global) and maps it to a cryptographic application which performs cryptographic operations. Cryptography application supports symmetric and asymmetric encryption algorithms to encrypt/decrypt data for uploading/downloading within cloud storage.

3. OVERVIEW OF THE SYSTEM

3.1 Existing system

Many of these challenges should be addressed through management initiatives. These management initiatives will require clearly delineating the ownership and responsibility roles of both the cloud provider and the organization functioning in the role of customer. Security managers must be able to determine what detective and preventive controls exist to clearly define the security posture of the organization. Although proper security controls must be implemented based on asset, threat, and vulnerability risk assessment matrices. Cloud computing security risk assessment report mainly from the vendor's point of view about security capabilities analyzed security risks faced by the cloud.

3.1.1 Disadvantages Of Existing System:

Security managers must be able to determine what detective and preventive controls exist to clearly define the security posture of the organization.

3.2 Proposed system

All existing algorithms require large size of keys generation and management which took heavy computation time and resources which may increase cloud usage cost and to overcome from this problem ECC (elliptic curve cryptography) algorithm is introduce which is lighter to generate keys and take less computation time and resources to encrypt or decrypt data. The Cloud Computing systems that provide services to the Internet users apply the public key and private or traditional identity based cryptography that has some identity elements that fit well in the requirements of cloud computing. This work aims at improving cloud computing within Cloud Organizations with encryption awareness based on Elliptic Curve Cryptography. The need to access cloud storage on thin clients and mobile devices is becoming an emerging application. Security of stored data and data in transit may be a concern when storing sensitive data at a cloud storage provider.

3.3 Software Requirements:

- Python idle 3.7 version (or)
- Anaconda 3.7 (or)
- Jupiter (or)
- Google colab

3.4 Hardware Requirements:

- Operating System: Windows, Linux
- Processor : Minimum Intel I3
- Ram : Minimum 4 Gb
- Hard Disk : Minimum 250gb

4. Technologies Used

4.1 Cloud computing

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers. The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games. Cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

4.2 Services Models

Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layers are completed by an end user layer that encapsulates the end user perspective on cloud services. The model is shown in figure below. If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider.

- Price: Pay for only the resources used.
- Security: Cloud instances are isolated in the network from other instances for improved security.
- Performance: Instances can be added instantly for improved performance. Clients have access to the total resources of the Cloud's core hardware.

- Scalability: Auto-deploy cloud instances when needed.
- Uptime: Uses multiple servers for maximum redundancies. In case of server failure, instances can be automatically created on another server.
- Control: Able to login from any location. Server snapshot and a software library lets you deploy custom instances.
- Traffic: Deals with spike in traffic with quick deployment of additional instances to handle the load.

4.3 Python

Programmers have to type relatively less and the indentation requirement of the language makes them readable all the time. Python language is being used by almost all tech-giant companies like – Google, Amazon, Facebook, Instagram, Dropbox, Uber… etc.
The biggest strength of Python is huge collection of standard library which can be used for the following –

- Machine Learning
- GUI(Graphical User Interface) Applications (like Kivy, Tkinter, PyQt etc.)
- Web frameworks like Django (used by YouTube, Instagram, Dropbox)
- Image processing (like Opencv, Pillow)
- Web scraping (like Scrapy, BeautifulSoup, Selenium)
- Test frameworks
- Multimedia

Python downloads with an extensive library and it contains code for various purposes like regular expressions, documentation-generation, unit-testing, web browsers, threading, databases, CGI, email, image manipulation, and more. So, we don't have to write the complete code for that manually.
1. Less Coding - Almost all of the tasks done in Python require less coding when the same task is done in other languages. Python also has an awesome standard library support, so you don't have to search for any third-party libraries to get your job done. This is the reason that many people suggest learning Python to beginners.
2. Affordable - Python is free therefore individuals, small companies or big organizations can leverage the free available resources to build applications. Python is popular and widely used so it gives you better community support.
3. Python is for Everyone - Python code can run on any machine whether it is Linux, Mac or Windows. Programmers need to learn different languages for different jobs but with Python, you can professionally build web apps, perform data analysis and machine learning, automate things, do web scraping and also build games and powerful visualizations. It is an all-rounder programming language.

4.4 System Design

The DFD is also called a bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system. The Data Flow Diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.

Economical Feasibility:

This study is carried out to check the economic impact that the system will have on the organization. The amount of funds that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

Technical Feasibility:

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

Social Feasibility:

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

5. Architecture

Cloud Server:

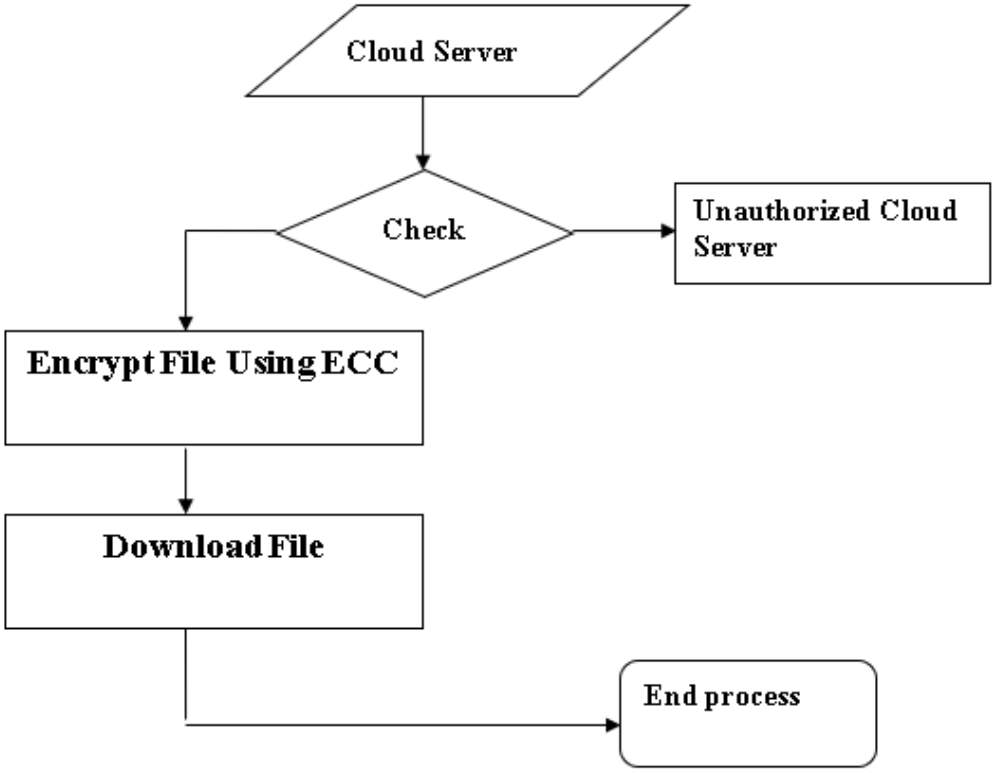

Fig 1: System Architecture

6. RESULTS SCREENSHOTS

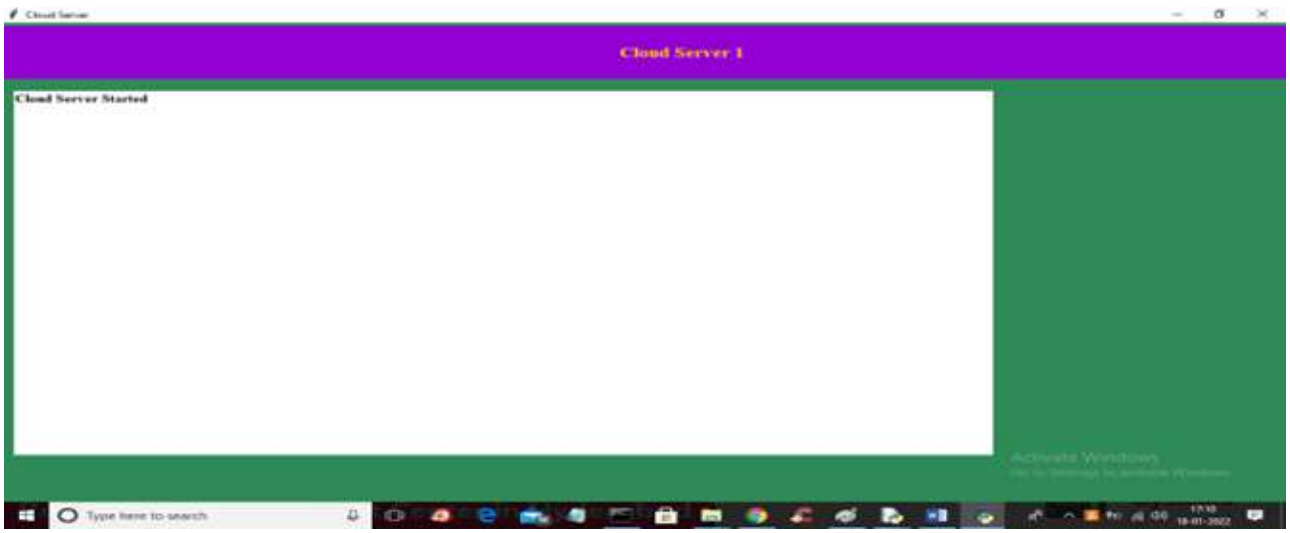

Fig 2: Cloud Server

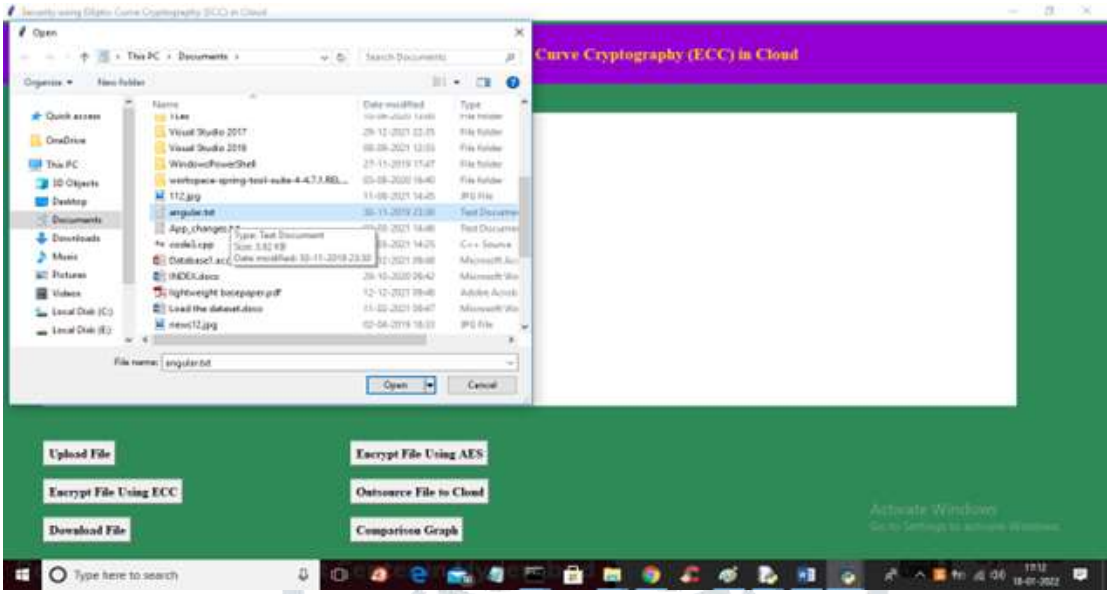

Fig 3:Upload Filet

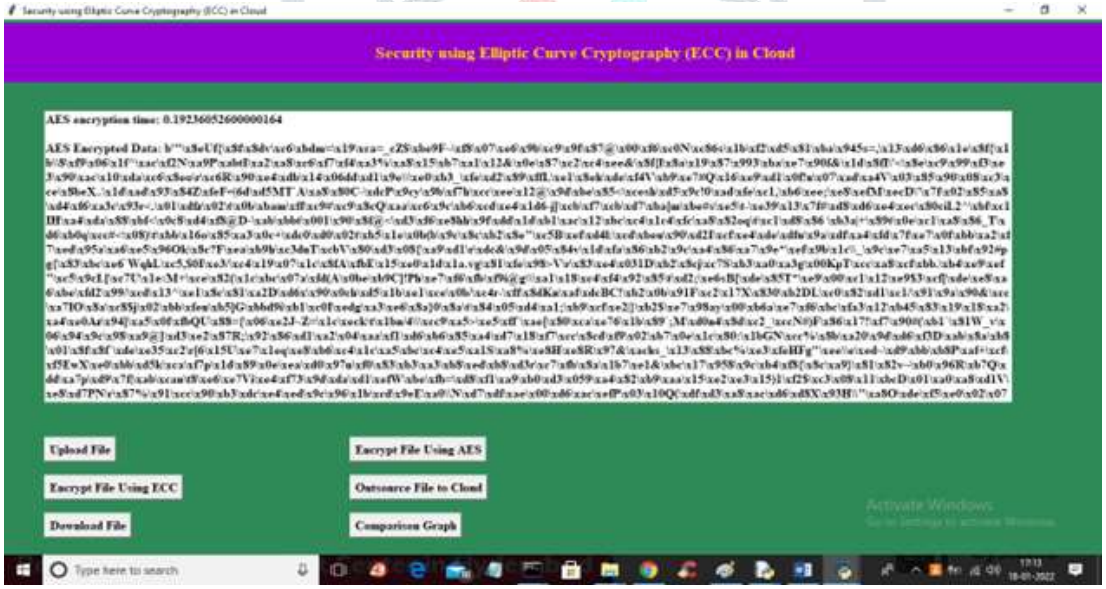

Fig 4: Encryption

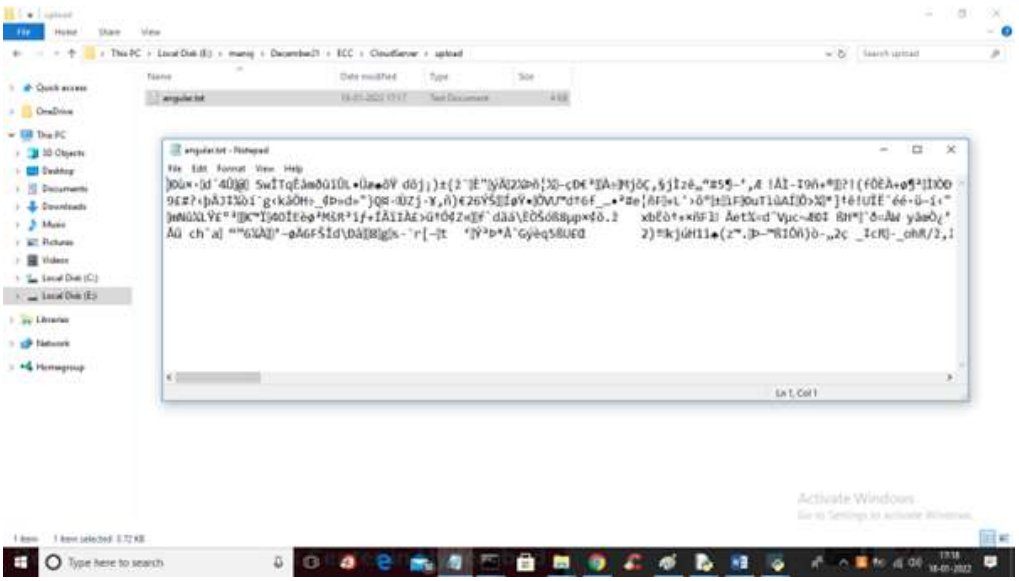

Fig5: File Saved In Encryption format

7. CONCLUSION

Cloud Computing provides a platform with an enhanced and efficient way to store data in the cloud. The functioning of Cloud Computing is significantly distressed by issues such as that of data security, integrity, theft, loss and presence of infected applications. These issues are the major disadvantages to the consumer to move their data to the cloud. This paper proposed a model using Elliptic Curve Cryptography to enable more efficient data security in cloud computing. Here, Security is based on the difficulty of computing discrete logarithm in a finite field. AES and ECC are forms of public key cryptography, in which one decryption key, known as the private key, is kept secret, while another, known as a public key, is freely distributed. Public key cryptography is computationally more expensive than private key encryption, which employs a single, shared encryption key. By using the proposed algorithm, Cloud computing can achieve a higher level of security than the security attained by the IT enterprises with their own hardware and software.

8. FUTURE ENHANCEMENT

Cloud Computing offers an advanced platform for efficient data storage, yet it faces significant challenges concerning data security, integrity, and privacy. The adoption of Cloud Computing by consumers is often hindered by concerns regarding the vulnerability of their data to theft, loss, or compromise by malicious applications. To address these challenges, this paper proposes a novel model leveraging Elliptic Curve Cryptography (ECC) to enhance data security in Cloud Computing environments. Elliptic Curve Cryptography offers a robust security mechanism based on the computational complexity of discrete logarithm calculations in finite fields. By incorporating ECC alongside established encryption techniques like AES, Cloud Computing platforms can fortify their security posture. AES and ECC, both forms of public key cryptography, ensure secure communication by employing asymmetric encryption, where a private key is kept secret while a public key is freely distributed. Although public key cryptography is computationally more intensive than traditional private key encryption, its adoption ensures a higher level of security for cloud-based data. Through the adoption of the proposed algorithm, Cloud Computing can achieve a heightened level of security compared to traditional IT infrastructure. This heightened security not only safeguards sensitive data but also instills confidence in consumers regarding the integrity and confidentiality of their information stored in the cloud. Ultimately, by embracing innovative security measures like Elliptic Curve Cryptography, Cloud Computing can overcome existing security challenges and continue to evolve as a trusted and reliable technology solution for businesses and individuals alike

9. REFERENCES

[1] AbhudayTripathi, and ParulYadav, Enhancing Security of Cloud Computing using Elliptic Curve Cryptography, International Journal of Computer Applications, 57(1), 2012, 0975-8887.

[2] Nilesh N. Kumbhar, Virendrasingh V. Chaudhari, and MohitA.Badhe, The Comprehensive Approach for Data Security in Cloud Computing: A Survey, International Journal of Computer Applications, 39(18), 2012, 0975-8887.

[3] N. Koblitz, Elliptic Curve Cryptosystems, Mathematics of Computation, 1987.

[4] Yubo Tan, and Xinlei Wang, Research of Cloud Computing Data Security Technology, 978-1-4577- 1415-3/12,IEEE 2012.

[5] YashpalsinhJadeja, and KiritModi, Cloud Computing - Concepts, Architecture and Challenges, International Conference on Computing, Electronics and Electrical Technologies,4(12), 2012, 978-1-4673-0210

[6] Dr. Chander Kant, and Yogesh Sharma, Enhanced Security Architecture for Cloud Data Security, International Journal of Advanced Research in Computer Science and Software Engineering, 3(5), 2013.

[7] Wayne Jansen, and Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing, National Institute of Standards and Technology, U.S. Department of Commerce, 800-144.

[8] VeerrajuGampala, Data Security in Cloud Computing With Elliptic Curve Cryptography, International Journal of Soft Computing and Engineering (IJSCE), 2, 2012.

[9] Dai Yuefa, Wu Bo, GuYaqiang, Zhang Quan, and Tang Chaojing, Data Security Model for Cloud Computing, Proc. International Workshop on Information Security and Application. Qingdao, China, 2009, 978-952-5726-06-0.

[10] IkshwansuNautiyal, and Madhu Sharma, Encryption Using Elliptic Curve Cryptography Using Java as Implementation Tool, International Journal of Advanced Research in Computer Science and Software Engineering, 4(1), 2014. [11] Vidyanand K\Ukey, and Nitin Mishra, Dataset Segmentation for Cloud Computing and Securing Data Using ECC, International Journal of Computer Science and Information Technologies, 5(3), 2014, 4210-4213.

[11] R. BalaChandar, and M. S. Kavitha, A Proficient Model For High End Security in Cloud Computing, ICTACT Journal of Soft Computing, 04(02), 2014.

[12] Nina Pearl Doe, and Sumaila Alfa, An Efficient Method to Prevent Information Leakage in Cloud, IOSR Journal of Computer Engineering (IOSR-JCE) 16(3), 2014, 2278-8727.

[13] NehaTirthani, and Ganesan R, Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography, International Association for Cryptologic Research Cryptology ePrint 49, 2014