Enhancing Cloud Security with the Implementation of Serpent Encryption Algorithm

Prathibha Simha. S & Prof. Hari Priya
Jain University

Abstract: Cloud computing plays an important role in the IT world for an individual as well as an organization. It provides services in infrastructure (IaaS), platform (PaaS), software (SaaS) and major ones like file storage and securing them from misuse. When it comes to security, protection of data has been a major challenge and where a huge amount of data is involved, it's difficult to maintain that huge amount of data and safeguard them from intruders. As new concepts get introduced into the cloud like resource sharing, outsourcing, new challenges arise in the cloud security domain. In order to tackle these security issues, cryptography has been brought into provide many encryption algorithms to encrypt the cloud files. In this paper, I would like to bring up the idea of implementing the Serpent encryption algorithm to enhance the security in cloud and making it hard for intruders to access it.

Keywords: cloud computing, benefits, cryptography, algorithm, serpent encryption data security.

1. INTRODUCTION

Cloud computing has provided its best services to the users using internet technologies and along with that has contributed a lot to the industries. Every individual is connected to their benefit needs through the cloud. It is evolved from grid computing, distributed computing and virtualization. As per NIST cloud computing, its divided into different categories as private, public community and hybrid. Cloud provides its facilities like infrastructure as a service, platform as a service and software as a service.

2. BENEFITS OF CLOUD COMPUTING

2.1 Flexibility

Cloud-based administrations are perfect for organizations with developing or fluctuating transmission capacity requests. On the off chance that your needs increment it's anything but difficult to scale up your cloud limit, drawing on the administration's remote servers. In like manner, in the event that you have to downsize once more, the adaptability is prepared into the administration. This level of spryness can give organizations utilizing distributed computing a genuine favorable position over contenders.

2.2 Disaster recovery

Organizations of all sizes ought to put resources into vigorous debacle recuperation, however for smaller organizations that do not have the required money and mastery, this is regularly more a perfect than the truth. Cloud is currently helping more associations avoid that pattern.

2.3 Capital expenditure free

Distributed computing removes the high cost of equipment. You basically pay as you go and appreciate a membership based model that is benevolent to your income. Add to that the simplicity of setup and administration and abruptly, your terrifying, bushy IT anticipate takes a gander at part friendlier. It's never been simpler to venture out cloud reception.

2.4 Increased collaboration

At the point when your groups can get to, alter and share reports at whatever time, from anyplace, they're ready to accomplish all the more together, and improve. Cloud-based work process and document sharing applications help them make refreshes continuously and gives them full perceivability of their joint efforts.

2.5 Security

Lost portable PCs are a billion dollar business issue. What's more, conceivably more prominent than the loss of a costly bit of pack is the loss of the delicate information inside it. Distributed computing gives you more noteworthy security when this happens. Since your information is put away in the cloud, you can get to it regardless of what happens to your machine. Furthermore, you can even remotely wipe information from lost portable PCs so it doesn't get into the wrong hands.
2.6 Environmentally Friendly
While the above focuses spell out the advantages of distributed computing for your business, moving to the cloud isn’t a completely egotistical act. The earth gets a little love as well. At the point when your cloud needs change, your server limit scales all over to fit. So you just utilize the vitality you need and you don’t leave curiously large carbon impressions. This is something near our souls at Salesforce, where we attempt our best to make reasonable arrangements with insignificant ecological effect.

3. BACKGROUND STUDY AND PROBLEM FORMULATION
Cloud administrations are mainstream since they can lessen the cost and intricacy of owning and working PCs and systems. Since cloud clients don’t need to put resources into data innovation framework, buy equipment, or purchase programming licenses, the advantages are low in advance costs, fast degree of profitability, quick sending, customization, adaptable utilize, and arrangements that can make utilization of new developments. Likewise, cloud suppliers that have had some expertise in a specific range, for example, email) can bring propelled administrations that a solitary organization won’t not have the capacity to bear the cost of or create.

Some different advantages to clients incorporate versatility, unwavering quality, and proficiency. Versatility implies that distributed computing offers boundless preparing and capacity limit. The cloud is dependable in that it empowers access to applications and reports anyplace on the planet by means of the Internet. Distributed computing is frequently viewed as proficient on the grounds that it permits associations to free up assets to concentrate on advancement and item improvement.

Another potential advantage is that individual data might be better secured in the cloud. In particular, distributed computing may enhance endeavors to incorporate protection insurance with innovation from the begin and the utilization of better security instruments. Distributed computing will empower more adaptable IT securing and changes, which may allow conformity to methods in view of the affectability of the information. In the utilization of the cloud which many result in open norms for distributed computing that will build up benchmark information security highlights basic crosswise over various administrations and suppliers. Distributed computing may take into account better review trails. Thus , data in the cloud is not as effortlessly lost (when contrasted with the paper reports or hard drives, for instance).

In cloud computing technology there are a set of policy issues which include issues of privacy,security,anonymity,telecommunications capacity, and others. the highlighted one is security and how cloud assures it.

Cloud generally have many customers like usual users , educational institute and enterprise who have different needs to opt to the cloud. If its educational, security effect is on performance of usage of the data and for this domain cloud provides a combo of security and performance. for enterprise the important problem is security but with different vision .From this , the perspective of different users is security but with point of view is different.

4. EXISTING WORK PLAN
The first level of security where cryptography can help cloud computing is secure storage. Cryptography is a mechanism or science of keeping data secure by converting the data into non readable forms. the current day, cryptography is considered to be a combined form of 3 algorithms i.e symmetric, asymmetric algorithms and hashing. but the main problems are related to data security,backup and network congestion etc to which cryptography can resolve to certain extent. Encryption will help prevent exploits such as man-in-middle, spoofed attacks and session hijacking. Some of the existing algorithms like AES, RSA, homomorphic algorithms, blowfish have played vital role in encryption of data. Many hybrid algorithms have also been proposed to enhance the data security. But cyber criminals can easily crack it whether it’s single level encryption or multilevel . Henceforth, in order to deceive attackers and intruders , single but a strong algorithm can be provided to secure the cloud storage.

5. PROPOSED WORK PLAN
To access a cloud based web application that will try to eliminate the concerns regarding data privacy, segregation.
In this paper, i would like to propose the idea of implementing an encryption algorithm in order to enhance the security of data in cloud environment i.e Serpent encryption algorithm. it has been for the different user perspective, this algorithm has been proposed.

Serpent was designed by Ross Anderson, Eli Biham, and Lars Knudsen.
Serpent is a symmetric key block cipher that was a finalist in the Advanced Encryption Standard
6. HOW SERPENT WORKS

The Serpent is a 128 bit block encryption that uses 32 rounds or 32 reiterations of the same algorithm using mathematical permutations and substitutions. The encrypting and decrypting phase have the same level of complexity. The decryption operations are exactly the inverted transformations used to encrypt the message but in opposite order.

Serpent uses different mathematical substitutions “S-boxes” with a 4 bit entrance and a 4 bit exit. Every encryption phase uses an S-box that work collaterally for the 32 times.

The algorithm consists of three basic functions. These functions are an initial permutation of bits named IP, a Round Function named R, and a final permutation of bits named FP. The initial permutation of bits is frequently performed by table lookup to decide which bit to place in which position. However, it can also be performed algorithmically by replacing a bit at position i with the bit at position \((i*32 \mod 127)\), leaving only bits 0 and 127 in place. The output of this permutation is labeled B0. The round function is performed 32 times on Bi (starting with B0). In each round of the function, Bi is first mixed with one of 32 keys (see Key Schedule below for generation notes) using the exclusive-OR operation and then passed through one of eight SBoxes 32 times in parallel. In all but the last round, it is then subjected to a linear transformation to produce Bi+1. In the last round, instead of performing the linear transformation the text is instead mixed with an additional 33rd key.

Once the round functions have been completed, a final permutation of bits is performed to place the bits back into the correct position. Like the initial permutation this is frequently done via table lookup but can also be done algorithmically. To perform this operation algorithmically, replace the bit at position i with the bit at position \((i*4 \mod 127)\), leaving only bits 0 and 127 in place. The output of this final permutation is the final ciphertext of the algorithm.

7. FLOWCHART

[Flowchart showing encryption and decryption processes]

Fig 1- This flowchart shows how encryption works and reverse of it is for decryption technique.

8. CONCLUSION

Cloud computing offers benefits for organizations and individuals. There are also privacy and security concerns. If you are considering a cloud service, you should think about how your personal information, and that of your customers, can best be protected. This algorithm serves the purpose of cloud security and from the survey done, it is a strong algorithm and considered to be implemented in data security.

9. FUTURE WORK

As the algorithm proposed, in the future work, implementation of this algorithm affects the systems and how it is beneficial can be found.
More simulations and try outs to check its purpose being served correctly can be measure.

10. REFERENCES

1) “TREM: A New Cloud Security Algorithm” V. Poongodi, Dr. K. Thangadurai
2) “Using encryption Algorithms to enhance the Data Security in Cloud Computing” MANDEEP KAUR#1, MANISH MAHAJAN# 
3) “Contriving Hybrid DESCAST Algorithm for Cloud Security” Nandita Sengupta* and Ramya Chinnasamy

5) “Data Encryption Method Using Environmental Secret Key with Server Assistance” Kun-Lin Tsai, Fang-Yie Leu & Shun-Hung Tsai
7) “Designing of Hybrid RSA Encryption Algorithm for Cloud Security” Dr. Nandita Sengupta Assistant Professor, Dept. of I.T.,
9) “An Investigation on Cloud data Storage and Confidentiality Techniques” S. Prabu, Prof. Gopinath Ganapathy