ABSTRACT

The Internet is becoming an increasingly vital tool in our everyday life, both professional and personal, as its users are becoming more numerous. It is not surprising that business is increasingly conducted over the Internet. Perhaps one of the most revolutionary concepts of recent years is Cloud Computing. The use of Cloud Computing is gaining popularity due to its mobility, huge availability and low cost. Many small businesses are realizing that cloud computing isn't just for large corporations. Many providers offer services that are targeted at the small business owner. Cloud computing presents unique opportunities for small businesses, giving them access to infrastructure that had traditionally only been available to much larger organizations. Cryptography is one of the solutions which can prevent the intruders to enter into clouds for hacking information. Our paper gives solution for small scale industry. Out Solutions For Encryption at Small Scale industry, which will work on, Encryption at System Level, Password protected encryption key, disk encryption. This system design in such a way that Disk level encryption is time and space consuming.
INTRODUCTION

Cloud computing is becoming popular day by day. Its performance is distributed in three main places, one in client’s place, one in network and the third is in server’s side. As complete data resides outside premises, maintaining confidentiality is becoming an important issue which needs to be addressed. So, security threat is an aspect to think for cloud computing. Because of this reason, research work for security in cloud computing is gaining attraction of the computer science researchers. Security in cloud computing has three components, detection, correction and prevention from attack. In our paper, prevention of attack is focused. For maintaining confidentiality on data, 3 layer encryption applied. Our system works on client level and server level also. No one can access our data through local internet file. In our system encryption key will be password protected and password will be in encrypted format. Once user will create encryption key then it will encrypted using password. When key will be encrypted then it will encrypted our data and it will store in server. Section II refers Cloud Computing, section III explains Proposed Cryptography System for Cloud, section IV depicts Experimental Results, and section V discusses Conclusion and Future Work.

CLOUD COMPUTING

Cloud computing is computing based on the internet. Where in the past, people would run applications or programs from software downloaded on a physical computer or server in their building, cloud computing allows people access the same kinds of applications through the internet. It is a solution growing in popularity, especially amongst SMEs. The CRN predicts that by 2014, small businesses will spend almost $100 billion on cloud computing services. National Institute of Standards and Technology has defined cloud computing as a model which has convenient on-demand network access for sharing hardware and software resources. Expenditure towards IT infrastructure is very less for cloud computing which is making it popular for many users. Services for cloud is available at any place online. Amazon, Google, IBM, Microsoft are some of the cloud providers. Cloud computing is classified in two ways in general. First classification is based on the location of cloud computing and second classification is based on the different services provided by cloud. According to first category, cloud computing is again subdivided as public cloud, private cloud, hybrid cloud, community cloud. In the second category, cloud computing is primarily subdivided as Infrastructure as a service, Platform as a service, Software as a service. Security of cloud computing is the most vulnerable issue for cloud which is getting focused for future research.
PROPOSED CRYPTOGRAPHY SYSTEM FOR CLOUD

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. Note that - as with any commercial software - the controls they implement may not necessarily fully mitigate all the risks they have identified, and that they may not necessarily have identified all the risks that are of concern to customers. Consequently, customers may also need to assure themselves that cloud applications are adequately secured for their specific purposes, including their compliance obligations.

Providers ensure that all critical data (credit card numbers, for example) are masked or encrypted and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

Encrypted Password

The data in your database is not safe. What if the password to the database is compromised? Then your entire user password database will be compromised as well. Even if you are quite certain of the security of your database, your users' passwords are still accessible to all administrators who work at the web hosting company where your database is hosted. Scrambling the passwords using some home-brewed algorithm may add some obscurity but not true "security." Another approach would be to encrypt all passwords in your database using some industry-standard cipher, such as the Message-Digest Algorithm 5.

Password Protected Encryption Keyword

In cryptography, a key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm or cipher. Without a key, the algorithm would produce no useful result. In encryption, a key specifies the particular transformation of plaintext into cipher text, or vice versa during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and message authentication codes.

Need for secrecy

In designing security systems, it is wise to assume that the details of the cryptographic algorithm are already available to the attacker. This is known as Kerchoffs' principle — "only secrecy of the key provides security", or, reformulated as Shannon's maxim, "the enemy knows the system". The history of cryptography provides evidence that it can be difficult to keep the details of a widely used algorithm secret (see security through obscurity). A key is often easier to protect (it's typically a small piece of information) than an encryption algorithm, and easier to change if compromised. Thus, the security of an encryption
system in most cases relies on some key being kept secret.

**Encryption through Keyword**

In designing security systems, it is wise to assume that the details of the cryptographic algorithm are already available to the attacker. This is known as Kerchoffs' principle — "only secrecy of the key provides security", or, reformulated as Shannon's maxim, "the enemy knows the system". The history of cryptography provides evidence that it can be difficult to keep the details of a widely used algorithm secret (see security through obscurity). A key is often easier to protect (it's typically a small piece of information) than an encryption algorithm, and easier to change if compromised. Thus, the security of an encryption system in most cases relies on some key being kept secret.

**Client Side Encryption**

Client-side encryption is the cryptographic technique of encrypting data before it is transmitted to a server in a computer network. Usually, encryption is performed with a key that is not known to the server. Consequently, the service provider is unable to decrypt the hosted data. In order to access the data, it must always be decrypted by the client. Client-side encryption allows for the creation of zero-knowledge applications whose providers cannot access the data its users have stored, thus offering a high level of privacy.

**Stronger Cloud-based Storage**

Client-side encryption clearly enhances users' ability to protect data and files. By denying viewing access to servers and service providers, client-side encryption ensures that the data and files that are stored in the cloud remain private, eliminating the possibility that sensitive information or photos can be accessed, stolen or leaked. For example, client-side encryption could have made a significant difference in the Sony leak, preventing the theft of unreleased films and the avalanche of negative publicity generated by Sony executives. Likewise, client-side encryption could have protected the individuals who were caught up in the celebrity iCloud scandal, ensuring that their private photos remained private.

**EXPERIMENTAL RESULTS**

**Phase 1 Encryption**

<table>
<thead>
<tr>
<th>Plain text character</th>
<th>Key</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>b</td>
<td>4</td>
<td>y</td>
</tr>
<tr>
<td>a</td>
<td>4</td>
<td>x</td>
</tr>
<tr>
<td>n</td>
<td>4</td>
<td>k</td>
</tr>
<tr>
<td>k</td>
<td>4</td>
<td>h</td>
</tr>
<tr>
<td>i</td>
<td>4</td>
<td>f</td>
</tr>
<tr>
<td>g</td>
<td>4</td>
<td>d</td>
</tr>
<tr>
<td>d</td>
<td>4</td>
<td>a</td>
</tr>
<tr>
<td>l</td>
<td>4</td>
<td>q</td>
</tr>
<tr>
<td>s</td>
<td>4</td>
<td>p</td>
</tr>
</tbody>
</table>
Phase 2 Encryption (with secret password)

<table>
<thead>
<tr>
<th>Phase 1 Result as Input</th>
<th>Secret Password</th>
<th>Result from 2nd Phase Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>ykhfdawqiyjdpblpollyjwqflihtxq</td>
<td>confidential</td>
<td>almmnlqxyoxqjdfjorwinkljwpxqjeclvsv</td>
</tr>
</tbody>
</table>

Output Content

File Encryption

Encrypt File

Client Side Encryption
CONCLUSION AND FUTURE WORK

Although encryption is not a new innovation, it is a new IT trend. Cloud already have basic protection in place are considering implementing encryption solutions. Securely encrypted data is completely protecte.

Just as data security is ensured on all devices, encrypting data also provides security benefits during transmission. Users sending files via email or distributing them via a cloud server can use encryption to ensure that no unauthorised user can view them.

Targeted data theft is one thing, but another way to misuse data is through manipulation. Even though a hacker may have absolutely no interest in the information in question, he or she can manipulate specific data to disrupt corporate communications. If encrypted data is used, the recipient will definitely notice that it has been tampered with.

LIMITATIONS

Disk level encryption is time and space consuming. So disk level limitation is size. Encryption algorithm is fix, so if strength of securities key is not high then hacker can break it.

FUTURE ENHANCEMENT

Now a day's everyone is using web services for all of his need. And user wants to upload his information on online storage because of securities and availability issue. So disk level encryption must be efficient regarding time and space. If user have option to select encryption algorithm then it’s not easy to hacker analysis pattern.

REFERENCES


