A REVIEW ON VARIOUS SECURITY TECNIQUES IN CLOUD COMPUTING

Randeep Kaur
Assistant Professor, Department of Computer Engineering, Chandigarh University, Gharuan
(E-mail:randeep.e7950@cumail.in)

Abstract—
Cloud computing is an imminent upset in data innovation (IT) industry due to its execution, openness, minimal effort and numerous different opportunities. It is a way to deal with increasing the benefits or venture up capacities enthusiastically without putting resources into new framework, sustaining new faculty or authorizing new programming. It gives huge capacity to information and quicker computing to clients over the web. It basically moves the database and application programming to the large number of servers, i.e., cloud, where the executives of information and administrations houses may not be totally dependable. That is the reason organizations are hesitant to send their business in the cloud even cloud computing offers a wide scope of extravagances. Security of information in cloud is one of the serious issues which goes about as a hindrance in the execution of cloud computing. In this paper we have talked about different sorts of security assaults, their counteractive action systems and information encryption algorithms.

Keywords— *Cloud computing, security, RSA, AES, DES, cryptography, plain text, encryption, decryption, cipher.*

I. INTRODUCTION

Cloud computing is utilizing the web to get to another person's product running on another person's equipment in another person's server farm. Cloud computing is getting a lot of consideration, both in distributions and among clients, from people at home to the U.S. government. However it isn't in every case obviously characterized Cloud computing is a membership based administration where you can acquire arranged extra room and PC assets. One approach to consider cloud computing is to think about your involvement with email. Your email customer, on the off chance that it is Yahoo!, Gmail, Hotmail, etc, deals with lodging the majority of the equipment and programming important to help your own email account. When you need to get to your email you open your internet browser, go to the email customer, and sign in. The most imperative piece of the condition is having web get to. Your email isn't housed on your physical PC; you get to it through a web association, and you can get to it anyplace. On the off chance that you are on an outing, at work, or down the road getting espresso, you can browse your email as long as you approach the web. Your email is not the same as programming introduced on your PC, for example, a word handling program. When you make a report utilizing word preparing programming, that archive remains on the gadget you used to make it except if you physically move it. An email customer is like how cloud computing functions. Aside from as opposed to getting to simply your email, you can pick what data you approach inside the cloud. Cloud Computing is normally characterized as kind of computing that depends on sharing computing assets as opposed to having individual to deal with applications. Cloud Computing, in which not just our data but even our software resides within the Cloud, and we access everything not only through our PCs but also Cloud-friendly devices, such as smart phones, PDA's, the mega computer enabled by virtualization and software as a service. This is utility computing powered by massive utility data centers. The main attributes of cloud computing are illustrated as follows [1]:

- Multi-tenancy (shared resources): Cloud computing is based on a business model in which resources are shared (i.e., multiple users use the same resource) at the network level, host level, and application level.
- Massive scalability: Cloud computing provides the ability to scale to tens of thousands of systems, as well
as the ability to massively scale bandwidth and storage space
- Elasticity: Users can rapidly increase and decrease their computing resources as needed.
- Pay as you used: Users to pay for only the resources they actually use and for only the time they require them.
- Self-provisioning of resources: Users self-provision resources, such as additional systems (processing capability, software, storage) and network resources.
- Cloud computing can be confused with distributed system, grid computing, utility computing, service oriented architecture, web application, web 2.0, broadband network, browser as a platform, Virtualization, and free/open software [2].

Cloud computing is a vital structure with remarkable potential in diminishing the expenses by improving and creating usefulness and monetary result which thusly can expand collaboration, pace and adaptability acknowledgment to fathomable degree [1, 2]. This innovation has given numerous chances to vast partnerships and IT organizations in created nations, in any case, these open doors face with difficulties like security that is a standout amongst the most essential worry in the field of cloud computing [2, 3]. On the off chance that security administrations use seriously the all pieces of cloud computing face with issues, for example, the administration of individual data in an open system or put away information clients on the servers giving cloud services[2].It can be communicated that wellbeing is a virtual interstate to the selection of the cloud, if the suppliers of this innovation can devastate the deterrent from the way or limits it, cloud computing will be an essential factor in the field of data innovation, so it is less demanding to organizations and open to acknowledge and trust to utilize it [2]. Today, the principle worry in cloud computing is the means by which to make trust in tolerating, sharing applications, equipment, and so on., in a domain that we don't have the foggiest idea who is in charge of verifying our information [2, 4].So to manufacture trust and build up the cloud computing use, it wants to fix the security defects and limit the difficulties are fundamental. The cloud computing model revolves around three functional units or components as listed below:

1. Cloud service provider: It is an entity, which manages Cloud Storage Server (CSS), has significant storage space to preserve the clients' data and high computation power.
2. Client/owner: It is an entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation; it can either be individual consumer or organizations.
3. User: It is a unit, which is registered with the owner and uses the data of owner stored on the cloud. The user can be an owner itself as well.

In this paper, security issues in cloud technology, with emphasis on security challenges in the field of saving data examined. In addition to research in the field of cloud security and the issues and weaknesses in their investigation and decided to solutions for a better offer, and we refer to this issue that we build trust with consumers to transfer their data into the cloud and store them in the server side of a provider of cloud services necessary to develop and expand to use green technology by users. Also, due to economic problems in the world and reduce the purchasing power of people the act of decrease security challenges and enhance public confidence in the services provided by the technology of cloud computing will follow economy for many people and governments.

II. CLOUD SERVICES MODEL

Each service serves a specific function, giving users more or less control over their cloud depending on the type. When we choose a provider, compare our needs to the cloud services available. If it will be for personal home use, will need a different cloud type and provider than using the cloud for business. Keep in mind that the cloud provider will be pay-as-you-go, meaning that if the technology needs change at any point one can purchase more storage space (or less for that matter) from the cloud provider.

These three types differ in the amount of control that one have over the information, and conversely, how much one can expect the provider to do.

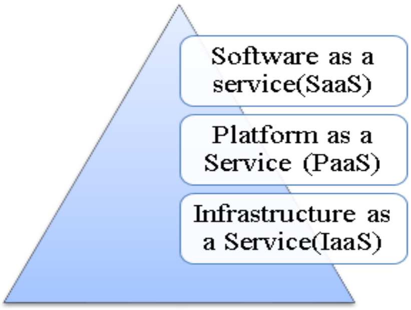
Software as a service(SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service(IaaS)

Figure 1. Cloud Services

Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources. Consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components.

Platform as a Service (PaaS): Consumer created or acquired applications using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. The capability provided to the consumer is to deploy onto the cloud infrastructure.

Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., Web-based email). The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

III. CLOUD DEPLOYMENT MODELS

There are different types of clouds that one can subscribe to depending on the needs.

Public Cloud: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space.

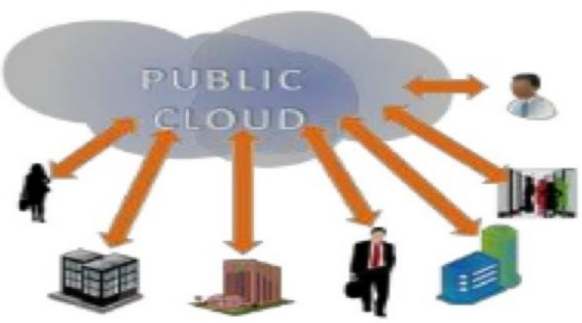

Figure 2. Public Cloud

Private Cloud: A private cloud is established for a specific group or organization and limits access to just that group.

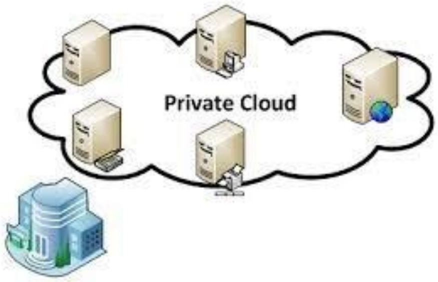

Figure 3. Private Cloud

Hybrid Cloud: The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities, but are bound together by standardized technology that enables data and application portability. Example cloud bursting for load-balancing between clouds. Figure 4 shows the basic diagram of a hybrid cloud.

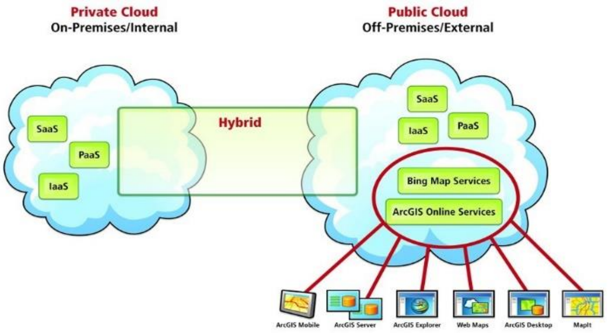

Figure 4. Hybrid Cloud

Community Cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns. A community cloud is shared among two or more organizations that have similar cloud requirements. Example: security requirements, policy, compliance considerations. It may be managed by the organizations or a third party.

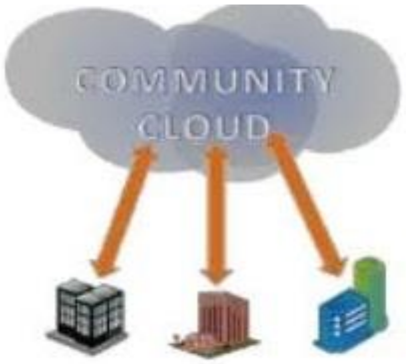

Figure 5. Community cloud

IV. COMMON CLOUD EXAMPLES

The lines between local computing and cloud computing sometimes get very, very blurry. That's because the cloud is part of almost everything on computers these days. One can simply have a local piece of software (for instance, Microsoft Office 365) that utilizes a form of cloud computing for storage (Microsoft One Drive). It is said, Microsoft also offers a set of Web-based apps, Office Online, that are Internet-only versions of Word, Excel, PowerPoint, and One Note accessed via one’s Web browser without installing anything. That makes them a version of cloud computing (Web-based cloud). Some other major examples of cloud computing are:

Google Drive: This is a pure cloud computing service, with all the storage found online so it can work with the cloud apps: Google Docs, Google Sheets, and Google Slides. Drive is also available on more than just desktop computers; one can use it on tablets like the iPad or on smartphones, and there are separate apps for Docs and Sheets, as well. In fact, most of Google's services could be considered cloud computing: Gmail, Google Calendar, Google Maps, and so on.

Apple iCloud: Apple's cloud service is primarily used for online storage, backup, and synchronization of the mail, contacts, calendar, and more. All the data one needs is available on iOS, Mac OS, or Windows device (Windows users have to install the iCloud control panel). Naturally, Apple won't be outdone by rivals: it offers cloud-based versions of its word processor (Pages), spreadsheet (Numbers), and presentations (Keynote) for use by any iCloud subscriber. iCloud is also the place iPhone users go to utilize the Find My iPhone feature that's all important when the handset goes missing.

Amazon Cloud Drive: Storage at the big retailer is mainly for music, preferably MP3s that one purchase from Amazon, and images—if one has Amazon Prime, get unlimited image storage. Amazon Cloud Drive also holds anything one buys for the Kindle. It's essentially storage for anything digital one would buy from Amazon, baked into all its products and services.

Hybrid services like Box, Dropbox, and Sugar Sync all say they work in the cloud because they store a synced version of files online, but they also sync those files with local storage. Synchronization is a cornerstone of the cloud computing experience, even if one does access the file locally. Likewise, it's considered cloud computing if one have a community of people with separate devices that need the same data synced, be it for work collaboration projects or just to keep the family in sync.

V. SECURITY IN CLOUD COMPUTING

Cloud can guarantee the client's information security utilizing the idea of firewalls, virtual private systems and by actualizing other security strategies inside its own fringe or border. Since the idea of cloud requires asset surveying with other cloud owner's, subsequently, business basic or other essential information of customer isn't just accessible to cloud yet additionally to outsider cloud [10]. Security is accordingly a noteworthy component in any distributed computing foundation, since it is fundamental to guarantee that just approved access is allowed and secure conduct is normal. The different security concerns and up and coming difficulties are tended to in [10] and furthermore looked into buries of measures. There are likewise compositional security issues which are changing as per different engineering configuration working over distributed computing. Since re-appropriating is the fundamental topic of distributed computing, there are two principle worries around there:

1. Outside aggressor (any unapproved individual) can get to the basic information, as the control isn't in the hands of the proprietor.

2. Cloud specialist organization himself can rupture the proprietor, as information is to be kept in his premises.

Any sort of security and protection infringement is basic and can deliver desperate outcomes. When cloud protection issues are additionally sorted out and exacting guidelines and administration for cloud activity are in position, increasingly more entrepreneurs will feel safe to settle on distributed computing. Different Issues in Cloud Environment:-

- Ensuring proper access control (authentication, authorization, and auditing)
- Network level migration, so that it requires minimum cost and time to move a job.
- To provide proper security to the data in transit and to the data at rest.
- Legal quagmire and transitive trust issues.
- Data availability issues in cloud.. The most prevalent problem in Cloud computing is the problem of data availibity or we can say that unavailability of services, resources provided by Cloud. There are most dangerous attacks known as DDoS Attacks which results in scarcity of resources or services from service provider to the consumers.

VI. TYPES OF ATTACKS

Network Layer DDoS Attacks: There are number of attacks those effect network layer services or applications:

TCP SYN Flooding Attacks: In TCP SYN flooding, the attacking system sends a TCP SYN request with a spoofed source IP address to a host. While these TCP SYN requests look legitimate, the spoofed address refers to a client that doesn't exist so the final ACK message is never sent to the victim host.The result is half- open connections at the victim site. A backlog queue stores these half-open connections, which bind the server's resources so that no new legitimate connections can be made, resulting in Denial of Service.

UDP Attacks: In a UDP flood attack, the attacker sends a large number of UDP packets to random ports on the target. As the UDP does not have a congestion control system, the attacker can potentially send a very large number of packets. This attack is generally used with IP address spoofing, so that the attacker can stay away from detection.

DNS Amplification Attacks: DNS amplification attack uses DNS queries. The size of the reply to a DNS query can be much larger than the DNS query. The attacker creates a reliable domain name server, and registers a garbage text of large size, for example 5000 bytes, as the text Resource Record (RR) of chance .com. Next, the attacker commands zombies to send queries to their domain name servers for the text RR of chance.com, with the zombies' IP address which is spoofed to be the victim's IP address. When the domain name servers that receive queries allow recursion, they recursively query the reliable name server of chance .com for its text RR and get the reply to the source IP address, which is the address of the victim.

ICMP Attacks: Internet Control Message Protocol (ICMP) flood attacks have existed for many years. They are among the oldest types of DoS attacks. In ICMP flood attacks, the attacker overwhelms the targeted resource with ICMP echo request (ping) packets, large ICMP packets, and other ICMP types to significantly saturate and slow down the victim's network infrastructure.

Transport Layer Attacks: There are number of attacks those have adverse effect on application layer incloud:

Request-Flooding Attacks: These attacks send high rates of legitimate application-layer requests (e.g., HTTP GETs, DNS queries and SIP INVITEs) to a server in an attempt to overwhelm its session resources.

Asymmetric Attacks: These send normal rates of "high-workload" requests. For example, a single request from a client generates a large amount of work for a Web server. The objective of these attacks is to consume large amounts of server resources such as CPU, memory or disk space in order to severely degrade the service or bring it completely down.

Repeated One-Shot Attacks: These send a high workload request across many TCP sessions. This is a stealthier means of executing request-flooding and asymmetric application-layer attacks, but the goal is still the same-to degrade or bring down the service.

Application-Exploit Attacks: These deliberately target vulnerabilities in applications- causing a fault in a server's operating system or applications and allowing the attacker to gain control of the application, system or network. Examples include scripting vulnerabilities, buffer over flows, cookie poisoning, hidden field manipulation, cross-site scripting and Structured Query Language (SQL) injection.

VII. RELATED WORK

Since the creation of computer networks and the expansion of Internet security issues of data transfer and storage, it was an important and growing importance of the subject is enhanced because the advancement of technology and the transfer of data from high-volume, high importance requires channels with a greater safety factor for transferring data is felt. Accordingly, in this section we review presents offers and prior business to improving data security, especially in a cloud environment. Tsai W, et al within [5], framework of four-layer for the development of Web-based was made it interesting, but only one aspect of security in this process is discussed. Sources separation offer`s take place to ensure data security during the process, by separating processor`s cache in the virtual machines and separation of the virtual cache from hypervisor cache [6]. In reference [7], a security framework by different methods provided dynamically, that one of the components of this framework refers to provide data security by storage and access to data based on meta-data, which is similar to storing related data in different areas based on metadata, and if the destruction of user data takes place, it can be retrieved. Each part of the framework in "security as a service" is provided for practical applications by providers of security as a layer or multiple layers of required applications [7]. This research explains the concept of cloud security and the security system in the real world where security is depend on poses of individuals and organizations. Perhaps this is a good offer, but it should be clear that is security as a service provides with delivers service? In this case, the service provider must be put part of its focus on providing security and this is not good because it maybe decrease the growing of providing application services [7, 8]. M. Ahmed et al. [9], the accuracy of certain security issues related to cloud computing have examined and its aim is to explore and establish a secure channel for communication INO with the CSP, while the reliability and confidentiality of information is maintained. In addition, they have compared the provided protocol by the SSL of the activities associated with the work, along with the trustworthy security way to securing data. In the paper [10], the security problems at different levels of the architecture of cloud computing services have been studied. Security of customer-related data is a substantial need for services which is provided by each model of cloud computing [10]. They have studied matters of on-going security software as a service (SaaS), platform as a service (PaaS) and Infrastructure as a Service (IaaS). This paper focuses on the use of cloud services and security for working cross-domain Internet connected [10].

VIII. MITIGATION TECHNIQUES AGAINST ATTACKS

Attacks have severe effect on the cloud services provided by cloud provider to the users or companies. It results in scarcity of resources and services to the intended users and applications are no more available to them. So, it is very important to detect and prevent these attacks. There are number of detection and prevention techniques available for the security of cloud against various attacks.

Detection Techniques against Attacks: There are number of techniques available to detect the impact of attacks:

Covariance matrix Approach: Covariance-matrix statistical approach has been used for flooding based DoS attack detection, covariance-matrix depend on study and monitor of network traffic features correlativity changes and compare the covariance matrix of normal traffic and any new observed traffic and classify the comparison results according predefined threshold and finding the degree of anomaly of new captured traffic and normal traffic profile, and implementation of this approach has proven more accuracy and efficiency through simulation experiments to two of most famous flooding based attack Neptune and Smurf attacks.

Cloud Trace Back Method: The Cloud Trace Back (CTB) is a method where the detection is performed at the edge routers in between the clients and web servers. The main objective of this method is to apply a SOA approach to Trace Back methodology, in order to identify the true source of a DDoS. In a CTB framework, Cloud TraceBack Mark (CTM) is placed within a web service message [6].It marks the request from the client with CTB Marker within header. All service requests are first sent to CTB which prevents the direct attack on the web servers. The attack client will then formulate a SOAP request message based on the service description. Upon receipt of SOAP request message, CTB will place a CTM within the header. Once the CTM has been placed, the SOAP message will be sent to the Web Server. When attack is detected the victim will ask for reconstruction to extract the mark. This will help in tracing the source. The cloud protector detects and filters the attack. However, the detection and filtering of attack starts only after the attack traffic reaches the victim. The message is normal, the SOAP message is then forwarded to the request handler for processing. Upon receipt of the SOAP request; the Web Service will prepare a SOAP response. The web server then takes the SOAP response and sends it back to the client as part of the HTTP response.

Intrusion detection system (IDS): It is an essential component of defensive measure to protect network and computer system against various attacks. It is defined as techniques which are used to detect and respond to the intrusion activities from malicious host or network. The key feature of IDS is its ability to provide the view of unusual activity and to generate the alerts in order to notify the administrators and/or block the suspended connection. IDS tools are capable of distinguishing between the insider attacks, inside the organization and external ones (attacks and the threats by hackers). If an intrusion has been detected, IDS issues alert as notification [11]. These alerts are based on true positives or true alarms when actual intrusion takes place and false alarms in case of wrong detection of the system. There are two types IDS:

1. Signature Based Detection: This method uses specifically known patterns of unauthorized behavior, called signatures, to predict and detect subsequent similar attempts.This method is extremely accurate for known attacks. It produces a low false alarm. With the help of this technique, we can cover a broader range of unknown attacks.
2. Anomaly Based Detection: Anomaly detectors are designed to identify abnormal patterns of behavior on a host or network. It functions on the assumption that attacks are different from normal activity and can be detected by systems that recognize these variations.

Entropy Based Method: The entropy algorithm first builds a profile of the network's normal behavior monitored at selected networks nodes, in the absence of any attack. In fact given a certain PSN setup (i.e. topology, routing algorithm, and source load) a natural level/value of entropy, a sort of fingerprint of the given PSN setup, characterizes normal PSN operation, i.e. normal traffic. Whenever, the entropy deviates from this profile, it means that some vulnerable traffic anomaly is emerging. Detecting shifts in entropy in turn detects anomalous traffic.

IX. PREVENTION TECHNIQUES AGAINST ATTACKS

There are several useful techniques that not only detect these attacks but also prevent and filter them.

Hop Count Filtering Technique: This method uses the relationship of source IP address and TTL value to carry out filtering. The inspection algorithm extracts the source IP address and the final TTL value from each IP packet. The algorithm infers the initial TTL value and subtracts the final TTL value from it to obtain the hop-count. The source IP address serves as the index into the table to retrieve the correct hop-count for this IP address. If the calculated hop-count matches the stored hop-count, the packet has been authenticated otherwise; the packet is likely spoofed

CBF Method: This method focuses our probe on transport and network layers. In order to discriminate attack packets from legitimate ones, this method utilizes correlation patterns. CBF utilizes the attribute value pairs in TCP and IP headers to construct correlation patterns. The concept of correlation refers to the situation that some interior characteristics and there are indeed some unique correlation patterns in legitimate packet flows. The correlation patterns in network and transport layers are the co- appearances between attributes in IP header and TCP header. These attribute pair patterns are distinctive because certain characteristics of the operating system, network structure and even hobbies of users can affect the values of these attributes, and thus make some attribute pairs related.

Port Hopping Technique: This approach is an end point based solution to DoS/DDoS protection, in that changes are made to the servers or clients, but not to the Internet routers. The tests are carried out by the end hosts, and can be conducted at the network layer (IP), transport layer (TCP) application layer. PRNGs are algorithms that use mathematical formulae or simply pre calculated list of tables to produce sequences of numbers that appear randomly. .Let Pi represents the port number used by the server in time slot Si. k is a shared cryptographic key between the server and the client communication and f is a pseudo-random number generator. When a client needs to communicate with the server, it will identify the servers current port number Pi using the shared secret key k and the time slot number i. When the server receives packets of data that carry invalid port numbers, they can be easily detected and filtered off.

Ingress/Engress Filtering: Ingress Filtering, proposed by Ferguson et al., is a restrictive mechanism to drop traffic with IP addresses that do not match a domain prefix connected to the ingress router. Egress filtering is an outbound filter, which ensures that only assigned or allocated IP address space leaves the network. A key requirement for ingress or egress filtering is knowledge of the expected IP addresses at a particular port.

X. EXISTING ALGORITHMS FOR DATA STORAGE SECURITY

RSA algorithm: Today RSA algorithm is one of the public key cryptography algorithms used for encryption and decryption by many vendors. This is the first generation algorithm that used for providing security to data [18]. It can encrypt a message without the need to exchange a separate secret key. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers. Party A1 can send an encrypted message to party B1 without any prior secret keys exchange. A1 uses B1's public key to encrypt the message and B1 decrypts it using the private key, which only he knows. RSA can also be used to sign a message, so A1 can sign a message using their private key and B1 can verify it using A1's public key [18].

Elliptic Curve Cryptography (ECC) algorithms: Elliptic Curve Cryptography is a secure and more efficient encryption algorithm than RSA as it uses smaller key sizes for same level of security as compared to RSA. For example a 256-bit ECC public key provides equivalent security to a 3072-bit RSA public key [28]. Elliptic Curve Cryptography (ECC) was introduced in 1985 by Victor Miller (IBM) and Neal Koblitz (University of Washington) as an alternative mechanism for implementing public-key cryptography. Public key algorithms provide a mechanism for sharing keys among a large number of participants in a complex information system. Compared to other famous algorithms such as RSA, ECC is based on discrete logarithms that are much more difficult to challenge at similar key lengths [19]. Every participant in the public key cryptography will have two keys, apublic key and private key, used for encryption and decryption operations. Public key is distributed to all the participants where as private key is known to a particular participant only.

Data Encryption Standard (DES): Data Encryption Standard (DES) is a block cipher with 64 bits of block size. It was developed by IBM in the 1970s, and adopted in the United States of America as a standard encryption technique in 1976. Firstly it was mostly used in the United States of America, and then it became more and more popular around the world. DES is using substitutions and transpositions one after other in 16 cycles in a very complicated way [19]. For this algorithm, key length is fixed to 56 bits, which seems too weak while it has been proved that the power of computing resources is getting more and more. However it is useful to mention that 3DES, also called triple DES, is a method to make DES more difficult to decode. 3DES uses DES three times on every data block,

and in this way the length of the key is increased. In fact it uses a “bunch of keys” containing three DES keys, K1, K2 and K3, which each of them is 56 bits [15].

Advanced Encryption Standard (AES): The weakness of the DES has been accepted; In January 1997 NIST (National Institute of Standards and Technology) announced that instead of DES, a new method will be used as the AES (Advanced Encryption Standard). It led to a competition between the open cryptographic community members, and in nine months, NIST received fifteen different algorithms from several countries. In 1999, from the received algorithms NIST choose the algorithm “Rijndael”, which was developed by two Dutch cryptographers, Vincent Rijmen and Joan Daemen [17]. This algorithm officially became the encryption algorithm for AES in 2001. AES is a block cipher with 128 bits of block size. In AES key length is variable (not fixed), then it can be 128, 192, and 256 bits (and probably more). The structure of AES is mainly created from Encryption techniques such as substitutions and transpositions [15]. Same as DES, AES uses repeated cycles, which are 10, 12 or 14 cycles (called rounds in AES). In order to achieve perfect confusion and diffusion, every round contains four steps. These steps are substitutions, transpositions, shifting the bits and applying exclusive OR to the bits [13].

XI. CONCLUSION

As noted in the system of cloud data storage, users store their data in the cloud, so there is no need to store them locally. Therefore, the security, integrity and availability of data files on storage distributed cloud servers are guaranteed. To accomplish this, the structure and security solutions of involved elements in the process of data storage in the cloud environment should be investigated. About the data of the client; we suggest to use an encryption mechanism from the customer like AES encryption that its high security and resistance has been proven in many testing. AES has been investigated and analyzed by the NIST and its security has been approved by this validated Institute, and this encryption is used to encrypt sensitive information in the United States of America. Also we can use encryption algorithm by means of new methods like genetic algorithm or other dynamic algorithm which security can increase dramatically in this way.

XII. REFERENCES

[1] H.Takabi, J.B.D.Joshi, G.Ahn., “Security and Privacy Challenges in Cloud Computing Environments”, IEEE Security Privacy Magazine, Vol 8, pp.24-31, 2010.

[2] F. Soleimanian, S. Hashemi, “Security Challenges in Cloud Computing with More Emphasis on Trust and Privacy”, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, Vol. 1, ISSUE 6, pp. 49-54, 2012.

[3] M.Monsef, N.Gidado, “Trust and privacy concern in the Cloud”, 2011 European Cup, IT Security for the Next Generation, pp. 1-15, 2011.

[4] D Zissis, D Lekkas, “Addressing cloud computing security issues, Future Generation Computer Systems”, Elsevier B.V, Vol.28, pp.583-592, 2010.

[5] Tsai W, Jin Z, Bai X.,”Internetware computing: issues and perspective.” Proceedings of the first Asia-Pacific symposium on Internetware. Beijing,China: ACM, pp. 1–10, 2009.

[6] Raj H, Nathuji R, Singh A, England P. “Resource management for isolation enhanced cloud services.”, Proceedings of the 2009 ACM workshop on cloud computing security, Chicago, Illinois, USA, pp. 77–84, 2009.

[7] S Subashini, V Kavitha, “A survey on security issues in service delivery models of cloud computing”, Network and Computer Applications, Elsevier, Vol. 34, pp. 1-11, 2010.

[8] KapilSachdeva, Cloud Computing: Security Risk Analysis and Recommendations, Master Thesis, University of Texas, Austin, 2011.

[9] Mahbub Ahmed, Yang Xiang, Shawkat Ali, “Above the Trust and Security in Cloud Computing: A Notion towards Innovation”, 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, pp.723-730, 2010.

[10]V.KRISHNA REDDY, Dr. L.S.S.REDDY, “Security Architecture of Cloud Computing”, International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 9, pp.7149-7155, 2011.

[11] Siani Pearson, “Privacy, Security and Trust in Cloud Computing”, HP Laboratories, appeared as a book chapter by Springer, UK, 2012.

[12] Fariborz farahmand, “Risk Perception and Trust in Cloud”, ISACA JOURNAL VOLUME 4, pp.1-8, 2010.

[13] Weiss, A.; “Computing in the Clouds,” netWorker, vol. 11, issue 4, p.16-25, 2007.

[14] Mohamed Al Morsy, John Grundy and Ingo Müller, “An Analysis of The Cloud Computing Security Problem”, In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30 Nov 2010.

[15] M. Firdhous, O. Ghazali, and S. Hassan, Trust and Trust Manage-ment in Cloud Computing – A Survey, Inter Networks Research Group, University Utara Malaysia, Technical Report UUM/CAS/InterNetWorks/TR2011-01, 2011.

[16] T. Mather, S. kumaraswamy, S. Latif, Cloud Security and privacy: an Enterprise perspective on Risk and Compliance, Governance An International Journal Of Policy And Administration, O'Reilly Media, Inc., p. 312, 2009.

[17] D. Jamil, H. Zaki, Security Issues in Cloud Computing and Countermeasures, International Journal of Engineering Science and Technology, Vol. 3, No. 4, p. 2672-2676, 2011.

[18] Yashpal Kadam, “Security Issues in Cloud Computing A Transparent View”, International Journal of Computer Science & Emerging Technologies, Vol-2 No 5 October, 2011.

[19] S. Qaisar, K.F. Khawaja, Cloud Computing: Network/Security Threats and Countermeasures, Interdisciplinary journal of con-temporary research in business, Vol.3, No 9, p. 1323-1329, 2012.

[20] J.R. Winkler, Securing the Cloud: Cloud Computer Security Techniques and Tactics, Technical EditorBill Meine, Elsevier Publishing, 2011.

[21] K, Sachdeva, Cloud Computing: Security Risk Analysis and Recommendations, Master Thesis, University of Texas, Austin, 2011.

[22] J. Hurwitz, R. Bloor, M. Kaufman, F. Halper, Cloud computing for dummies, Wiley, 2009.

[23] Z. A.Khalifehlou, F. S. Gharehchopogh, “Security Directions in cloud Computing Environments”, 5th International Conference on Information Security and Cryptology (ISCTURKEY2012), Ankara, Turkey, pp. 327-330, 17-19, 2012.

[24] B. Shwetha Bindu, B. Yadaiah, “Secure Data Storage In Cloud Computing”, International Journal of Research in Computer Science, Vol 1 Issue 1, pp. 63-73, 2011.

[25] Abbas Amini, Secure Storage in Cloud Computing, Master Thesis, Technical University of Denmark, Kongens Lyngby, Denmark, 2012.