ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Cloud Computing: Data Security and Future Perspectives

Divya Sindhu, Saurabh Sindhu

Lecturer, Department of Computer Science, CRM Jat College, Hisar, Haryana, India

ABSTRACT: Cloud computing provides a platform with an enhanced and efficient way to store data in the cloud i.e., server with different range of capabilities and applications. Cloud computing is a compilation of existing techniques and technologies, packaged within a new infrastructure that offers improved scalability, elasticity, business agility, faster startup time, reduced management costs and just-in-time availability of resources. It provides an easy way of accessing one's personal file or data and use application without installing it on machines by just having Internet access. The server and the email management software is installed on the cloud and managed by service providers. The involvement of cloud based services and service providers have resulted in a new business trend based on cloud technology and cloud computing has become a boon for IT industry nowadays. However, data security has been a major and challenging aspect in the internet and network applications. Especially it becomes serious in the cloud environment because the data is located in different places all over the world. The purpose of securing data is that only concerned and authorized users can access it. If security is not robust and convenient, the flexibility and advantages of cloud computing will have low creditability and it could ultimately result in higher costs and potential loss of business. Encryption algorithms are used to ensure the security of data in cloud computing. This paper presents cloud computing architecture as well as security issues inherent within the concept of cloud computing and cloud infrastructure. The encryption and decryption algorithms used for data storage security in the cloud are also discussed.

KEYWORDS: Cloud computing, Computer network, Internet, Data security, Encryption algorithms, Cloud infrastructure

I. INTRODUCTION

Cloud computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services [1]. The server and the e-mail management software is installed on the cloud and managed by service providers. Because of these benefits, every organization is moving their data to the cloud. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations [2]. Cloud services include online file storage, social networking sites, webmail and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. It provides a shared pool of configurable computing resources, including data storage space, networks, computer processing power and specialized corporate and user applications with minimal management effort or service provider interaction. Cloud computing has now become a highly demanded service or utility due to the advantages of high computing power, cheap cost of services, high performance, scalability, accessibility as well as availability. Cloud vendors are experiencing appreciable growth rates in their business. Nowadays, Yahoo, Gmail, Amazon Rackspace, Google, Microsoft, VMware, iCloud, Drop Box etc. are good cloud service providers.

In recent years, advances in web technology and the proliferation of mobile devices and sensors connected to the internet have resulted in the generation of immense data sets that need to be processed and stored [3]. Moreover, business and commerce applications generate massive volume of data which has to be managed and analyzed by traditional data processing tools. Therefore, data security has become a challenging issue of data communications recently and is the main aspect of secure data transmission over unreliable network [4,5]. Different systems are at risk in lack of data security, which include financial systems, utilities and industrial equipment, aviation, consumer devices, large corporations, automobiles, government official work and internet. Data security touches many areas including

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

secure communication channel, strong data encryption technique and trusted third party to maintain the database. As crackers troubled away at networks and computer systems, there is a need to protect that data against unauthorized access, alternation or interchanging [6,7]. The cloud provider must ensure that their infrastructure is secure and their clients' data and applications are protected, while the user must take measures to fortify their application and use strong passwords and authentification measures. To secure the cloud means securing the treatments (calculations) and storage (databases hosted by the cloud provider). Therefore, security is considered as one of the most critical features for computer network due to sensitivity and importance of data stored [8].

The rapid developments in information technology involve the secure transmission of confidential data and the conventional methods of encryption are employed to maintain the data security [9,10]. Data security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among organizations, enterprises and other types of institutions, businesses, government agencies and individuals. Network security starts with authenticating the user, commonly with a username and a password. Since this requires just one detail authenticating the user name i.e. the password, this is sometimes termed one-factor authentication. With two factor authentication, a security token or 'dongle', an ATM card or a mobile phone is used [11,12]. With three-factor authentication, a fingerprint or retinal scan is used. Once authenticated, firewall forces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. An anomaly based intrusion detection system may also monitor the network and traffic for unexpected (i.e. suspicious) content or behaviour and other anomalies to protect resources, e.g. from denial of service attacks or an employee accessing files at strange times.

II. CLOUD BASED COMPUTING INFRASTRUCTURE

The difference between cloud-based and traditional software is that when you access the cloud, your desktop, laptop or mobile device isn't doing the actual computing. The computing happens in a large data center outside your organization and we simply see the results of it on our own screen. Most cloud computing services are accessed through a web browser like Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, or Google Chrome. Certain cloud services could be used via a dedicated mobile app or through a browser on a smartphone or tablet. Therefore, cloud services don't require users to have sophisticated computers that can run specialized software. Specifically, cloud computing refers to a cloud alternative to something that organizations would traditionally manage in-house. For example, a webmail service is a cloud-based alternative to hosting your own email server. A cloud-based constituent relationship management (CRM) database system is an alternative to running a donor database in your office.

In a cloud based computing infrastructure, the resources are normally in someone else's premise or network and accessed remotely by the cloud users [13,14]. The users 'rent' it for the time they use the infrastructure [15]. Processing is done remotely implying the fact that the data and other elements from a person need to be transmitted to the cloud infrastructure or server for processing; and the output is returned upon completion of required processing. In some cases, it might be required or at least possible for a person to store data on remote cloud servers. These gives the following three sensitive states that are of particular concern within the operational context of cloud computing:

- The transmission of personal sensitive data to the cloud server,
- The transmission of data from the cloud server to clients' computers and
- The storage of clients' personal data in cloud servers which are remote server not owned by the clients.

All the above three states of cloud computing are severely prone to security breach that makes the research and investigation within the security aspects of cloud computing practice. There have been a number of different blends that are being used in cloud computing realm, but the core concept is the infrastructure. In the cloud/client architecture, the client is a rich application running on an Internet-connected device and the server is a set of application services hosted in an increasingly elastically scalable cloud computing platform. The client environment may be a native application or browser-based; the increasing power of the browser is available to many client devices, mobile and desktop alike. Web-scale IT is a pattern of global-class computing that delivers the capabilities of large cloud service providers within an enterprise IT setting by rethinking positions across several dimensions.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Cloud service deals with web-fronted applications by using various languages java, php etc. Cloud infrastructure provides user the remote infrastructures and the web fronted application are further connected to the database i.e. cloud storage. The cloud computing field is commonly categorized into three main layers. These layers vary slightly from one source to the next, but they can generally be summarized as infrastructure as a service, platform as a service and software as a service (Fig. 1). Service model is also called as SPI model as Software, Platform and Infrastructure Model.

(i) Infrastructure as a Service (IaaS)

IaaS is the foundation or bottom layer of cloud computing. It includes services like storage, backup and security. Infrastructure as a service (IaaS) users utilizes remote infrastructure, allows users to run any applications they want on cloud hardware of their own choice. Example is Amazon Web Services, which includes database, storage, virtual private server and support services that are available on demand by the hour or by the MB. Many SaaS applications rely on Amazon Web Services or other IaaS providers. Cloud-based Voice over Internet Protocol (VoIP) telephone service is another example of IaaS. Other examples are; Private cloud, dedicated hosting, hybrid hosting.

(ii) Platform as a Service (PaaS)

PaaS is the next level of the cloud. Platform as a Service provides platform to users to work on web application or software. It allows users to create own cloud applications using supplier-specific tools and language. The vendors of PaaS services provide a certain framework and a basic set of functions that customers can customize and use to develop their own applications. Examples of PaaS services include Google App Engine, Force.com from Salesforce and Microsoft Azure.

In Platform as a Service, the organizations or industries have to decide at which applications are most appropriate for maintenance on the cloud. It will obviously differ from organization to organization, taking care of the critical key missions or tasks to maintain on the cloud. For instance, a company that develops software for healthcare providers is going to have different needs than a financial advisor. But even within the same industry, different organizations/scctions will get different things out of the cloud.

(iii) Software as a Service (SaaS)

SaaS basically means any Internet-based software or service that you rent, usually on a per-user, per-month basis. It is the most common type of cloud service that small offices use. Web based application are those applications that are built using web languages like php, java, .net, etc. This model of cloud allows one to run existing online applications. The example is Google Docs. Some SaaS applications are highly customizable and we may even need a consultant to help set them up, but they generally don't require specialized knowledge for day-to-day operation and maintenance. In SaaS, an application is hosted by a service provider and then accessed via the World Wide Web by a client. Examples of SaaS include Microsoft Office 365, Google Apps and Salesforce.

III. DATA SECURITY IN CLOUD COMPUTING

Huge amount of data transfer is a common application in a cloud environment. The security concerns of the adapted communication technology also become a security concern for the cloud computing approach. Cloud environment is associated with both physical and virtual resources and they pose different level of security issues. To fully address the security threats, without having sophisticated authentication mechanism is an existing problem for cloud computing. As the virtualized resources are highly coupled with a cloud infrastructure, intrusion related security concerns are of utmost priority as part of security issues. Arbitrary intermittent intrusion needs to be monitored in the operational context of a cloud computing infrastructure where the severity of possibility for a virtual machine to be compromised is to be taken into account [16].

Cryptography not only protects data from theft or alteration, but can also be used for user authentication. Thus, cryptographic algorithms play a major role for data user security [17]. As the complexity of algorithm is high, the risk of breaking the original plaintext from that of ciphertext is less. The main issues involved in data security are provided below:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

(i) Data integrity: The data in the cloud floats from the actual data holder to the other side end user. Due to migration of data to cloud, the service provider cannot maintain data integrity and safety. For the security of the data, cloud service providers should apply mechanisms to convince data truthfulness and define data set at the point [18]. It is ensured by Firewalls and intrusion detection.

(ii) Data confidentiality: Data confidentiality is the quality that data contents are not accessible to the illegal users. Users can supply their data and information on remote servers accessed through the internet. Only authorized users can access the sensitive data while others do not gain information of the data. Cloud data services, data search, data computation and data sharing utilize the data without the leakage of data [19]. It is ensured by security protocols, authentication services and data encryption services.

(iii) Data access: Data access is primarily informed to the security schemes that are given to the users while ensuring cloud data. The organization uses the cloud provided by the provider to conducting its business process and the organization have notice polices to access the business data stored on cloud.

(iv) Privacy: The providers ensure that all crucial data such as credit card number are masked or encrypted and only authorized users can access to data. Digital identities and credentials along with the data that the provider produces about costumer's activity in cloud ought to be protected. Cloud providers ensure that applications available as a service via the cloud (SaaS) are secure by specifying, designing, implementing, testing and maintaining appropriate application security measures in the production environment.

(v) Goverence: Cloud computing need suitable IT goverence model to assure a secured computing environment and to carry with all relevant organizational information technology schemes. Organization requires a set of capabilities that are important when effectively implementing and arranging cloud services that include demand management, data security management risks and compliance management.

(vi) Denial of service: Denial of service is a discrete problem for cloud computing. Attackers highjack the service and easily target the machine those which are connected outside the world of cloud and IP addresses.

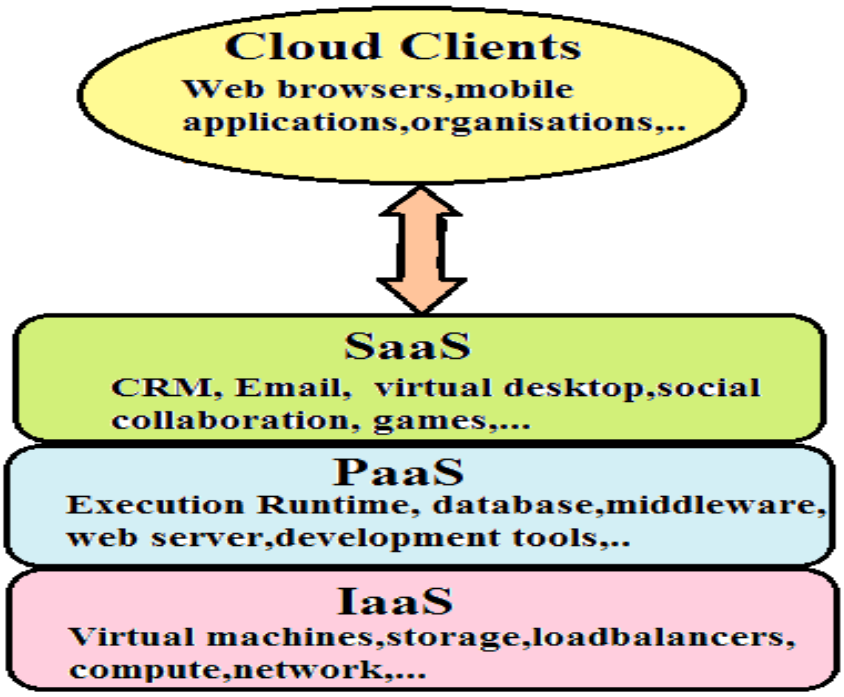

Figure 1. The cloud service provides service as a platform and service as an Infrastructure

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

The cost efficiency and globalization trends will enforce and motivate almost all the businesses to admit internet and associated technologies to be the ultimate means towards cloud computing approach [20]. As a result, total internet related security concerns are anticipated to be automatically added on top of the cloud-specific security issues. Cloud portability would make cloud services flexible and will enable the cloud users to switch among different cloud service providers without being affected with the necessity to change the ways to accomplish tasks in different ways. It is a clear provision on bargaining power for the cloud users; but at the same time, the security issues with cloud portability are to be counted. Cloud portability might bring severe degree of API based security threats [21].

IV. SECURITY ISSUES: USE OF CRYPTOGRAPHIC ALGORITHMS

Security goals of data include three points namely; availability, confidentiality and integrity. Confidentiality of data in the cloud is accomplished by cryptography [22]. Encryption/decryption process, in modern days is considered combination of three types of algorithms [23]. Symmetric encryption, also referred to as single-key encryption, was the only type of encryption in use prior to the introduction of public key encryption in the late 1970s [24].

The method of covering up of plaintext in such a way as to hide its substance is called encryption. Encryption is a well-known technology for protecting sensitive data [25]. The encryption algorithm performs various substitutions and transformations on the plaintext (Fig. 2). The secret key is also input to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key. Encrypting plaintext results in unreadable data called ciphertext. This is the scrambled message produced as output. It depends on the plaintext and the secret key. Thus, encryption is used to protect the information in hidden from anyone for whom it is not projected, even those who can see the encrypted data. For a given message, two different keys will produce two different ciphertexts. The process of reversing ciphertext to its original plaintext is called decryption. It takes the ciphertext and the secret key, and produces the original plaintext.

There are several ways of classifying cryptographic algorithms. These algorithms can be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. Cryptographic algorithms can be implemented in either hardware (for speed) or in software (for flexibility). In general, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher whereas the same plaintext will encrypt to different ciphertext in a stream cipher. The three types of algorithms using keys for encryption and decryption are as follows:.

- Symmetric (secret) key cryptography (SKC): It uses a single key for both encryption and decryption.
- Assymmetric (public) key cryptography (PKC): It uses one key for encryption and another for decryption.
- Hash functions: It uses a mathematical transformation to irreversibly "encrypt" the information.

4.1. Symmetric (secret) key cryptography

This cryptographic method uses two different algorithms for encryption and decryption respectively, and a same key is used both for the sender and the receiver. The sender uses this key and an encryption algorithm to encrypt data, the receiver also uses the same key and the corresponding decryption algorithm to decrypt that data [26]. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. With this form of cryptography, the key must be known to both the sender and the receiver. Advanced encryption standard (AES), data encryption standard (DES) and RC4 are the most widely used symmetric key cryptographic algorithms.

(i) Advanced encryption standard (AES)

National Institute of Standards and Technology (NIST) developed a new secure cryptosystem for U.S. government applications and formal adoption as the AES standard came in December 2001. AES uses an SKC scheme called Rijndael, a block cipher designed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The algorithm can use a variable block length and key length. The latest specification allowed any combination of keys lengths of 128, 192 or 256 bits and blocks of length 128, 192 or 256 bits [27]. FIPS PUB 197 describes a 128-bit block cipher employing a 128-, 192- or 256-bit key. It encrypts data blocks of 128 bits in 10, 12 and 14 roundS depending on the key size [28].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

(ii) Data encryption standard (DES)

It was designed by IBM in the 1970s and adopted by the National Bureau of Standards (NBS) [now the National Institute for Standards and Technology] in 1977 for commercial and unclassified government applications. Now-a-days, the DES algorithm is the most broadly used encryption algorithm in the world. The same algorithm and key are used for encryption and decryption, with minor differences. DES accepts an input of 64-bit long plaintext and 56-bitkey (8 bits of parity) and produce output of 64 bit block. DES has a complex set of rules and transformations that were designed specifically to yield fast hardware implementations. A variant of DES i.e., Triple-DES (3DES) employs up to three 56-bit keys and makes three encryption/decryption passes over the block is the recommended replacement to DES. Triple Data Encryption Algorithm (TDEA) is a symmetric-key block cipher standard which is similar to DES method but increases encryption level 3 times than DES. As a result, this is slower than other block cipher methods. The block size of 3DES is 64 bit with 192 bits key size [29].

(iii) RC4

The RC4 (Rivest Cipher 4) was named for Ron Rivest and is an encryption algorithm designed in 1987 by Ron Rivest for RSA security. It is a variable key-size stream cipher with byte-oriented operations. The algorithm is based on the use of a random permutation. It is a shared key stream cipher algorithm requiring a secure exchange of a shared key [30]. The RC4 encryption algorithm is used by standards such as IEEE 802.11 within WEP (Wireless encryption protocol) using 40 and 128-bit keys. It is widely used in commercial cryptography products. An update to RC4, called Spritz was designed by Rivest and Jacob Schuldt. RC4 is used in the SSL/TLS (Secure sockets layer/Transport layer security) standards that have been defined for communication between web browsers and servers. It is also used in the WEP (Wired equivalent privacy) protocol and the newer WiFi protected access (WPA) protocols that are part of the IEEE 802.11 wireless LAN standard.

4.2. Asymmetric (public) key cryptography

Public-key cryptography (PKC) was first described publicly by Professor Martin Hellman and graduate student Whitfield Diffie (Stanford University) in 1976. This cryptographic method makes use of two different algorithms for encryption and decryption respectively; a public key for encryption and a private key for decryption. The public key of the sender is used to encrypt the message. The receiver decrypts the cipher text with the help of a private key. The descriptions of some widely used asymmetric key cryptographic algorithms are given below:

(i) RSA

RSA is the first and most common, PKC implementation, named for the three MIT mathematicians, who developed it; Ronald Rivest, Adi Shamir and Leonard Adleman. RSA is broadly used an asymmetric encryption/decryption algorithm. The public key can be informed to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. It secured user data assimilate encryption before the storage, user authentication procedures prior to storage or retrieval and making secure channels for data transmission [31, 32].

(ii) Diffie-Hellman

Diffie and Hellman (D-H) algorithm was published, this algorithm was first revealed by Whitfield Diffie and Martin Hellman in 1976. D-H is used for secret-key key exchange only and not for authentication or digital signatures. Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. It permits two parties that have no prior knowledge of each other to jointly make a shared secret key over an insecure communications channel. This key can then be used to encrypt posterior communications using a symmetric key cipher.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

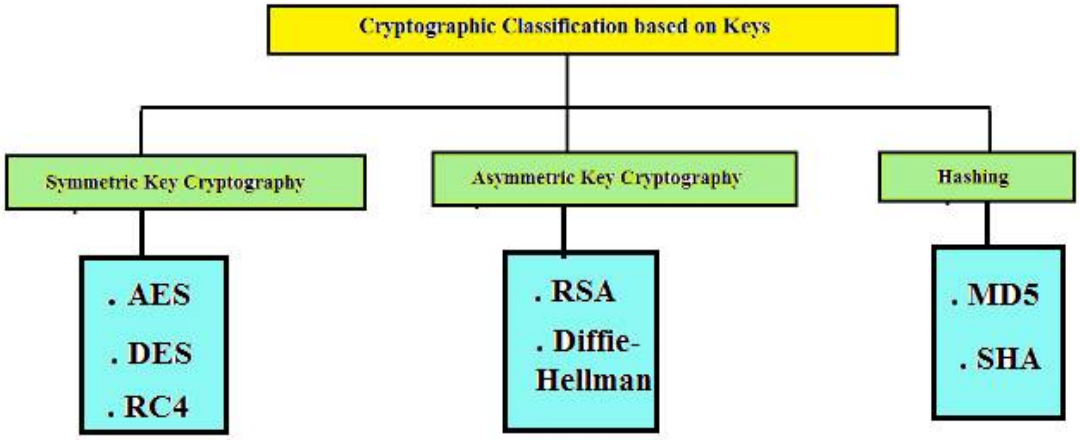

Figure 2. Schematic representation of some widely used symmetric, asymmetric and hashing key cryptographic algorithms.

4.3. Hashing cryptography

Hash functions are fundamental in the field of cryptography and used widely in a broad spectrum of important applications involving message integrity and authentication, digital signatures, secure time stamping etc. Hash functions, also called message digests and one-way encryption, are algorithms that use no key. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents often used to ensure that the file has not been altered by an intruder or virus. Hash functions provide a measure of the integrity of a file.

(i) Message Digest (MD) algorithms

MD algorithms include a series of byte-oriented algorithms that produce a 128-bit hash value from an arbitrary-length message. MD5 (Message Digest 5) is a broadly used cryptographic hash function with a 128-bit hash value. It processes a variable-size message into a fixed-length output of 128 bits [33]. The input message is divided into chunks of 512-bit blocks; then the message is padded for making its length divisible by 512. In this algorithm, sender use the public key of the receiver to encrypt the message and receiver use its private key to decrypt the message.

(ii) Secure hash algorithm (SHA)

Algorithm for NIST's Secure Hash Standard (SHS) was described in FIPS 180-4. SHA-1 produces a 160-bit hash value and was originally published as FIPS PUB 180-1 and RFC 3174. It was deprecated by NIST at the end of 2013, although it is still widely used. SHA-2 was originally described in FIPS PUB 180-2 and eventually replaced by FIPS PUB 180-3 and FIPS PUB 180-4. It comprises five algorithms in the SHS: SHA-1 plus SHA-224, SHA-256, SHA-384 and SHA-512, which can produce hash values that are 224, 256, 384 or 512 bits in length, respectively. The newer and stronger SHA-2 hash function is currently used in a wide variety of applications, including TLS, SSL, SSH and PGP. SHA-3 is the current SHS algorithm. The NIST version can support hash output sizes of 256 and 512 bits.

V. POTENTIAL ADVANTAGES OF CLOUD COMPUTING

Cloud computing holds a lot of exciting potential. Many organizations are able to realize cost savings because they do not have to run and maintain their own server(s) (or pay a consultant to do so). Many cloud tools enable new levels of sharing and collaboration, which can transform our working. There is an increasing need to partner with other organizations with greater transparency to achieve real impact. Using the right cloud tools, the barriers can be broken down that we currently face and organizations can be the more open, effective and resilient. Businesses can reap huge benefits from cloud computing.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

The most important cloud computing benefits are in terms of IT cost savings. Every business exists to earn money, with keeping assets and operational expenses to a minimum. With cloud computing, we can save extensive capital costs with zero in-house server storage and application necessities. The lack of on-premises infrastructure removes their connected prepared costs in the form of authority, air training and supervision costs. In fact, cloud services are very much logical for smaller businesses. In addition, with the shift of more business and critical applications into the cloud, the regular upgradation of computers is not required. That's because the actual computing isn't happening on the computer: A los cost tablet can access your Salesforce and Google Apps accounts just as quickly as a costly laptop can. Similarly, you may find that a cloud computing infrastructure requires a smaller IT staff than a traditional IT setup does because your organization would not be managing the software anymore.

Moreover, if the organization or company is having staff members working off-site, they can access their work just as easily at home as they can in the office. Thus, software as a service can act as a great simplifier for many organizations. If they're using a private or secure Wi-Fi connection, there's also no need to set up a virtual private network (VPN). Cloud tools can make it easier to collaborate with colleagues from outside the organization. For example, it's easy to create a Basecamp project where everyone can see each other's work. People working in the same organization might benefit from team collaboration tools like shared calendars, video conferencing, instant messaging and file sharing via Office 365.

Cloud computing provides improved and simplified IT management and maintenance capabilities through central administration of resources, vendor managed infrastructure and SLA backed agreements. IT infrastructure updates and maintenance are removed, as all resources are maintained by the service provider. We enjoy an easy web-based user interface to access applications, software and services without the installation and an SLA facilitates the timely and assured delivery, maintenance and management of our IT services. Moreover, with a managed service platform, cloud computing is much more reliable and more dependable than in-house IT infrastructure. The majority providers offer a Service Level Agreement (SLA) which guarantees 24 hours services throughout the week for whole year. Organizations can benefit from a huge pool of redundant IT resources, as well as a quick failover mechanism. If a server fails, hosted applications and services can simply be transited to any of the available servers.

Cloud computing solutions are also generally greener than traditional IT because they require less in-office IT equipment. While huge data centers require a lot of electricity, it's still a lot less than the thousands of office-grade computers it would take to perform the same big tasks. Large cloud computing providers can also optimize their data centers for energy efficiency much more precisely than manufacturers of desktops and laptops. Furthermore, rising computing resources give us a competitive edge over competitors, as the time we necessitate for IT procurement is almost nil. The company can arrange mission crucial applications that deliver significant business benefits, without any truthful costs and minimum provisioning time. Cloud computing focusses on key business activities and objectives. It can also help to reduce the time needed to market newer applications and services.

VI. DISADVANTAGES OF CLOUD COMPUTING

With many advantages of cloud computing, some drawbacks have also been reported. Several outstanding issues exist, particularly related to service-level agreements (SLA), security and privacy, and power efficiency. Security has also a lot of loose ends which scares away several potential users. Until a proper security module is in place, potential users will not be able to leverage the true benefits of this technology. Although cloud service providers execute the finest security principles and industry certifications, saving data and main files on external service providers always open up risks. Using cloud-powered technologies mean we need to provide our service provider with access to significant business data. The ease in procuring and accessing cloud forces can also give reprehensible users the ability to scan, identify and exploit loopholes and vulnerabilities in a system. For example, in a multi-tenant cloud architecture where multiple users are hosted on the same server, a operator might attempt to break into the data of more users hosted and stored on the identical server.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

As cloud service providers take care of a number of clients each day, they can become overwhelmed and may even come up against technical outages. This can lead to your business processes being temporarily suspended. Additionally, if your internet connection is offline, you will not be able to access any of your applications, server or data from the cloud. In cloud server, the customer will be able to control and manage the limited functions, applications, devices, and data but not on the backend infrastructure since the infrastructure of the cloud is fully managed and monitored by the service provider and minimum power will be transferred to the customer. The end user is not facilitated with the administrative tasks like firmware management, updating and shell accessing. Key administrative tasks such as server shell access, updating and firmware management may not be passed to the customer or end user.

The vendor lock-in is a major issue in cloud server since it was with traditional IT. Even though a cloud server works in a flexible and integrated manner, it is challenging to the organizations to transfer their services from one seller to another. We may face difficulty such as inter-operability and support issues in hosting and integrating current cloud applications on another platform. For example, the applications developed on Microsoft Development Framework (.Net) may not be able to function properly on the Linux platform. Cloud computing is still a quickly changing field, and there's always the danger that a new company might go out of business or radically change its service. A sudden change in service might not be too detrimental if you were only using the application for a one-time project, but it could be disastrous if you were using it for your entire donor database. When evaluating cloud providers, find out what options you have for backing up and extracting your data. The best services allow you to download your data in a standard, nonproprietary format. Finally, the user will become more dependent on a good Internet connection if you rely on the cloud. As more mission-critical work is done on the Internet, organizations will need much more internet access, connection speed, bandwidth in internet connectivity.

VII. CONCLUSIONS AND FUTURE PROSPECTS

Cloud computing appeared in 2006, when Amazon's Elastic Computing Cloud (EC2) was introduced into the world. Subsequently, many information enterprises developed their platform for cloud computing. In 2007, Dell released his solution of cloud computing and at the same time IBM's Blue Cloud appeared followed by Google's Map-reduce, Microsoft's Windows Azure. The number of research publications in IEEE Xplore and ScienceDirect were searched from the year 2006-2014 using keyword "Cloud Computing" and the total number of papers published in IEEE Xplore and ScienceDirect increased from one in 2006 to 5646 in 2014. Recently, cloud computing has received increasing interest from various industry professionals and enterprises, and recently cloud service providers are offering a wide range of solutions to businesses. Enterprise businesses are moving their IT services, applications and infrastructure to cloud-based architecture.

The wide transition to mobile computing practices in recent years has made it imperative to include mobile computing and its associated technologies as an essential part of cloud computing. The demand of huge data processing is a problem for mobile end-user devices which has been further complemented by the security concerns of mobile cloud computing. For mobile cloud computing, the device level limitations has inspired researchers to suggest the inclusion of another level of cloud termed as 'mobile cloud' to aid the processing of the specific computing and processing for mobile computing devices [34].

Although, cloud computing has enormous prospects, but the security threats embedded in cloud computing approach are directly proportional to its offered advantages. The security issues in cloud computing are sensitive and crucial on the basis of sociological and technological viewpoints. The social implications of cloud computing approaches might emerge with severe impact of robust security models for cloud computing. With the goal of secured exploitation of a Service Oriented Architecture, the security aspects and issues of cloud computing are inherent not only with the elements from the cloud infrastructure but also with all associated services as well as the ways computing is done both at the users' and the cloud service providers' ends. Service oriented architecture and other characteristics of cloud computing suggests that the concept of cloud computing would require regular and practical analysis in line

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

with social, business, technical and legal perspectives. Although, security itself is conceptualized in cloud computing infrastructure as a distinct layer [35] and security for cloud computing environment is a non-compromising requirement. Thus, cloud computing is inevitable to become the ultimate approach to business computing though the security barriers to make it more viable [36].

Still, several outstanding issues exist, particularly related to service-level agreements (SLA), security and privacy, and power efficiency. Currently, security has lot of loose ends which scares away several potential users. Until a proper security module is not operative, potential users will not be able to leverage the true benefits of this technology. This security module should cater to all the issues and every element in the cloud should be analyzed at both the macro and micro level. Research efforts are being made to develop faster and secured Scientific Cloud Computing (SCC) tools [37], which will greatly influence the pace of research and motivation in various fields together with clouding computing itself. Subsequently, an integrated solution must be designed and deployed in the cloud to attract and retain the potential consumers.

REFERENCES

[1] Ahmed, M. and Hossain, M. A., "Cloud computing and security issues in the cloud", International Journal of Network Security and its Applications, Vol. 6 (1). pp. 25–36, 2014.
[2] Adamuthe, A. C., Salunkhe, V. D., Patil, S, H. and Thampi, G. T., " Cloud computing – A market perspective and research directions" , I. J. Information Technology and Computer Science, Vol. 10, pp. 42–53, 2015. DOI: 10.5815/ijitcs.2015.10.06.
[3] Sindhu, S. and Sindhu, D., " Cryptographic algorithms: Applications in network security", International Journal of New Innovations in Engineering and Technology, ISSN : 2319-6319, Vol. 7(1), pp. 18–28, 2017.
[4] Bollavarapu, S. and Gupta, B., " Data security in cloud computing", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4(3), pp. 1208–1215, 2014.
[5] Sharma, M., Husain, S. and Ali, S., "Cloud computing risks and recommendations for security", International Journal of Latest Research in Science and Technolgy, ISSN:2278-5299, Vol. 6, pp. 52–56, 2017.
[6] Krombholz, K., Hobel, H., Huber, M. and Weippl, E., "Advanced social engineering attacks", Journal of Information Security and Applications, Vol. 22, pp. 113–122, 2015.
[7] Zeng, W., Koutny, M., Watson, P. and Germanos, V., " Formal verification of secure information flow in cloud computing", Journal of Information Security and Applications, Vol. 27-28, pp. 103–116, 2016.
[8] Ryan, M.D., "Cloud computing security: The scientific challenge and a survey of solutions", The Journal of Systems and Software, Vol. 86, pp. 2263–2268, 2013.
[9] Khan, S. S. and Tuteja, R. R., "Security in cloud computing using cryptographic algorithms", International Journal of Innovative Research in Compute and Communication Engineering, Vol. 3(1), pp. 148–154, 2015.
[10] Nithya, R., " Network security using cryptographic techniques", International Journal of Innovative Research in Computer Science and Communication Engineering, Vol. 4(5), pp. 111–113, 2016.
[11] Mason, S. and George, E., " Digital evidence and 'cloud' computing", Computer Law and Security Review, Vol. 27, pp. 524–528, 2011. doi:10.1016/j.clsr.2011.07.005.
[12] Yassin, A.A., Jin, H., Ibrahim, A., Qiang, W. and Zou, D., "Efficient pass word based two factors authentification in cloud computing" , International Journal of Security and its Applications, Vol. 6(2), pp. 143–148, 2012.
[13] Petre, R., "Data mining in cloud computing", Database Systems Journal, Vol. 3(3), pp. 67–71, 2012.
[14] Singh, S. and Jangwal, T., "Cost breakdown of public cloud computing and private cloud computing and security issues", International Journal of Computer Science and Information Technology, Vol. 4(2), pp. 17–31, 2012.
[15] Rashmi, Sahoo, G. and Mehfuz, S., "Securing software as a service model of cloud computing: Issues and solutions", International Journal on Cloud Computing: Services and Architecture, Vol. 3(4), pp. 1–11, 2013. Doi: 10.5121/ijccsa.2013.3401.
[16] Arshad, J, Townsend, P. and Xu, J., "A novel intrusion severity analysis approach for clouds", Future Generation Computer Systems, Vol. 29, pp. 416–428, 2013. doi:10.1016/j.future.2011.08.009.
[17] Potey, M. M., Dhote, C. A. and Sharma, D. H., "Homomorpic encryption for security of cloud data", Procedia Computer Science, Vol. 79, pp. 175–181, 2016.
[18] Patwal, M. and Mittal, T., "A Survey of Cryptographic based Security Algorithms for Cloud Computing", HCTL Open International Journal of Technology Innovations and Research HCT, E-ISSN: 2321-1814, Vol. 8, pp. 1–17, 2014.
[19] Singh, J. and Sharma, S., "Review on Cloud Computing Security Issues and Encryption Techniques", International Journal of Engineering Development and Research, ISSN: 2321-9939, Vol. 3(2), pp. 1051–1053, 2015.
[20] Khorshed, T. M., Ali, A. B. M. S. and Wasimi, S. A., "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing", Future Generation Computer Systems, Vol. 28, pp. 833–851, 2012. doi:10.1016/j.future.2012.01.006.
[21] Petcu, D., Macariu, G., Panica, S. and Craciun, C., "Portable cloud applications—from theory to practice", Future Generation Computer Systems, Vol. 29, pp. 1417–1430, 2013. doi:10.1016/j.future.2012.01.009.
[22] Atayero, A. A. and Feyisetan, O., "Security issues in cloud computing: The potentials of homomorphic encryption", Journal of Emerging Trends in Computing and Information Services, Vol. 2(10), pp. 546–552, 2011.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

[23] Bhardwaj, A., Subrahmanyan, G.V.B., Avasti, B. and Sastry, H., "Security algorithms for cloud computing", Procedia Computer Science, Vol. 85, pp. 535–542, 2016.
[24] Kaur, M. and Singh, R., "Implementing encryption algorithms to enhance data security of cloud in cloud computing", International Journal of Computer Applications, ISSN 0975 – 8887, Vol. 70, pp. 16–21, 2013.
[25] Jasim, O. K., Abbas, S., El-Horbaty El. S. M. and Salem, A. B. M., "Efficiency of modern encryption algorithms in cloud computing", International Journal of Emerging Trends and Technology in Computer Science, ISSN 2278-2286, Vol. 2(6), pp. 123–128, 2013.
[26] Arora, R. and Parashar, A., " Secure user data in cloud computing using encryption algorithms", International Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 3(4), pp. 1922–1926, 2013.
[27] Mahajan, P. and Sachdeva, A., "A study of encryption algorithms AES, DES and RSA for security", Global Journal of Computer Science and Technology Network, Web and Security, ISSN: 0975-4350, Vol. 13, pp. 15–22, 2013.
[28] Kaur, G. and Mahajan, M., "Analyzing data security for cloud computing using cryptographic algorithms", International Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 3(5), pp. 782–786, 2013.
[29] Singh, G. and Kinger, S., "Integrating AES, DES, and 3-DES encryption algorithms for enhanced data security", International Journal of Scientific and Engineering Research, Vol. 4(7), pp. 78–85, 2013.
[30] Ahmad, I. and Khandekar, A., " Homomorphic encryption method applied to cloud computing", International Journal of Information and Computation Technology, ISSN: 0974-2239, Vol. 4(15), pp. 1519–1530, 2014.
[31] Parsi, K. and Sudha, S., " Data Security in cloud computing using RSA algorithm", International Journal of Research in Computer and Communication technology, ISSN: 2278-5841, Vol. 1(4), pp. 145–152, 2012.
[32] Dharini, A., Devi, R. M. and Chandrasekar, I., "Data security for cloud computing using RSA with magic square algorithm", International Journal of Innovation and Scientific Research, ISSN: 2351-8014, Vol. 11(2), pp. 439–444, 2014.
[33] Singh, V. K. and Dutta, M., "Analyzing cryptographic algorithms for secure cloud network", International Journal of Advanced Studies in Computer Science and Engineering, Vol. 3(6), pp. 1–9, 2014.
[34] Fernando, N., Loke, S. W. and Rahayu, W., " Mobile cloud computing: A survey", Future Generation Computer Systems, Vol. 29, pp. 84–106, 2013. doi:10.1016/j.future.2012.05.023.
[35] Dukaric, R. and Juric, M. B., "Towards a unified taxonomy and architecture of cloud frameworks", Future Generation Computer Systems, Vol. 29, pp. 1196–1210, 2013. doi:10.1016/j.future.2012.09.006.
[36] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A., "Cloud computing: The business perspective", Decision Support Systems, Vol. 51, pp. 176–189, 2011. doi:10.1016/j.dss.2010.12.006.
[37] Jorissen, K., Villa, F. D. and Rehr, J. J., "A high performance scientific cloud computing environment for materials simulations". Computer Physics Communications, Vol. 183, pp. 1911–1919, 2012. doi:10.1016/j.cpc.2012.04.010.