ISSN:0975-9646

Akash Shrivastava et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015, 1669-1671

Reliable Cloud Using elliptical Curve Deffie Hellman and Elliptical Curve Digital Signature

Akash Shrivastava, Nitya M Nerli

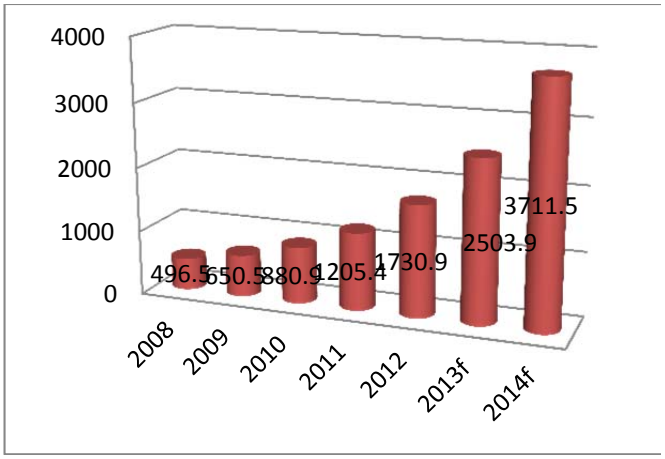
CSE Dept.
DIT University, Dehradun, INDIA

***Abstract*- Cloud has gained grounds in the organizations making computing much easy. Cloud technology has become the most talked research areas. Most of which is related to the security of the system. Cloud has been used extensively and it is the prime issue of how secure this computation is.**

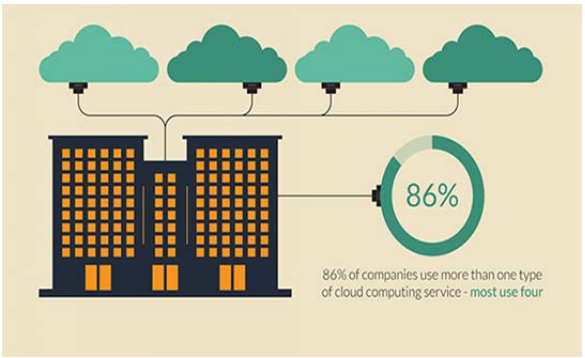
***Keywords*-cloud computing, concept of cloud, challenges, elliptical curve cryptography.**

I. INTRODUCTION

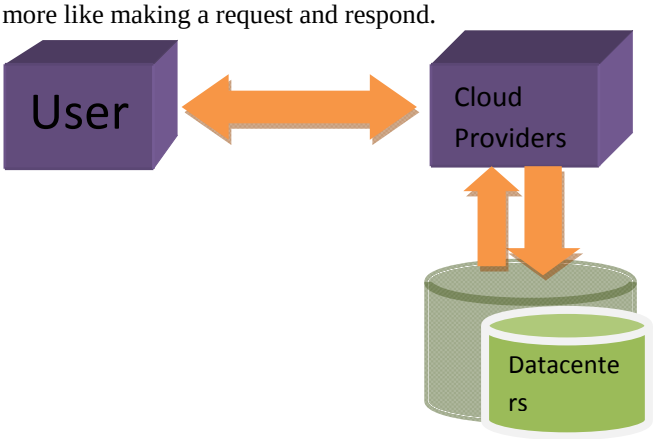
Cloud Computing has become one of the hottest research topics due to its ability in reducing costs and associated computing .As organizations are always in pursuit to gaining more secure most of them are find cloud computing more helpful. According to the study cloud has shown development over the years .The statistics also show a rise in the use of this technology.



Here is a graph that shows the Market size of the Cloud Computing Industry (Globally) over 7 years.
More over the 86% of companies use more than one cloud computing services. Some use even more.



With such massive access to the technology it becomes more important to have a rain check on all the factors of cloud. This includes the infrastructure, the network, the storage and the security. These need task force to maintain this technology.
A cloud typically is a virtualized pool of computing resources, which could be used for different purposes in different places with limited frames.th entire process, is more like making a request and respond.



Cloud allows the people to compute without the need to actually buy the entire IT infrastructure or even understand the underlined technology that is put in use. Understanding the core complexes of cloud computing is most interesting, all the burden is handled on the user terminal by constantly improvising the technology, increasing the applicability and increasing its basic ability.
However, the study continues as there lay many loop holes in regards to the security of this technology, hence working on the ground zero is must.
Cloud allows the people to compute without the need to actually buy the entire IT infrastructure or even understand the underlined technology that is put in use. Understanding the core complexes of cloud computing is most interesting, all the burden is handled on the user terminal by constantly improvising the technology, increasing the applicability and increasing its basic ability.
However, the study continues as there lay many loop holes in regards to the security of this technology, hence working on the ground zero is must.

II. CONCEPTS OF CLOUD

There are four basic group models (Deployment Models) for the specific purpose.

- Public cloud: the cloud infrastructure that is made available to the public is called as the Public cloud. Based on the standards of generalized cloud

computing model and architecture in which the service provider provides services like application and storage .These are generally free or sometimes even they prefer the pay-per-usage.
Benefits of using public cloud: Easy and inexpensible, Scalability and no wasted resources as you pay for what you use.
Examples: Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google AppEngine and Windows Azure Service provider.

- Private Cloud: a cloud that is opened solely to a particular cliental. The main advantage of having a private cloud is Security compliance and Quality of Service (QoS).
  These clouds are basically customized according to the needs and requirements of the client. Private cloud computes basic power-as-a-Service (PoaaS).
- Community Cloud: A cloud that is shared with multiple organizations. The infrastructure is such that many organizational groups can access the resources .The organizations outside the group are forbidden to uses the services. Most likely this helps in providing the organization the security and compliance considerations.
  Community clouds can be thought of as subset of public clouds that are tailored to a specific vertical industry, such as government, healthcare or finance, offering a range of services, including infrastructure, software or platform as a service. The National Institute for Standards in Technology defines them as being "an infrastructure shared by several organizations that supports a specific community that has shared concerns."
  ~ By Brandon Butler, Network World | Mar 1, 2012 [3]
  International Game Technology, a vendor of computerized game technology, recently launched its IGT Cloud, aimed specifically at gaming companies. It uses the AppLogic cloud computing platform from CA Technologies to provide cloud-based SaaS offerings for casinos to better manage their games.

III. CLOUD SECURITY CHALLENGES

Privileged user access: the Inherent level of risk lies when the sensitive data proceeds outside the bounds of organization.

- Data location: The location of the data storage is not known to the user
- Data Segregation: In cloud the data lies in a shared environment with the data of the other customers. Chances of having malfunction are high during the course
- Recovery: Since the location of the data stored and segregation issues it becomes another challenge to recover the data rightfully to its owner.
- Long term Viability: long term viability refers to the time frame of the data storage.
- Investigation Support: sometimes it becomes impossible to detect inappropriate or illegal activity in cloud.
- Regulatory Compliance: service providers refuse to make an external audit or even give a security certification which is another threat to this technology usage.

IV. SECURITY SOLUTIONS

Cloud being a virtual environment that transfers data, several data storage concerns arises. A common example would be, the end user (customer) will not know the exact location of the data stored or will not know the other sources of data collectively stored with theirs.
To preserve the security of the clouds infrastructure it is perform practice of looking into the crucial aspects. Like authentication, integrity and availability. Hence the provider must follow certain ground written rules:

- Encryption: To secure sensitive data, to protect under the breaches to secure against advanced and persistent threats to the data
- Physical Security of the Cloud: Just as a bank repository is an attraction of robbers similarly data centers are attraction to the malicious users. Hence providing physical security is must
- Authentication and Access Control: Authentication is used by a client when the client needs to know that the server is system it claims to be. Authentication by a client usually involves the server giving a certificate to the client in which a trusted third party such as Verisign or Thawte states that the server belongs to the entity (such as a bank) that the client expects it to.
- Access Control or Authorization is a process by which a server determines if the client has permission to use a resource or access a file. Authorization is usually coupled with authentication so that the server has some concept of which the client is that is requesting access.
- Separation of duties: to avoid misconfiguration and to determine expertise is a must .Separation of sectors on the bases of liability and responsibility should hold great attention.
- Configuration, change control and patch management: though being very important it is sometimes ignore/overlooked by smaller organizations. Configuration, change control, patch management and updated process needs to be handled
- Intrusion detection and prevention: to detect the intrusions. What's coming in and what's going out must be checked in order to keep a tab of things.

Looking at all the above solutions this paper proposes on using the elliptical curve cryptography it can be used in authentication and encryption of secure data transmission.

V. ELLIPTICAL CURVE CRYPTOGRAPHY

The study of cryptography is the area of mathematics that disguises the data. The purpose of cryptography is to secure the message between two persons so another person or adversary cannot understand the enciphered message. The recipient can decipher the message. The objective of this paper is to present the encryption and decryption by elliptic curve cryptography.

The curve cryptography was invented by Neal Koblitz and Victor S. Miller in 1985. This is an efficient algorithm because it is based on the discrete logarithm problem. These algorithms are apparently harder to solve than other algorithms, especially factorized once.

When the use of Elliptical Curve Diffie Hellman and Elliptical Curve Digital Signature it is known as Elliptic curve Diffie–Hellman (ECDH). This algorithm particularly is an anonymous key agreement protocol that allows, both parties having an elliptic curve. The public–private key pair establishes the sharing of secret over an insecure channel.

The Elliptic Curve Digital Signature Algorithm (ECDSA) addresses the Digital Signature Algorithm (DSA) .The DSA is beneficial because it uses cryptography. Generally elliptic-curve cryptography, the bit size of the public key needed for ECDSA is about twice the size of that security level (in bits). At an instance a security of 80 bits (meaning a requirement of about 2^{80} operations to find the private key).When we compare the size of a DSA with ECDSA; the public key of DSA is 1024 bits whereas the ECDSA would be 160 bits. The signature size of both DSA and ECDSA is the same, i.e. $4t$ bits, (t is the security level measure).That is if we calculate is about 320 bits.

VI. CONCLUSION

Cloud computation technology is been built on decades of research in virtual computing and its benefactors. Utility of cloud has more add-ons.Hence it is necessary to develop the awareness as well as the right science to make use of this technology. Since cloud is such a new concept it must be dealt with great care. Security always comes first hand in establishing any technology. Nevertheless there are algorithms that help in the different areas of security. Elliptical Curve Cryptography is there one such algorithmic solution that can handle the authentication and security of the data.

ACKNOWLEDGEMENT

I wish to express my sincere thanks to our Head of Department, for providing me with all the necessary facilities for the research also wish to express my sincere thank you to my guide Akash Shrivastava CSE Department,DIT Dehradun, for the continuos encouragement. I am extremely thankful to him for sharing his experience .I take the opportunity to express gratitude to all of the Department faculty members for their support. I also thank my parents for encouraging me.

REFERENCES

[1] Cloud Computing, Brain Hayes July 2008|vol.51|No.7|Communications of the ACM
[2] http://en.wikipedia.org/wiki/Cloud_computing
[3] http://www.networkworld.com/article/2186444/cloud-computing/are-community-cloud-services-the-next-hot-thing-.html
[4] http://blog.sina.com.cn/s/blog_5foda5590100cmxw.html
[5] Data security in cloud computing with elliptical curve cryptography by Veerraju Gampala, Srilakshmi Inganti,Satish Muppiddi.International Journal of Soft Computing and Engineering(IJSCE)
[6] Security and Privacy Challenges in Cloud Computing Environment, Hassan Takabiand James B.D. University of Pittsburgh and Gail-Joom Ahn Arizona State university.
[7] www.wiki.openssl.org/index.php/Elliptic_Curve_Cryptography.
[8] Amazon Elastic Compute Cloud (EC2) http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html
[9] http://en.wikipedia.org/wiki/Elliptic_curve_cryptography
[10] http://en.wikipedia.org/wiki/Digital_Signature_Algorithm
[11]http://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm
[12]http://en.wikipedia.org/wiki/Elliptic_curve_Diffie%E2%80%93Hellman
[13] Cryptography and Network Security, William Stalling.