Cloud Computing Security Issues

Vineesha Thallapaneni

Abstract

Cloud computing, "the practice of using the cloud" is a virtual storage place where people can store, share and run their data. Back when it first started out, the security level was not that sophisticated thus making it vulnerable to attacks. As time passes, people have leveled up the defense in the cloud. It is an internet – based computing that provides shared processing resources and data to computer and other devices on demand. Current data encryption mechanism might not be so strong to provide true privacy and reliability. In this paper, we presented an approach to data security that combines data encryption with salted password hashing. The effectiveness of the suggested strategy is confirmed by contrast with the present conventional security approach based on the security parameters. The issues of data availability, location, storage, backup or recovery, data integrity, confidentiality and privacy, and data authentication are all mentioned in the paper. Additionally, certain workable solutions such as network-based intrusion prevention systems, strong data encryption, routine audits, and compliance were discovered.

Introduction

Cloud Computing is one of the highest-rated computing services in the IT sector. A model for providing ubiquitous, practical, on-demand network access to a pool of configurable shared computing resources that can be quickly supplied and released with little administration work or service provider contact is called cloud computing. Capital formerly invested on services like infrastructure, software, and other items has decreased as a result of cloud computing. IaaS, PaaS, and SaaS are the three main service models offered by cloud computing. On a pay-per-use basis, IaaS offers fundamental computing and storage services over the network, including servers, processing, data centers, storage, and routers. PaaS offers a cloud-based platform where new services can be developed. PaaS occasionally offer API that can be used to build various applications and services. SaaS offers cloud-based software services that enable multiple individuals or organizations to access the same instance of an application from a single provider. The implementation of the pay and use model in cloud brings efficiency on resource utilization. A cloud computing paradigm that combines widespread computer networks, storage, servers, services, and applications makes it simple to create a shared pool of resources that can be deployed fast and without restriction with little administrative labor and contact with service providers. Cloud storage, a product of cloud computing technology, refers to the decision to store data in online storage services supplied by cloud service providers. Google Drive, iCloud, Amazon Web Services, and Dropbox are just a few of the most popular cloud storage options. However, there is a persistent risk to the security of the documents posted online and kept in these cloud storage facilities. The protection of data and applications using cloud services is achieved through a variety of solutions known as cloud security. Cloud security therefore continues to be a key factor in order to take use of the different opportunities offered by cloud technology.

Background Information

Cloud computing models

The service model is the foundation for cloud computing, or we could argue that it serves as its reference model. The three fundamental models that make up the backbone of the service model are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service. The service model is made up of many different models (SaaS). The "Anything as a Service" paradigm also includes other models, such as "Business as a Service," "Strategy as a Service," "Network as a Service," and others.

Infrastructure as a Service (IaaS)

The most basic level of service model is IaaS. It distributes resources like servers, virtual computers, and storage as a service over the network. In this architecture, a third-party supplier manages all the infrastructure's elements (hardware, storage, software, etc.). Clients have no influence over the activities of the infrastructure's parts. The third-party supplier oversees managing duties including maintenance, backup, and recovery planning. Iaas is a very flexible on-demand platform that may be modified depending on the type of workload. Users are charged on a pay-per-use basis.

Platform as a service (PaaS)

When using the cloud, Applications are delivered via the internet using the platform as a service paradigm. Cloud service providers offer hardware and software tools to its consumers as a service. Users are unable to manage cloud infrastructure, i.e., they do not need to install hardware or software locally; instead, cloud providers, who host the gear and software, do this task. Only the applications that the user has downloaded are accessible. This does not imply that the PaaS replaces the entire corporate infrastructure; rather, consumers simply need some critical services, such as Java programming tools.

Software as a Service (SaaS)

When using the cloud, distribute software as a service using the SaaS paradigm. The program is hosted by a third party, who also distributes the software to the app's numerous users. Users have no control over the storage, application capabilities, or cloud infrastructure. Applications don't need to be installed or operate on internal PCs when using a SaaS approach. It fixes the issues with maintenance, license renewal, and support. Instead of purchasing the software, consumers can just sign up for SaaS offerings and pay for them on a pay-per-use basis.

Aspects of security and privacy related to cloud providers

The use of cloud technology requires the authentication and permission of users. Typically, identifying techniques that are always predefined are used for this. It is necessary to modify data items in order to make sure that any resources required are available. De-provisioning services from heterogeneous suppliers are expected to guarantee seamless identity management and access. Individually Identifiable Information is designed to be shielded from any hostile cloud-based attacks. This makes sure that privacy needs are met. In order to guarantee that regulations are properly stated and upheld, policy management is essential. This may be improved by taking steps that include, but are not limited to, auditing and providing evidence of compliance. Monitoring the cloud's infrastructure makes sure that regulations are followed in terms of guaranteeing consumer security. It is worth noting that no single algorithm is 100 percent secure from any security breaches. The key management tool was developed in order to ensure that an individual can select a party that will manage their security features. Key length also plays in superbly. In the case of a symmetric encryption, it has been noted that the length. of the key is proportional to the encryption strength.

Security of Cloud

There are various lessons to be learned while examining infrastructure security at its three levels—application, host, and network.

Cloud computing is a symptom of a broader set of security vulnerabilities that affect networks but are not directly related to it. Cloud will only make these issues worse [4]. The same holds true for host-level features, such as the increased requirement for host perimeter security and the security of virtualized environments. This is true at the application level as well.

As a result, it becomes necessary to make sure that software development life cycles are properly protected and/or secured. This is because cloud applications are public facing. Concerns about privacy in the cloud

Without recognizing it, security and privacy are frequently used synonymously. However, one might have data security while still not having adequate privacy protections. Lack of security in and of itself can immediately result in a lack of privacy [11]. The issues about privacy with the cloud must therefore be addressed in a systematic manner, and any company will find it difficult to do so due to both local and worldwide legislation.

With the necessity to emphasize compliance in connection to cloud privacy, compliance is a big challenge. Clouds have been shown to transcend multiple legal jurisdictions; therefore, it is crucial to prevent loopholes from developing in such circumstances.

The proposed approach to provide data security:

In this part, a straightforward yet effective approach for safely storing and accessing data from the cloud computing infrastructure has been presented. Here, the two separate approaches have been integrated to offer the highest level of cloud data protection. Data encryption and password hashing are the techniques. Data encryption is the process of encrypting data with the use of an encryption key, which renders it unintelligible until it is converted back to its original form using a password or decryption key. The privacy and secrecy of the data can be readily preserved by encrypting it before uploading to the cloud storage. Here, we're going to employ asymmetric key encryption, where the encryption key is made public so that multiple people working for the same company can use it to encrypt the data before it's uploaded to the cloud. The asymmetric encryption approach maintains the decryption key in confidence so that only the chosen user with whom the organization wishes to share the data will have access to it. The empowerment of the keys ensures the security of the encrypted data that is kept in the cloud. However, modern techniques such as brute-force attacks, dictionary attacks, lookup tables, reverse lookup tables, rainbow tables, etc. can be used to crack passwords. These are all straightforward but effective hacking techniques. So, there is cause for concern regarding the security of cloud data. Here we propose a salted password hashing method, which is a one-way function, to address the cloud security issue. Therefore, using the salted hashing technique, encryption in one direction is simple, but decryption in the opposite direction is practically impossible. In certain sophisticated hashing algorithms, it is a fixed-length collection of strings that includes both random numbers and letters. Additional use of special characters string serves as an authentication "fingerprint" for the password. The hashed string will be entirely different if the password is altered even slightly. The asymmetrically encrypted private key will be more secure thanks to hashing. But in order to stay one step ahead of security, we'll employ a method called salted password hashing. The section that follows provides a more thorough explanation of this strategy.

The new data security algorithm is powered by Asymmetric data encryption, in which the encryption key is made public, but the decryption key is kept secret, is used to encrypt the data on the cloud. Private Key Generation: The first step in the proposed model is the generation of the private key which can only be generated once the data is encrypted using the most secure encryption algorithm like Triple DES, RSA, Blowfish etc. The private key will be generated following the data's encryption, further enhancing its security. Private key salted hashing, the next step is to strengthen and impenetrably secure the private key after it has been generated. Salted hashing is employed in order to achieve this goal.

Prior to storing the hashed string, the private key is first hashed using a secure hashing function, such as WHIRLPOOL, Ripe MD, SHA512, or SHA256. • The salt, which is a random string, is then taken, hashed, and saved. • The hashed salt is now added to or prepended to the hashed private key to combine the hashed salt and the hashed private key. The final key is then generated, and the combination is once more hashed. This is the safest method for safeguarding data on the cloud. Only the private key can be decrypted most effectively if a hacker attempts to decrypt the encrypted material using the digital signature of the private key. However, since our authentication is based on the final hash, the data cannot ever be decrypted. The cloud service provider will supply the salt, and the authorized individual will keep the private key secure. Data access with key authentication: The access to the cloud-based data will be the last step. By providing the private key, the user will ask the cloud server to retrieve the needed data. If both the requested file and the private key are valid, the cloud server will choose the appropriate salt and hash the data. If the final key matches the decryption key, the user is authorized, and the data is provided later, it will hash it once again with the hashed private key that was previously entered. As a result, the entire process can be summarized by noting that the sender's data is first encrypted using public key encryption. The encrypted data would then be uploaded to a cloud server, maintaining the confidentiality of the data. By using a salted hashed private key, the cloud-hosted encrypted data can be downloaded and then restored. The authenticated user who possesses the private key can decode the data in this case. can be reverse encrypted by the authorized user who possesses the private key.

Conclusion:

One of the primary concerns is the security of data in cloud computing infrastructure, which can be more effectively addressed by using cryptographic approaches. In order to address the security issues, we have combined two separate techniques—asymmetric data encryption and salted password hashing—in this paper's solution proposal. In our method, the user's data is first encrypted using a public key, and then the private key is hashed with a random salt to make the encryption unbreakable and the private key secure. The suggested method is quick and more secure, and it is also quite simple to use. The risk of data leakage and worldwide cloud theft can both be significantly decreased by encryption. Lately, we have shifted toward storing our personal data in the cloud architecture. Therefore, creating a secure environment is crucial for using new cloud technology.

.

REFERENCES

[1] [1] Buyya, Rajkumar and et al. "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility." Future Generation computer systems 25.6 (2009): 599-616. PDF.

[2] Dhar, Subhankar. "From outsourcing to Cloud computing: evolution of IT services." Management Research Review 35.8 (2012): 664-675. PDF.

[3] Ferkoun, Maamar. How cloud computing is impacting everyday life. 4

April 2013. Webpage. 16 April 2018. <https://www.ibm.com/blogs/cloud-computing/2013/04/04/how-cloudcomputing-is-impacting-everyday-life/>.

[4] Fernandes, Diogo AB and et al. "Security issues in cloud environments: a survey." International Journal of Information Security 13.2 (2014): 113170. Document.

[5] Kalaiprasath, R, R Elankavi and D.R Udayakumar. "Cloud. Security and Compliance-A Semantic Approach in End to End Security." Cloud. Security and Compliance-A Semantic Approach in End to End Security.
8.5 (2017): 2-47. Print.

[6] Krutz, Ronald L and Russell D Vines. Cloud security: A comprehensive guide to secure cloud computing. New York: Wiley Publishing, 2010. Document.

[7] Kshetri, Nir. "Privacy and security issues in cloud computing: The role of institutions and institutional evolution." Telecommunications Policy 37.4-5 (2013): 372-386. PDF.

[8] Majhi, Santosh Kumar and Sunil Kumarr Dhal. "A Study on Security
Vulnerability on Cloud Platforms." Procedia Computer Science 78 (2016):
55-60. PDF. <https://www.sciencedirect.com/science/article/pii/S1877050916000120 >.

[9] Mather, Tim, Subra Kumaraswamy and Shahed Latif. Cloud Security and Privacy. Carlifonia : O'Reilly Media, 2009. PDF.

[10] Ohkubo, Miyako, Suzuki Koutarou and Kinoshita Shingo. "RFID privacy issues and technical challenges." Communications of the ACM 48.9 (2005): 66-71. PDF.