Preet Dabhi CWID: 10459151

Assignment 2

Assessment on potential security threats and introducing novel data security model in cloud environment

Cloud computing in the recent years has emerged a lot and has many advantages such as scalability, quick elasticity, and one of the most important is cost savings, but at the same time it has security risks as well. Most of the data are kept on the severs and it can be accessed through a simple one factor authentication system from wherever on the globe. These systems are vulnerable most of the time and can be very easy to infiltrate the system and steal the data. This paper describes the possible various attacks which can happen on the cloud computing and ways to solve these problems.

There are multiple cloud computing layers an organization can have such as SaaS, PaaS and IaaS, and various models such as **private cloud** which have high costs to develop a private infrastructure, **public cloud** which have a higher security risks and lack of customization, **community cloud** have a shared infrastructure which can be disadvantage to many organizations and **hybrid cloud** which have a high challenge in integration. Each of these models have some threats and security concerns associated with it. Despite the many advances in the R&D and technology cloud security still has a lot of flaws. Data is the most precious to any organization as it contains sensitive information about its users, an attacker can gain the personal data and might sell it to other companies, Application program interfaces are used by cloud services providers to deliver range of services to the consumer which leads to lack of protection authentication and the attacker can easily manipulate, listen to the data and perform assaults to the system. The data which is lost in irreversible and cannot be retrieved back, these attackers use advanced persistent threats on the system, they use complex tactics such as direct hacking, phishing network infiltration which gives them access to the infrastructure and can cause major damage to the system with the system knowing about it.

There are potential cloud attacks that can happen such as **DDOS (Distributed Denial of Service)** in which there is a heavy request sent to the system which makes the system more vulnerable to rejection this can make the system down for a while which can make a huge impact on cloud systems which needs to be up and ready all the time, **Malware infiltration in the cloud** in this type of attack a malware machine acts as an imposter VM machine and it makes itself act as an infrastructure and waits to the data to be stored on it so the attacker can steal the data, **Authentication- related attacks** in these type of attacks the attacker tries to infiltrate the system acting as a user, this can be achieved but doing a brute attack on the system , they can even try to attack by trying to bypass any two factor or biometric authentication system**, Attacks on the middleman** in this attack the hacker listens to the exchange of keys and tries to change the package to their package and this gives them access to the system. To protect the cloud system to be attacked from such attacks organizations should use hardware security models and AES algorithms.

There are a lot of AES algorithms which are better in terms of security but have very huge delay in them, which relates to a tiny variation, such minor delays and variations can cause a lot of problems in cloud systems since they need to be active and running all the time and most of the organizations relay on cloud systems. These variations are seen because of the encoding and decoding and the collector might have to repeat thousands of bits. To avoid such delays cloud computing systems needs to have complex mathematical and organized algorithm capable of handling a huge amount of data and speeds. The suggested model in this paper which is (blowfish) it uses the ciphers AES and RSA to help given additional protection layer to the data stored in the cloud. RSA algorithm uses key paring and follows a public key encryption algorithm. Without exchanging secret keys, Client A delivers a communication to Client B that is encrypted. For the cipher message, only B's public key is used, and B only uses the private key that he knows.

But there is a better algorithm which can be used which is the blowfish algorithm it is a free, patented and unlicensed encryption algorithm. It is a 16 rounds and lengthy S chests it is the same as CAST-128 but the difference in this one is that it has S squares on the frame which are fixed with each line being 23-bit values. There are five primary ranges: an 18P range and four 265 S-boxes. The 32-bit Ip is split into four 8-bit quadrants and utilized as S-box input. S-is available in 8-bit I/p and 32-bit o/p formats. The last 32-bit outputs are XORed and performed at 232. According to the study conducted where various advanced encryption systems (RSA) and blowfish were used on IoT devices it showed that blowfish outperformed the other AES algorithms in terms of security, efficiency and speed. It showed that blowfish is far quicker than AES models, but in terms of dependability, storage space, data extraction speed and time AES models are still better.

I personally think that there much more scope in blowfish algorithm, if more time and efforts are given in developing the algorithm in terms of dependability and scalability it can outperform the other AES algorithms and it can replace the existing AES algorithms used in cloud computing, it can improve the overall performance and the security of the systems at the same time. As the number of keys used in blowfish are less, we can see that it can outperform the current algorithms. The main points that this paper covered were the security threats that are faced in cloud computing and how we can solve them using the new algorithms. To make the system stronger to the possible threats it has to have layers of encryption and decryption on the cloud, but the suggested approach is a cross level of encryption and decryption, this method only gives access to the individual who has the access to that layer and no one else, this makes it very difficult to break the system and even if the attacker gets the details of the system it still needs to be decrypt which is very difficult, therefore it provides the best security to the cloud systems.

Reference Paper: https://www.sciencedirect.com/science/article/pii/S2214785322018855