ROHINI COLLEGE OF ENGINEERING AND TECHNOLOGY

Kanyakumari Main Road, near Anjugramam, Palkulam, Anjugramam, Tamil Nadu 629401

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

ADD ON COURSE

EMAIL AND CLOUD SECURITY

COURSE MATERIAL

E-MAIL AND CLOUD SECURITY

1 Web-Security

1 Introduction to Web-Security

Internet has facilitated most of our operations and services through web sites. Majority of the on-line users spend their time in referring to the web sites for their official work, personal work like, entertainment, online purchases and online transactions and for many more activities. Websites are also vulnerable to cyber-attacks. Cybercrimes happen every day, and stringent security measures must be taken against attacks. Cyber-attacks can be executed on web sites, web servers and web applications. Unavailability of web sites due to denial of service attacks, displaying modified information on their homepages are some of the common attacks on web sites. In other high-profile cases, millions of passwords, email addresses, and credit card details are leaked to the public domain, exposing website users to both personal embarrassment and financial risks.

2 Why Web Security?

The purpose of web-security is to prevent the web sites, web servers and web applications from cyber-attacks in the form of detecting, preventing and responding to cyber-attacks. When the user runs an application, he accesses the sites by entering the login and password which is private and protected. The confidential information exchanged through internet can compromise individual data. Hence, web security plays major role in preventing users against vulnerabilities.

Website security can be defined as the act or practice of protecting websites from unauthorized access, use, modification, destruction, or disruption. Web site visitors may also become victims to the threats. The exploitation of visitor’s browser through concealed installation of code is an example of a common web site attack. The owners areignorant about the unusual actions taking place on their sites putting the visitors at risk. Visitors are subject to attack that includes installation of offensive codes into their computers.

An Enterprise network acts as the backbone of the organization connecting various departments and devices for data transfer and exchange. Indeed, an enterprise network face a high risk of vulnerability, due to the act of compromise between the network, the server and the website. Not only that, enterprise networks are operated through websites that mostly handles customer’s account details, social security numbers and other credential such as credit card details which are highly sensitive. Any security compromise will definitely lead to damage of reputation and financial loss to the organizations. The website security issues occur in numerous ways. Some of the significant ones are:

- Website source code
- Website visitor access
- Website security attacks are becoming more sophisticated

1 Website Source Code

When the website code is not developed properly based on the guidelines and standards, then there arises bugs and security flaws. If the website is more dynamic, then the possibilities of bugs and security loopholes are more.

2 Website Visitor Access

Some websites create room for chatting to promote visitor friendliness. They are highly vulnerable to attacks. It becomes very difficult to differentiate a genuine user from an illegitimate user at situations when corporate resources are accessed by large number of visitors.

3 Website Security Attacks are becoming more sophisticated

There are many new methods found by hackers more often to attack websites.

Even malwares are designed and developed to identify vulnerable websites. Some of the ways of handling these issues are:

- Website security software
- Malware does not differentiate

- **Website Security Software -** Website Security Software prevents the websites against cyber-attacks. Security-as-a-Service (SaaS) is the model used to implement security and manage them.
- **Malware does not differentiate -** Malware is not biased. It does not differentiate between websites. The website is ensured of handling malware attacks.

3 Top Web Security Risks

Some of the are:

□ SQL Injection

□ Password Breach

□ Data Breach

□ Remote File Inclusion

□ Code Injection

□ Cross Site Scripting (XSS)

□ Broken Authentication and Session Management

□ Insecure Direct Object References

□ Cross Site Request Forgery (CSRF)

□ Security Misconfigurations

□ Insecure Cryptographic Storage

□ Failure to Restrict URL Access

□ Insufficient Transport Layer Protection and

□ Invalidated Redirects and Page Forwards

1 SQL Injection

Injection flaws particularly involve SQL injection. Based on open web security project report Injection flaws occur during the interpretation of a command or query and the data becomes untrusted. This type of flaws includes SQL, OS, and LDAP injection. When the hacker injects any of these types, then there occurs an execution of unintended commands or unauthorized data access. As a result of successful injection, the hacker gains access to change, corrupt or delete user data by denial of access or a complete host takeover. An example for SQL Injection attack is displayed in figure

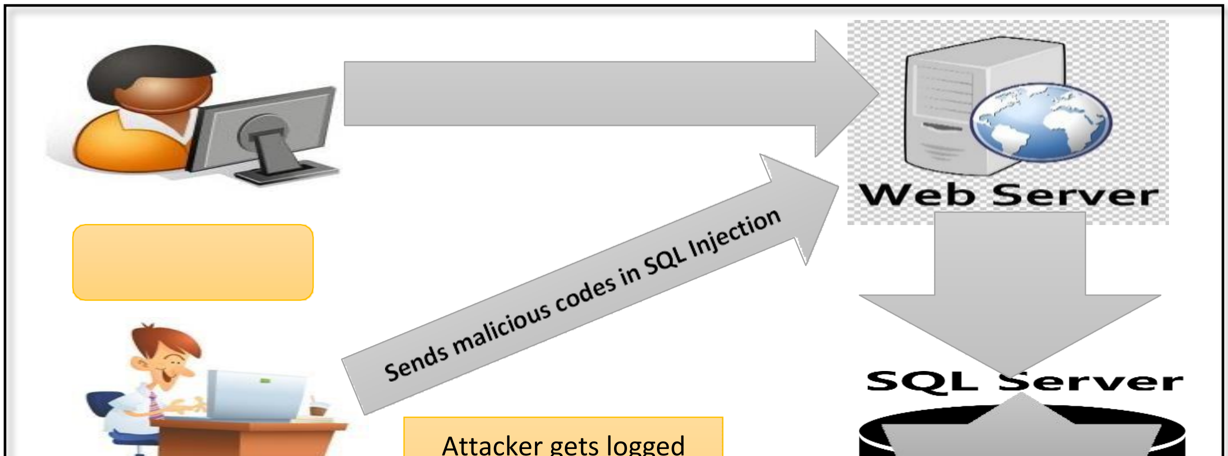
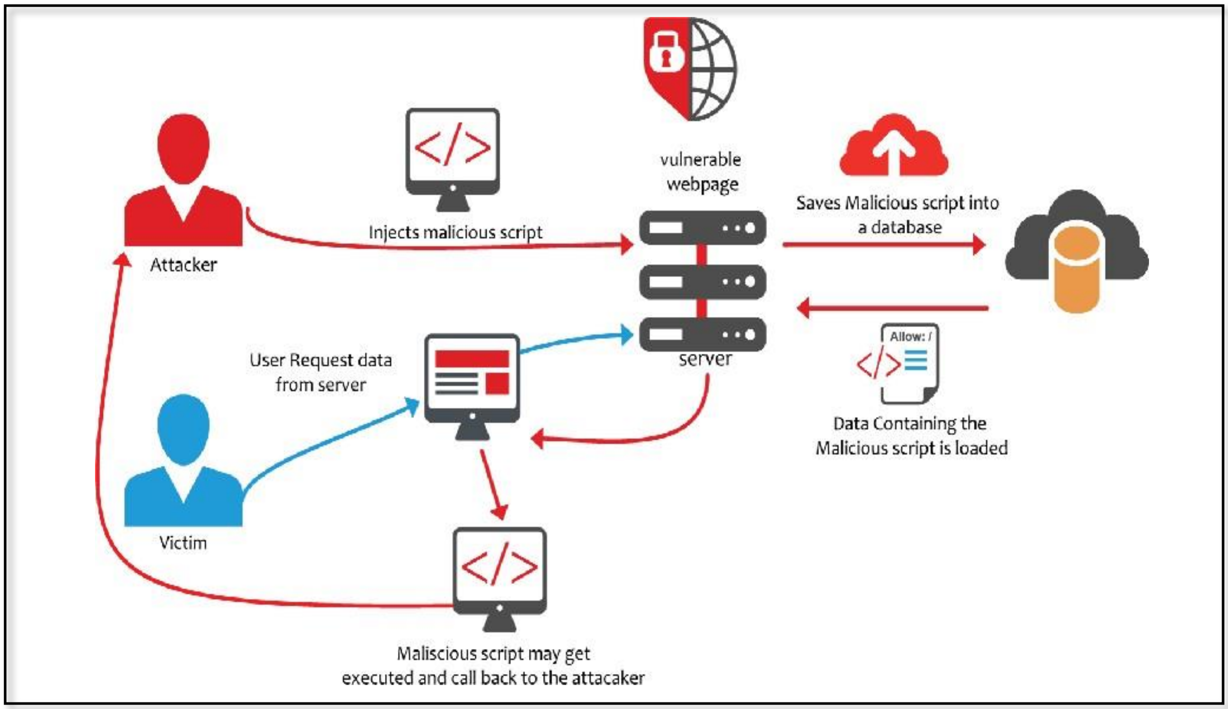


Figure 1 An Example for SQL Injection Attack

2 Cross Site Scripting (XSS)

Cross Site Scripting is shortly indicated as XSS. XSS vulnerabilities target the embedded scripts of the client execution page which is the web browser. These flaws occur due to improper validation of data entered in an untrusted web browser application. This attack enables the attackers to run the scripts only on the victim's browser. Attackers victim the web browsers by executing malicious scripts that cause session cookie hijacking, website defacing or sometimes the user is redirected to an inappropriate website. An example for XSS attack is displayed in figure



Attacker
Injects malicious script
vulnerable webpage
Saves Malicious script into a database
server
User Request data from server
Allow: /
Data Containing the Malicious script is loaded
Victim
Maliscious script may get executed and call back to the attacaker

An Example for XSS attack

3 Broken Authentication and Session Management

For each valid session during website access, there is a creation of session cookie and session that contains sensitive data like username and password. These cookies are destructed once the session ends or when the user abruptly leaves the browser or when the user signs out. Strong authentication and session management are important in these cases. For example, when a Cybercafé is used for important applications, instead of proper log out, if the user closes the session abruptly, the cookies become invalidated. A potential attacker could browse the previous session of the victim and can get access to sensitive information like profile information or credit card details. A proper implementation of keys, session tokens, cookies are necessary to prevent compromise of this type. An illustration of Broken authentication and session management is displayed in figure

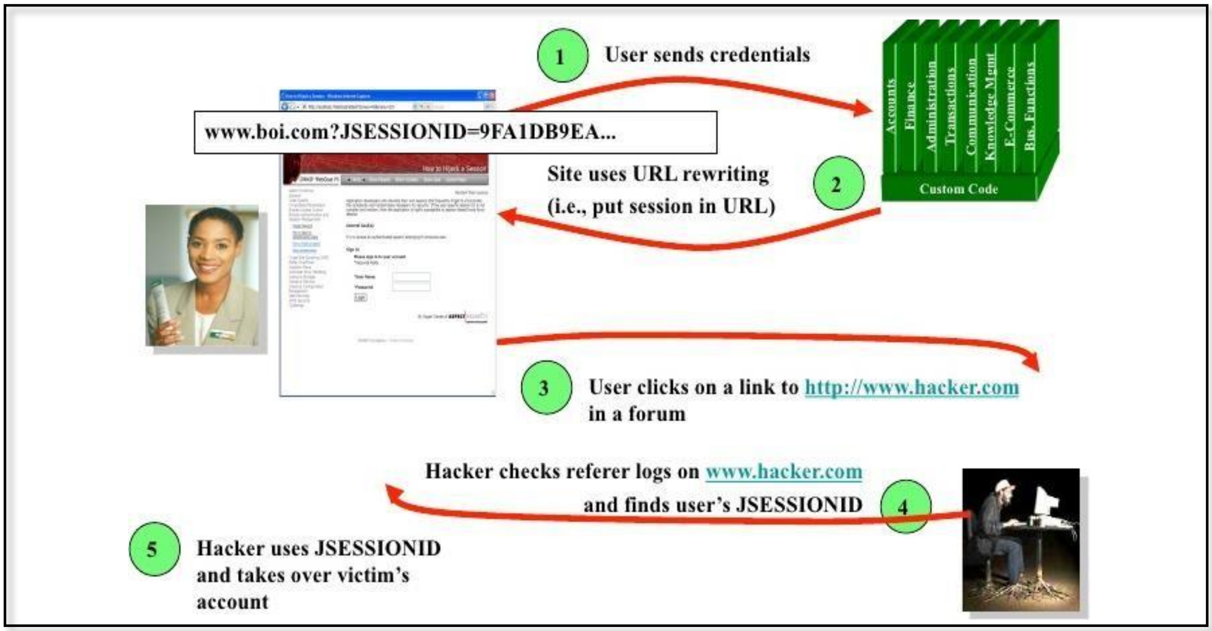


Illustration of Broken Authentication and Session Management

4 Insecure Direct Object References

When a developer uncovers a reference to an internal implementation of object then there happens a creation of direct object reference. The implementation objects may include files, directories or sometimes database keys. The hackers identify and make changes to these object references due to improper access control checks. As a result, the hackers gain access to the restricted data. Figure 4 shows an example of Insecure direct object references.

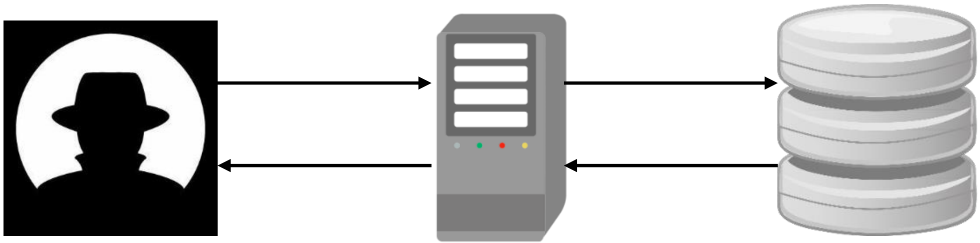


Figure 4 An example for Insecure Direct Object References

5 Cross Site Request Forgery (CSRF)

A CSRF refers to the process of forging a HTTP request when a victim signs in a vulnerable application. The forging may also occur on session cookies and on another automated authentication information. This encourages the attacker to send a fake link to the victim that forces the user to enter malicious website URL resulting in the theft of user's private data. An example for Cross Site Request Forgery is displayed in figure

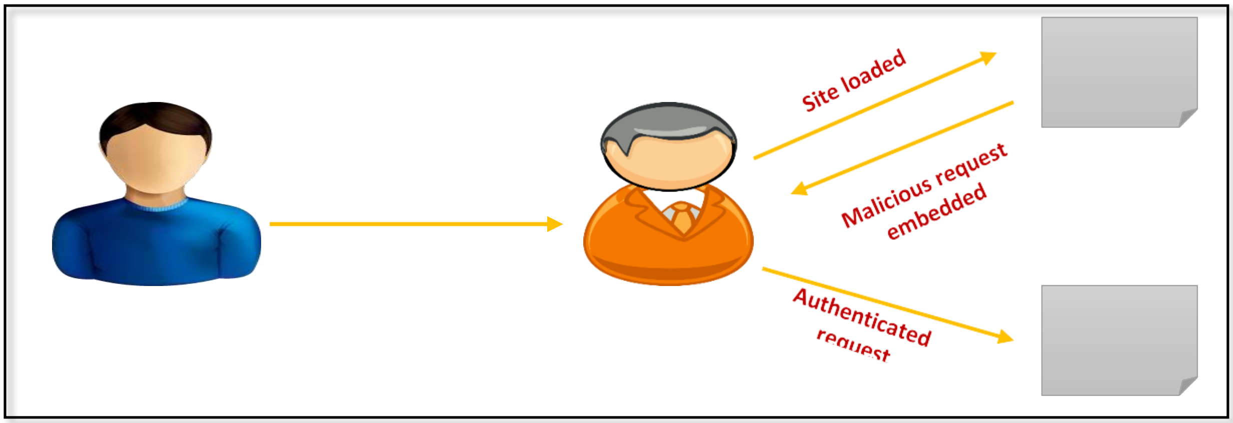


Figure 5 An example scenario of Cross Site Request Forgery Attack

6 Security Misconfigurations

All the components of a web like web applications, frameworks, application server, web server, database server, and platform require to be defined and deployed with security configuration. An attacker can fail in his attempt to access the authorized sensitive data or functionality if they are configured properly. It is necessary to maintain good security mechanism by regular update of the software. Otherwise, it results in complete system compromise. An example for security misconfiguration in a webserver is displayed in figure

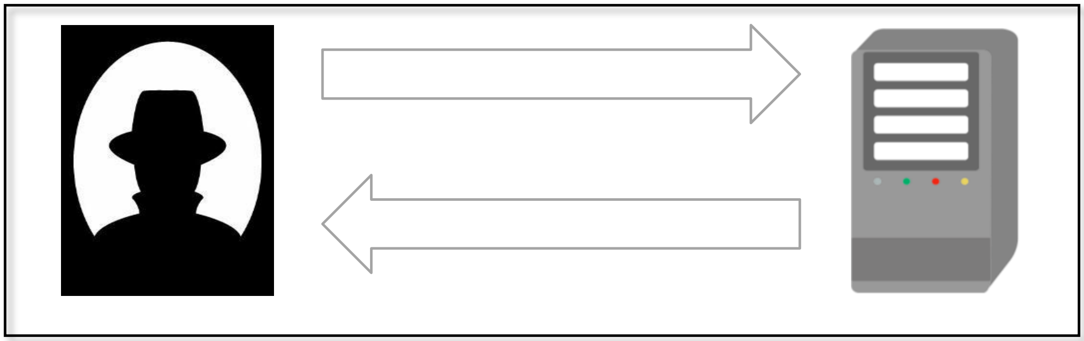


Figure An example of Security Misconfiguration

7 Insecure Cryptographic Storage

This is a common vulnerability that exists due to the insecure storage of the sensitive data. The user credentials such as personal profile, their health details, card processing information, are some forms of sensitive data. They are stored in the application database. When this data is stored without encryption or hashing, it becomes vulnerable to attacks. Hashing method is used to transform character strings to shorter strings of fixed length or a key. Hence, to decode the string, cryptographic algorithm and the secret key used for encryption must be known. An example for Insecure cryptographic storage of credit card details is displayed in figure

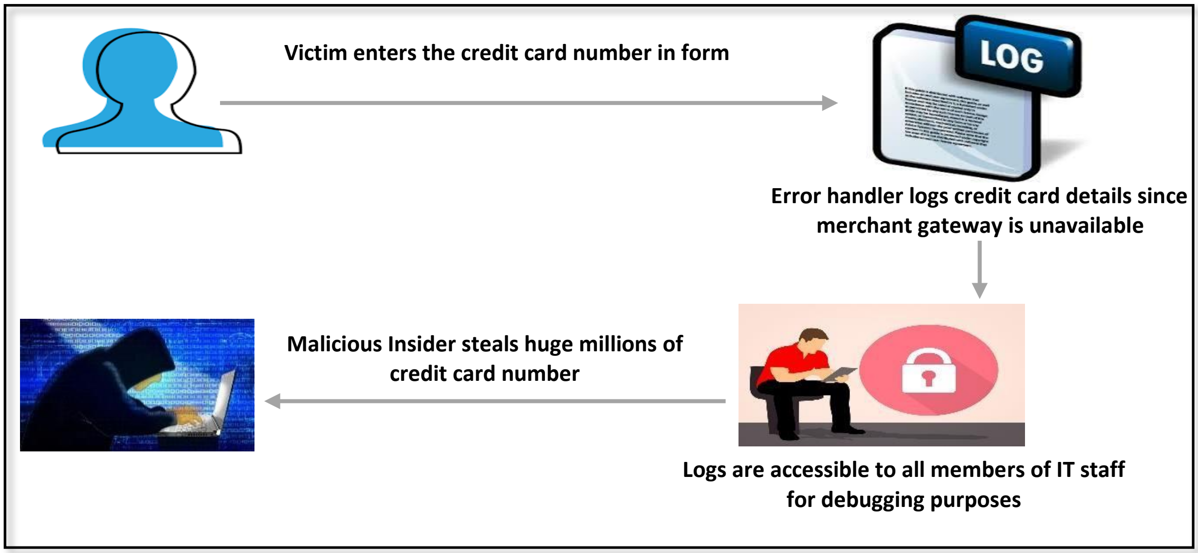

Victim enters the credit card number in form
LOG
Error handler logs credit card details since merchant gateway is unavailable
Malicious Insider steals huge millions of credit card number
Logs are accessible to all members of IT staff for debugging purposes

Figure An example for Insecure cryptographic storage

8 Failure to Restrict URL Access

Web applications often check the URL access rights before rendering protected links and buttons. Similarly, applications need to check for access controls whenever web pages are accessed. In most of the applications, the special rights to pages, locations and resources are not made available to the users. An attacker by intelligent guess, access these privileged pages by invoking functions to view confidential information.

9 Insufficient Transport Layer Protection

The sensitive information such as credit card credential, user authentication details, session tokens are transmitted over various network layers. These details are exposed to untrusted users due to the absence of Secure Socket Layer (SSL). This takes place due to the usage of weak algorithms, expired certificates or invalid certificates. This paves way to steal sensitive information or perform unwanted actions.

10 Un validated Redirects and Page Forwards

Sometimes, the users are redirected or forwarded to inappropriate pages for intended purpose by some web applications. If there is improper validations in redirecting or forwarding to other pages, attackers make use of this opportunity to attack victims by phishing or malware attacks to access unauthorized pages. Figure 8 shows an example scenario of unvalidated redirects and page forwards.

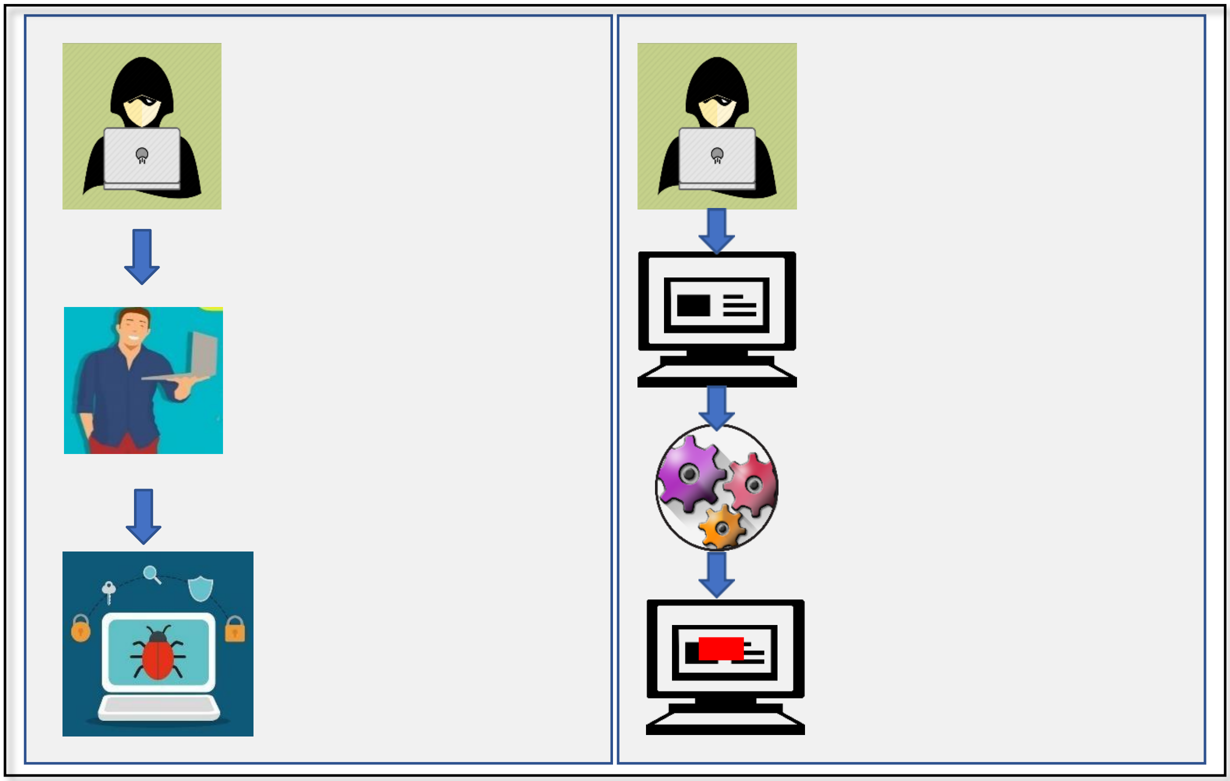


Figure 8An example scenario of unvalidated redirects and page forwards

6.1.4 How to handle these risks?

The security issues are sometimes handled through Better performance. The website contents are stored in multiple servers that can be accessed globally with the help of the Content Delivery Network (CDN). Some of the ways used in handling the risks are:

- By consistent scanning, Instant malware removal
- By advanced security monitoring.

    - Absolute malware protection

- **By Consistent scanning, Instant Malware removal –** At regular basis and in-depth website scanning are some important operations that assure security at server level.
- **By Advanced security monitoring –** The customer's or visitor's private information are kept confidential and prevented from redirecting onto malicious websites that are highly infective to the system. For this purpose, website security relies on Domain Name System (DNS), Secure Socket Layer (SSL) and WHOIS database.
- **Absolute Malware prevention –** Must be used to block a malware before it tries to affect the website.

Figure 9 shows the different ways of handling the risks.

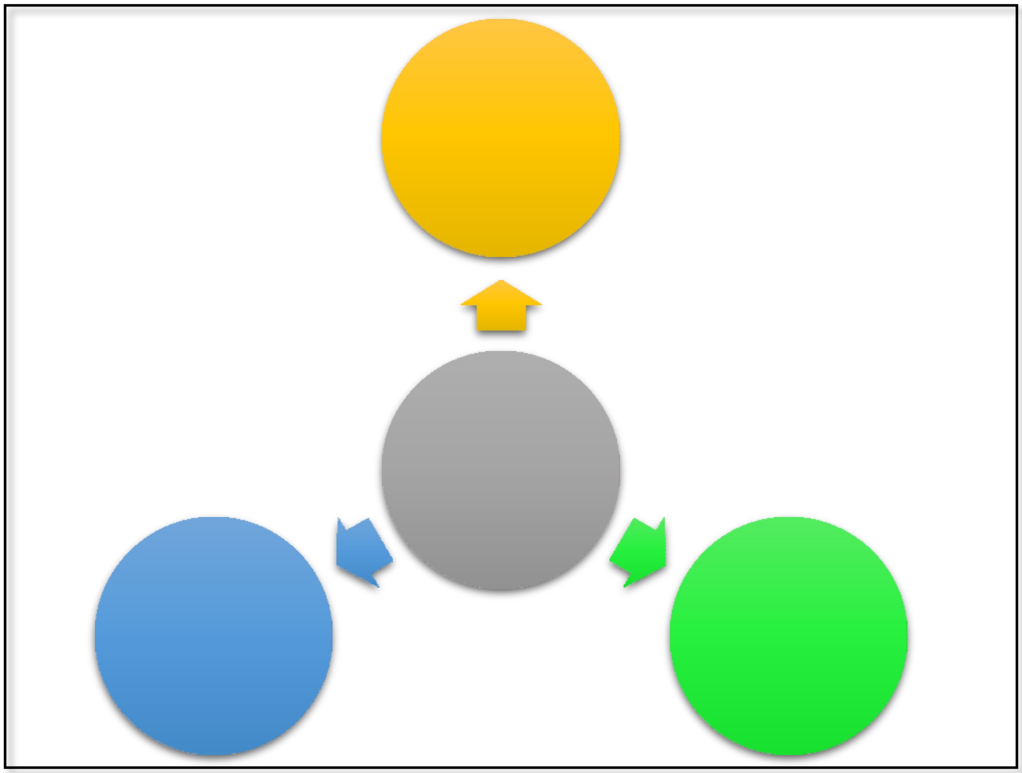


Figure 9 Different ways of handling risks

1 Open Web Security Project (OWASP)

Open Web Security Project (OWASP) mainly concentrates to improve the security of web applications and software. This is a non-profit charitable organization. The organization has prescribed many security standards. Hacking different web sites or services are closely monitored by maintaining web hacking incident databases. Different types of check points and techniques are applied to back web security. Depending on the data, every organization maintains a list of frequent web security vulnerabilities published.

They are prioritized based upon factors such as exploitability, detectability and impact on software.

- **Exploitability** – It defines the action performed to cause the security vulnerability. Highest exploitability occurs when the attack takes place over web browser. However, lowest exploitability occurs when the system is being protected by advanced programming and tools.
- **Detectability** – It defines the process of detecting the threat. Highest detectability can be done when the information is displayed as URL, Form or Error message and lowest rank of detection will be on the native code.
- **Impact or Damage** – It implies the consequences of vulnerability when security is exposed to attack. Highest damage will be complete system crash and lowest impact can be nothing at some cases.

6.1.5 Preventing Web-Security Risks

To prevent the above security risks, there exists two primary methods used namely automated scanning or detection tools and Security Audit. For example, complete code review is absolutely necessary to handle XSS vulnerability. Some XSS attacks can be caught using detection tools, whereas automated detection in combination with manual review of coding and penetration testing are used to prevent them to a full extent. An insecure direct object reference can be detected using automated tools. Website security vulnerability, scanning or exploit scanning service helps users in preventing them. Importantly, with the help of these tools and techniques a typical hacker can hack the user website in a systematic way.

As a result, automated detection tools and systematic reviewing of site can identify eight out of ten major vulnerability types. However, cross-site request forgery is an exception to this. It cannot be detected using these approaches. The identified vulnerabilities are documented in user website security risk report that helps the IT support team to enhance security.

Some of the ways to prevent web-security risks are:

- Performing website security audit
- Popular technology solutions available
- Web security defense strategy

1 Performing Website Security Audit

Regular scanning of currently running application on the domain and examining the website code are the best defense against the attack on websites. Web scanning or auditing is the other form of web site testing. It is provided by Web Site Security Audit for service host (WSSA). This functions without any software or hardware installation and web service interruption. The user can identify whether the server is vulnerable to attack or not by means of examining them for the open port, existing service or code, as exploits have a known fusion of web site weakness.

WSSA is capable of executing the entire database containing numerous vulnerabilities within a fraction of second and report the type of threat found. With this data, the user and the administrator can address the actual web security vulnerabilities. WSSA must run on regular basis to test the website for new vulnerabilities with solid database and determine whether the action is vitally needed or if it is of low priority. User is alerted when,

i. Unwanted addition of new code to the site,

ii. Opening of port,

iii. When a new service is loaded to the system without user's permission.

In complex and large systems, web scanning is done on daily basis to ensure that no changes are made to site code and the applications run within the established security
perimeter.

6.1.5.2 Popular Technical Solutions available

Web security is maintained with standards offered by different technologies done through testing, building and preventing threats. They are:

- Black box testing tools
- White box testing tools
- Web Application Firewalls (WAF)
- Security Scanners or Vulnerability Scanners
- Password cracking tools
- Fuzzing tools

The level of security depends on the level of exploitation by the threats as well as on the basis of equipping and testing the protection tools.

3 Web Security Defense Strategy

A developer can protect the website or applications developed using two primary defense strategies namely,

- Resource Assignment
- Web Scanning

- **Resource assignment** – To constantly alert users for new security issues, it is necessary to assign all the resources needed to defend against the vulnerabilities. This ensures that the security patches are kept up to date and reviews the protection of existing applications. The assignment of resources includes strong firewall protection, antivirus software and employing intrusion detection/prevention systems.
- **Web scanning** – It refers to the process of scanning or testing user's current equipment, applications and web site code for existence of known vulnerabilities. A simple logic of front door locking is applied apart from using firewalls, antivirus software and Intrusion Prevention System/ Intrusion Detection System (IPS/IDS). The most efficient form of detecting vulnerabilities is the usage of network and web site scanning methods. Since, unknown threats are complex to identify. The above

solutions can be used for detecting only known threats.

6 Important Features of a good Website Security Solution/Approach

Following are some of the features of a good website security,

- Malware Scan
- Malware Removal
- Manual malware and Hack removal
- File Change Monitoring
- Blacklist/Spam monitoring
- Blacklist Removal

- Security Monitoring
- Advanced DDoS Mitigation
- Web Application Firewall (WAF)
- Content Delivery Network (CDN)
- Site Seal

Another two solutions that help in managing a good website security are:

- Web server security
- Website code and web security

Web Server Security

A web server that is turned off is more secure than the one that is on. Because it simply restricts the number of open ports and services. A system can become vulnerable to attacks if it has multiple open ports, services or scripting languages resulting in security loop holes. If the computer systems are configured properly and security patches are updated continuously then the occurrence of risks can be eliminated or totally minimised. Web Applications must also need frequent updations.

Web Site Code and Web Security

The communication that takes place between the websites and the visitors, promotes lot of interactions and there occurs chances of potential web security vulnerabilities. Web sites often force visitors to the following situations:

- Loading into a new page that contains effective content
- Product or location searching
- Filling out a contact form using private details
- Searching inappropriate site contents
- Using an irrelevant shopping cart
- New account creation
- Existing account login

In each of the above cases, the visitors use some commands to access the web server or database. The form field, search field or the blogs are the places where interactions take place. The amount of commands or information types that pass in and out depends on the correctness of the program code. A properly coded program allows desired amount of commands or information to pass in and out. But sometimes the limits are not automatic. Only trained programmers can create codes to allow expected data to pass on and block inappropriate data to enter into the system.

Website codes are created by programmers, that may work for third party vendors. When the website runs the software from different sources and the codes may be continuously modified by site designer. Webmaster creates new codes or modify existing codes that sometimes overlooks previous web security limitations.

Most of the servers gather unused applications along with unfamiliar staff details. The codes may also be old and often it is difficult to find whether they are unused, patched or updated for years. But it becomes the tool for hackers to exploit web servers.

7 Known web security vulnerabilities and unknown vulnerabilities

_Web security vulnerabilities are further classified into two namely, known and unknown.

Which is the greatest web security risks: known or unknown?

Websites are mostly attacked with known exploit rather than by unknown exploits. With known exploits, the web servers and sites become highly complex. Chances of unknown exploits are generally smaller unless the network assets are of great value. The best approach is to eliminate the known vulnerabilities and look for unknown vulnerabilities. ______

2 E-mail Security

1 Introduction to E-mail System

E-mail is the popular form of sending or exchanging information between two or more parties. But today, it is the popular medium through which malware, spam and phishing attacks are executed. Email also acts the entry point for the enterprise network
to gain access to their valuable data.

6.2.2 The need for e-mail security

E-mail security deals with the different techniques that keeps the information sent through email accounts secure against unauthorized access, loss, or compromise. Sometimes, data security breaches inside an enterprise network mainly take place through e-mail which serves as the primary door of attack for attackers. It is important to provide e-mail security as individuals and business organizations expand their extensive communications through e-mail.

Moreover, the ease of use and popularity it becomes the attack vector for the intruders. Unauthorized access and attempts to e-mail accounts happen for every e-mail account holder today. Malware sent via e-mails is the most common threat. Phishing e- mails sent with malware attachments compromise the account as well as the device. Sometimes, phishing e-mails trick the users for sharing sensitive information. Phishing attacks also target departments that handle sensitive information like financial data, credit card details, personal id in business organization. To increase the chance of success, a sense of urgency will be instilled by phishing emails. Phishing e-mails involve confirmation of the recipient's login information, user password, social security number, bank account numbers, and even credit card information. Other form may be, directing the users to counterfeit websites that look similar to that original vendor site victimising users to disclose their account data or financial data.

E-mail messages must be secured as they are delivered and received across untrusted networks. When security measures are not in place e-mails are exposed to hackers like how postcards can be read or modified in midways. Hence it is necessary to provide security over external networks present outside the security boundary of an organization.

Every organisation must employ e-mail administrators responsible in providing security to the e-mail system. To maintain the CIA triad of information transferred, through e-mail it is necessary that every user must have enough knowledge about threat exploits and basic security measures to be adopted. Continuous security monitoring is essential to maintain the effectiveness of the e-mail security system and IT infrastructure security. Mail clients and mail servers are the two primary components of an e-mail system residing in an organization's IT infrastructure. Mail clients enable users to read the messages, compose a new mail and send to other recipients, and also store them as drafts or in drives. Mail is composed and sent from the mail client to the mail server through a network. The mail server is the computer that delivers, forwards, and stores e-mail messages. These components must be protected with e-mail security features.

The standards used for formatting, processing, transmitting, delivering, and displaying e-mail are Simple Mail Transfer Protocol (SMTP), Extended Simple Mail Transfer Protocol (ESMTP), Post Office Protocol (POP), Internet Message Access Protocol (IMAP). They help in ensuring interoperability between different mail clients and servers.

6.2.3 Common Threats to e-mail security

Since e-mail communication takes place over untrusted, external networks they are subject to primary threats like:

- Malware
- Spam and Phishing
- Social Engineering
- Entities with Malicious Intent
- Unintentional Acts by Authorized Users and
- Baiting

1 Malware

As discussed previously, malware is a serious threat to e-mail and the most common form of malware includes viruses, worms, Trojan horses, and spyware. They transfer malicious controls and access the resources present in servers or workstations unauthorizingly. They exploit the whole system by changing privileges and observe user actions. They may also indulge in malpractices maliciously.

2 Spam and Phishing

Spam refers to the process of sending unwanted commercial e-mails. These e- mails may cause damages to user's personal data present inside the computer system. They also include disruption to user productivity, excessive utilization of resources and unwanted distribution of malwares.

Phishing is similar to Spam and are generated by computers to trick the users who respond to the e-mail by entering sensitive information ignorant of the consequences. Most of the phishing attacks take place by modifying the recipient addresses with other trusted sources.

3 Social Engineering

It is a method used by the attacker to gain access to sensitive information of an individual or an organization with the help of an e-mail to perform further attacks. E-mail spoofing is an example of social engineering approach. It is the method where a true individual or program is faked as false recipient information by masquerading them.

Pretexting is another type of social engineering tactics used by the attacker to extract confidential information such as login or authentication credentials. The attacker exercise this method by faking a call to an employee forcing them to provide essential information for further proceedings. It is important that users must be conscious while sharing their login information and must prevent themselves from dangerous attacks.

4 Entities with Malicious Intent

Through a successful mail server attack on organization’s network, malicious entities gain access to resources. For example, an attacker can retrieve user password by compromising the mail server and can also grant access to another host in the organisation network.

6.2.3.5 Unintentional acts by authorized users

Security threats may be intentional or unintentional. But most of the time they are unintentional. At times authorized users transmit sensitive information over e-mail without any prior knowledge that they may be exposed to illegal actions.

6 Baiting

Baiting is an older form of social engineering. This program is created using a computer tool that lures a user to click a link or open an attachment. This link or the attachment contains malicious items designed based on different user’s interest. It is important to make the users understand that opening or clicking links will result in exploitation. Apart from this, the security system must also monitor for accidental actions by the users.

The various threats to email security are shown in figure

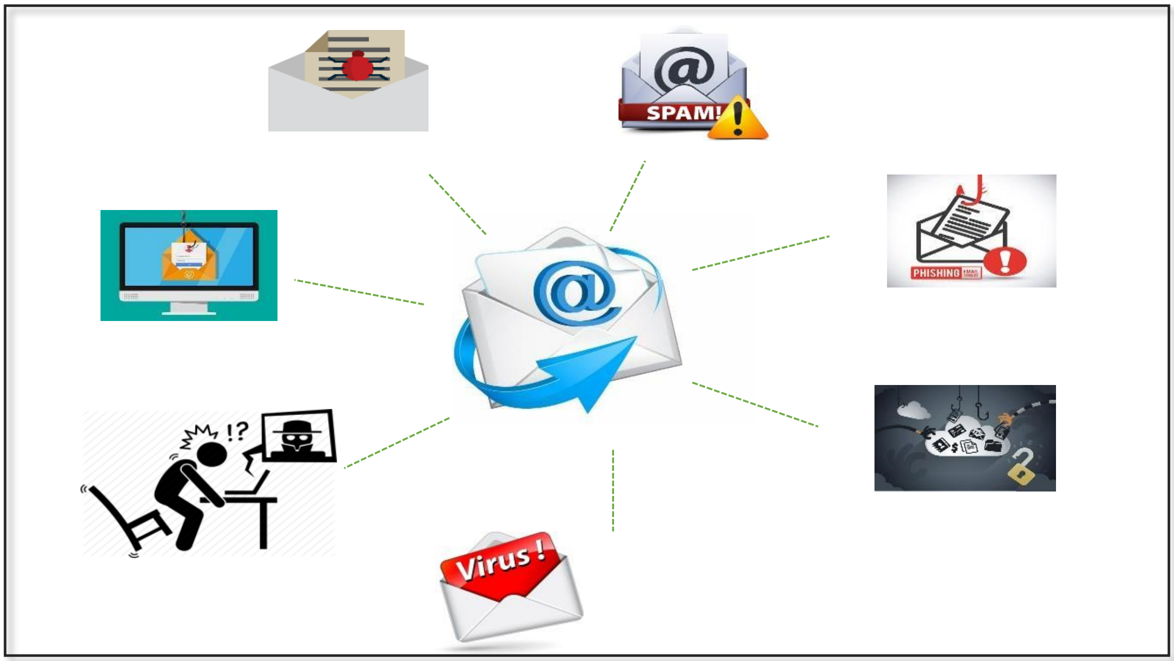


Figure 10 Various Threats to E-mail Security

4 Maintaining a Secure Mail System

Maintaining the security of e-mail system is a continuous process that requires constant effort, resources, and vigilance. Some of the actions that could be taken to maintain a secure mail system are as follows:

- Configure, protect and analyse log files
- Back up data frequently
- Protect against malware
- Perform periodic security testing

1 Configure, Protect, and Analyze Log Files

Log file contains the record of an organization’s behavior or in other words activities. With the help of these log files, the data collected is used for detecting successful and unsuccessful intrusions by observing the generated alerts for further investigation. This also helps in system recovery and post-event investigations which are the tools and procedures applied by the organizations for processing and analyzing log files.

2 Back up Data Frequently

Maintaining the integrity of data on the mail server is the most essential function of a mail server administrator. Because mail servers are the primary targets of the organization, the administrator is responsible to continuously create backups of the mail server to minimise the session events by supporting regulation compliances and archiving e-mails for protecting data and information.

There are many protection methods that can be used against malwares. Some of them include malware scanning and spam filtering. With this an organization can protect against malwares by employing them at the mail client level, server and system levels. It is also important to conduct training and awareness programs for users in the organization. Another program is the usage of telecommuters, which helps users to identify and handle inappropriate mails and attachments.

4 Perform Periodic Security Testing

Every security system installed in the organization, must be tested periodically to examine whether the security mechanisms are correctly implemented and confirm that the expected output are met as far as security requirements of the operational mail system is concerned. A combination of various methods such as vulnerability scanning, port scanning, spam filtering, malware scanning, firewall, intrusion detection system should be implemented by the organizations to assess and support the mail system and its environment.

6.2.5 E-mail Encryption Techniques

E-mail encryption refers to the technique of encrypting e-mail messages to ensure confidentiality of the email communication. There are two types of encryption types used in e-mail security. They are

i. Public Key Cryptography or Asymmetric Cryptography

ii. End-to-End Encryption

1 Public Key Cryptography

Most the e-mails are not transferred in encrypted form which helps the attacker to easily uncover them with the help of informal tools. E-mail encryption is based on the public-key cryptographic system. Two keys namely public-key and private key are used. Public key is used for encrypting the message and the private-key is used for decrypting the message. Figure 11 shows the encryption/decryption process.

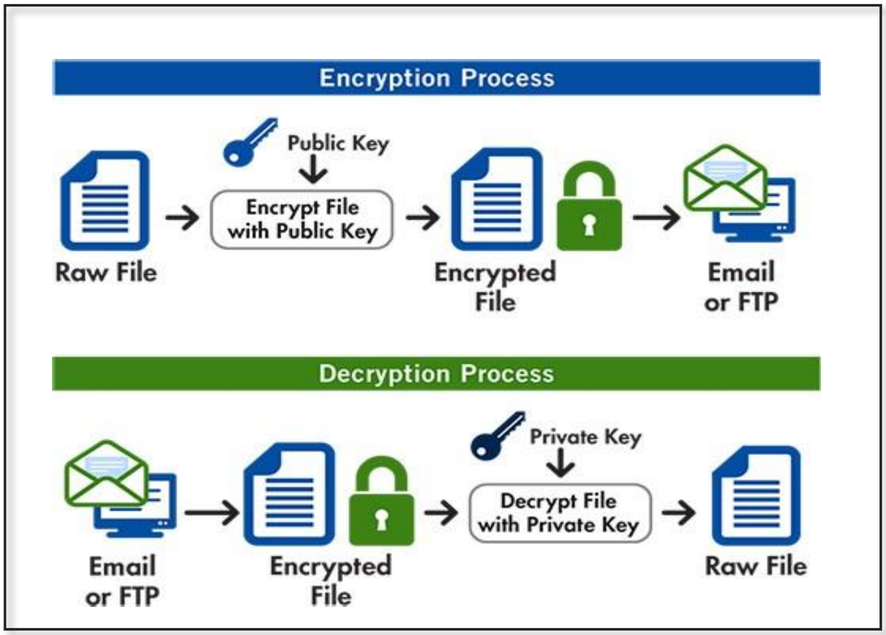


Figure 11 Encryption and Decryption Process

2 End-to-End Encryption

End-to-End encryption refers to the process where encrypting and decrypting of e- mail messages take place only at the end points. With the help of end-to-endencryption, the source and destination recipient’s messages are encrypted, and they cannot be read by e-mail service providers. These encryption takes place when the user composes and sends messages to the receiver. It reaches the receiver in the same encrypted form. The service providers like Gmail cannot decode the sent message. This encrypted e-mail can be decrypted only with the help of user’s private key. Few e-mail systems are protected with automatic end-to-end encryption techniques. Some of the protocols used in end-to- end e-mail encryption are as follows,

□ Bit Message

□ GNU Privacy Guard (GPG)

□ Pretty Good Privacy (PGP)

□ Secure/Multipurpose Internet Mail Extensions (S/MIME)

6.2.6 Open PGP Encryption

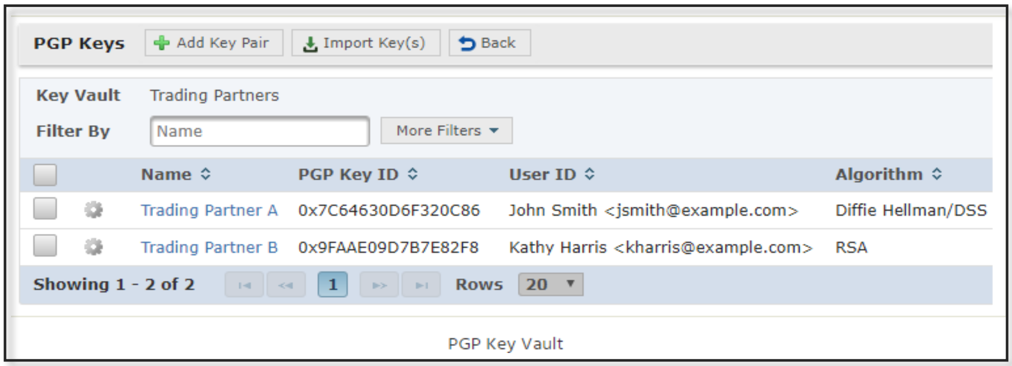
OpenPGP is an encryption standard used in end-to-end e-mail encryption. OpenPGP encryption enables to store sensitive information and to transmit the information across insecure networks like internet or e-mail, so that it cannot be read by anyone other than the intended receiver.

This method ensures only authorized recipients can read the messages without server support. Server-side system is not provided with decryption keys. This puts a limitation to end-to-end encryption affecting the usability of the messages and makes server-side searching difficult. OpenPGP also faces usability issues due to the reason that the user is responsible for setting up public and private key pair, where public keys are available open. This method protects only the contents and still the metadata prone to untrusted parties. In addition to this, the end user's activities are also monitored.

Open PGP based on public key cryptography where public and private keys are used to encrypt and decrypt messages. The message sent is encrypted using public key at the time of sending using software and e-mail-client plugins. The public key is used to encrypt the file and verify the signature. The private key is used by the owner to decrypt and to add digital signature to the file. User can create, import, and export PGP keys through the Go Anywhere Key Management System. Keys are protected and organized in Key Vaults for access controls. One can access the Key Management System through the Encryption drop-down menu. Getting the key pair through the open software is a simple process.

Following step-by-step procedure along with the screenshots explain the working of OpenPGP.

How to get started with PGP?



Key Vault: Trading Partners

Filter By: Name

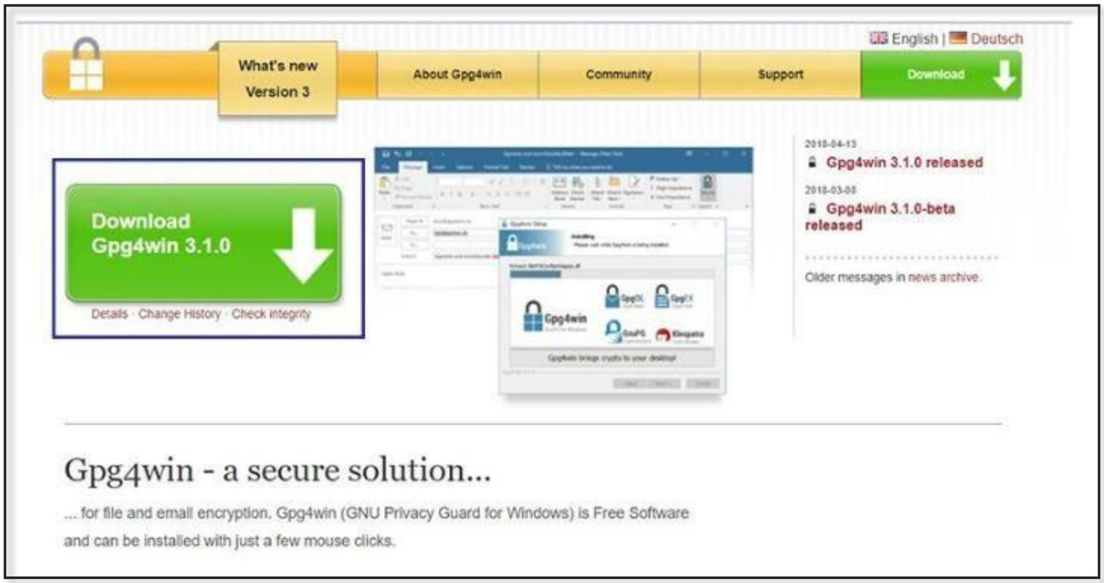
□		Name	PGP Key ID	User ID	Algorithm
□	⚙	Trading Partner A	0x7C64630D6F320C86	John Smith <jsmith@example.com>	Diffie Hellman/DSS
□	⚙	Trading Partner B	0x9FAAE09D7B7E82F8	Kathy Harris <kharris@example.com>	RSA

Showing 1 - 2 of 2 | 1 | Rows 20

Figure 12 OpenPGP Key Vault

Getting own key pair is much easier than it sounds. It just needs figuring out a few simple programs.

Step 1: Download Gpg4win. This is a free software with set of encryption packages and tools. For Mac users, checking out GPG Suite is advisable.



2018-04-13
Gpg4win 3.1.0 released

2018-03-08
Gpg4win 3.1.0-beta released

Older messages in news archive.

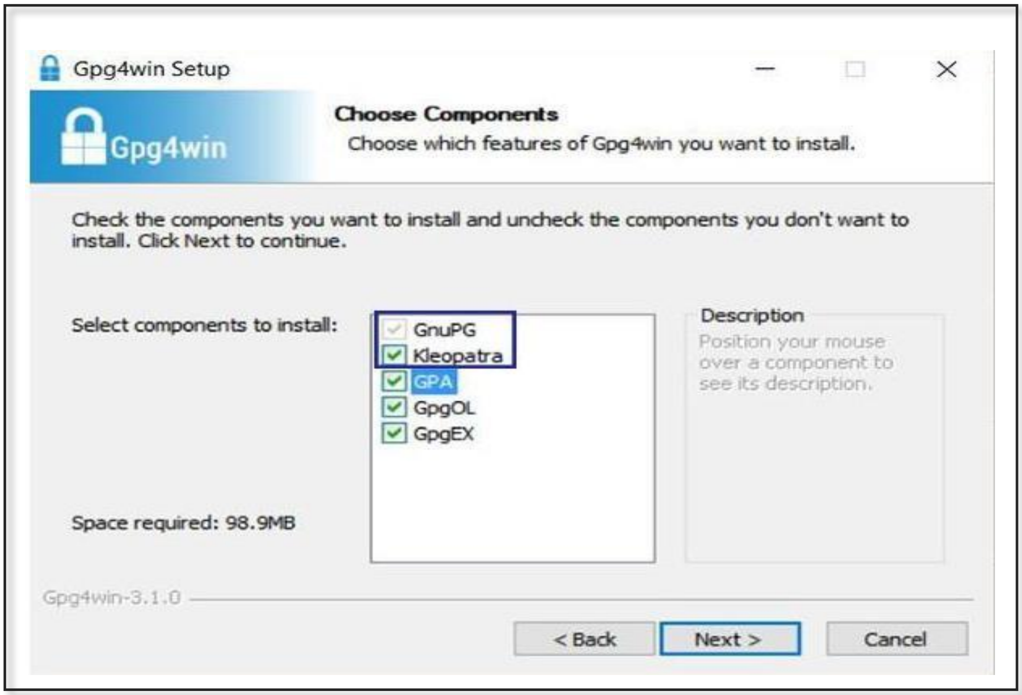
Gpg4win - a secure solution...

... for file and email encryption. Gpg4win (GNU Privacy Guard for Windows) is Free Software and can be installed with just a few mouse clicks.

Figure 13 Downloading Gpg4win

Step 2: Install Gpg4win. Make sure GnuPG-the actual encryption package and

Kleopatra-user interface are installed; the other components are optional.



Gpg4win Setup

Choose Components

Choose which features of Gpg4win you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

- ☑ GnuPG
- ☑ Kleopatra
- ☑ GPA
- ☑ GpgOL
- ☑ GpgEX

Description

Position your mouse over a component to see its description.

Space required: 98.9MB

Figure 14 Setting up Gpg4win

Step 3:

Once everything is installed, find the Kleopatra program on the computer and open it.

Step 4: Go to the "File" tab and select "New Certificate".

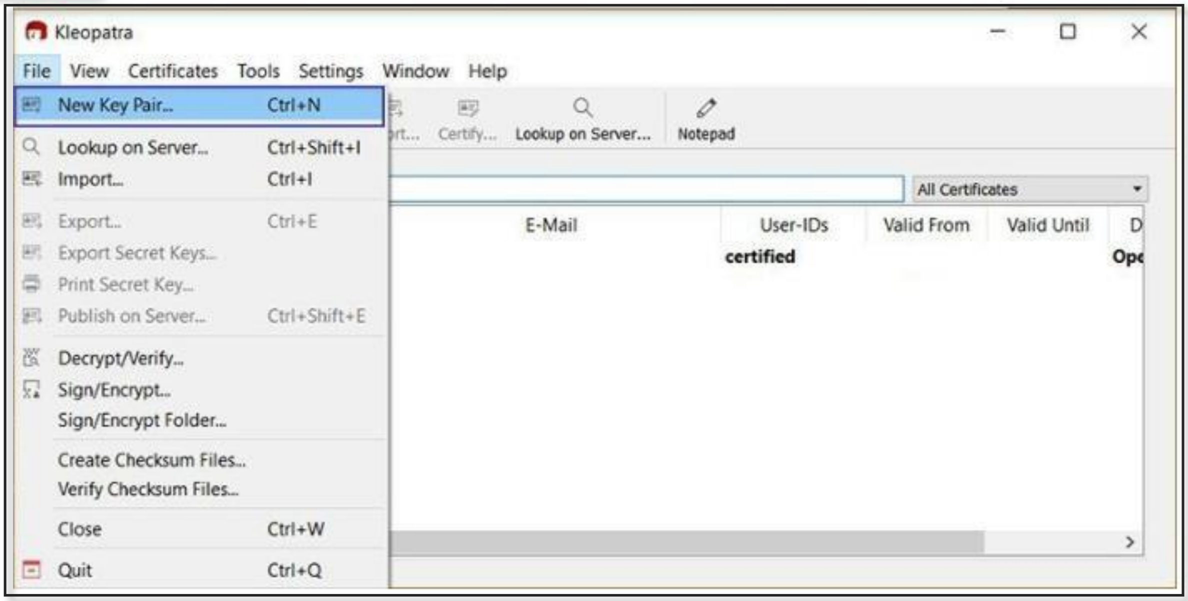
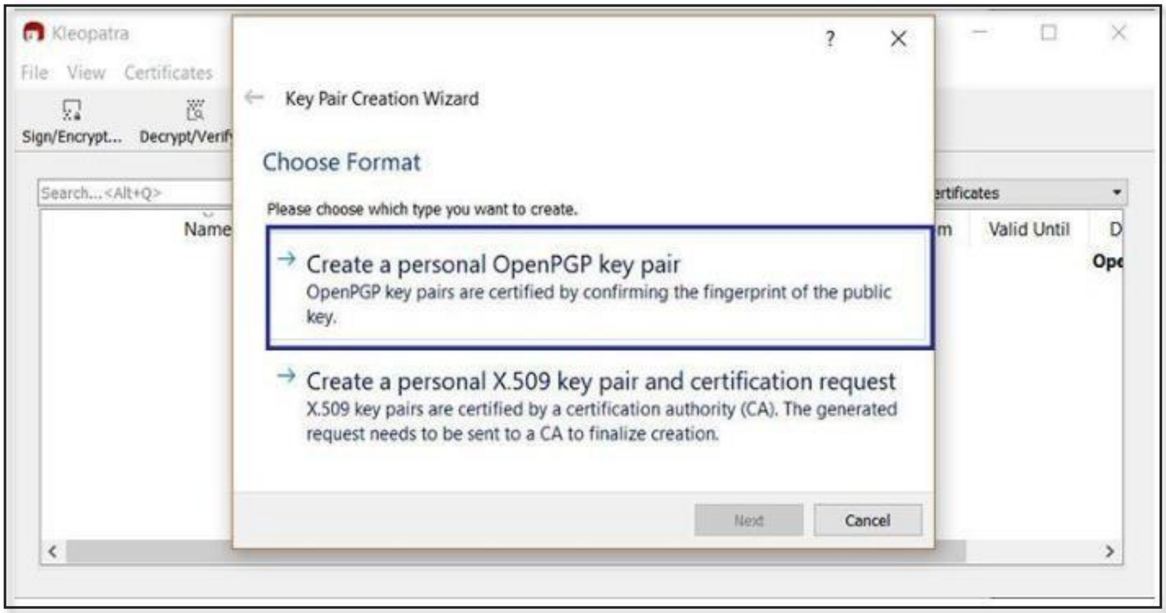


Figure 15 Creating New Key Pair Certificate

Step 5: Since user wants PGP keys, select "Create a personal OpenPGP key pair."



Key Pair Creation Wizard

Choose Format

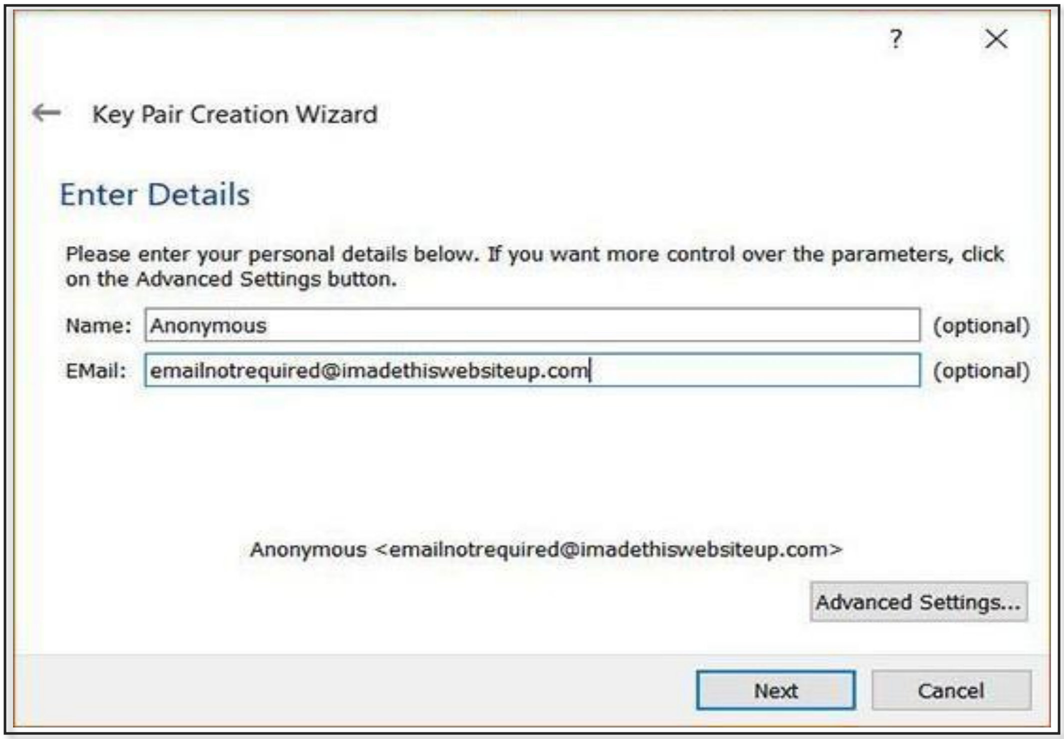
Please choose which type you want to create.

→ Create a personal OpenPGP key pair
OpenPGP key pairs are certified by confirming the fingerprint of the public key.

→ Create a personal X.509 key pair and certification request
X.509 key pairs are certified by a certification authority (CA). The generated request needs to be sent to a CA to finalize creation.

Figure 16 Creating a Personal OpenPGP key pair

Step 6: If one wants to attach the key to one's identity either real or fake, then information is entered here. Otherwise this step can be skipped.



Key Pair Creation Wizard

Enter Details

Please enter your personal details below. If you want more control over the parameters, click on the Advanced Settings button.

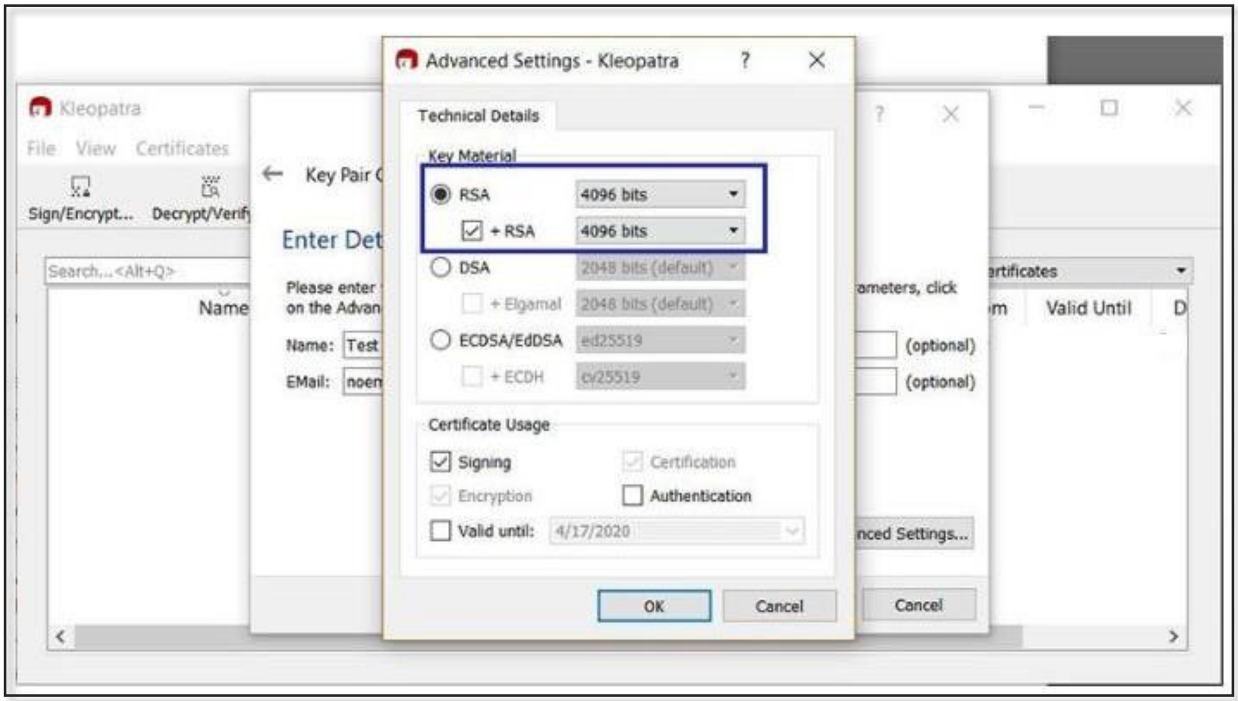
Name: Anonymous (optional)

EMail: emailnotrequired@imadethiswebsiteup.com (optional)

Anonymous <emailnotrequired@imadethiswebsiteup.com>

Figure 17 Entering details in Key Pair Creation Wizard

Step 7: Visit “Advanced Settings” and make sure “RSA” is selected. Change the default 2048 to 409 This level of encoding makes the encryption pretty much impenetrable and does not slow down during normal use.



Advanced Settings - Kleopatra

Technical Details

Key Material

● RSA 4096 bits

☑ + RSA 4096 bits

○ DSA 2048 bits (default)

□ + Elgamal 2048 bits (default)

○ ECDSA/EdDSA ed25519

□ + ECDH cv25519

Certificate Usage

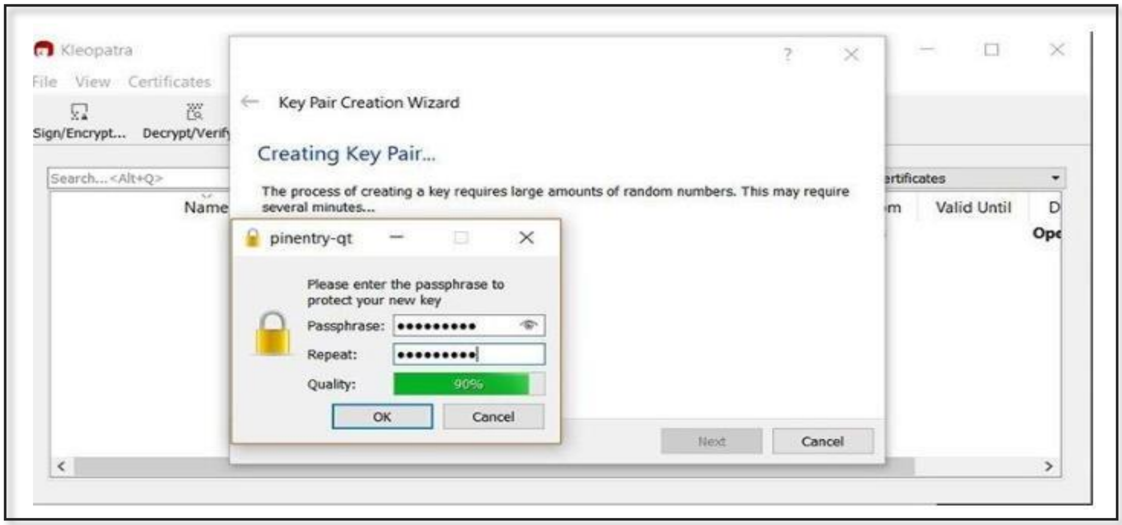
☑ Signing ☑ Certification

☑ Encryption □ Authentication

□ Valid until: 4/17/2020

Figure 18 Advanced Settings in Kleopatra

Step 8: Click “Okay” to exit this settings menu, and then click “Next” to start creating the key. The program is now generating thousands of random characters to make user keys and will ask for a passphrase. The passphrase is unrecoverable, so it should not be forgotten.



Key Pair Creation Wizard

Creating Key Pair...

The process of creating a key requires large amounts of random numbers. This may require several minutes...

pinentry-qt

Please enter the passphrase to protect your new key

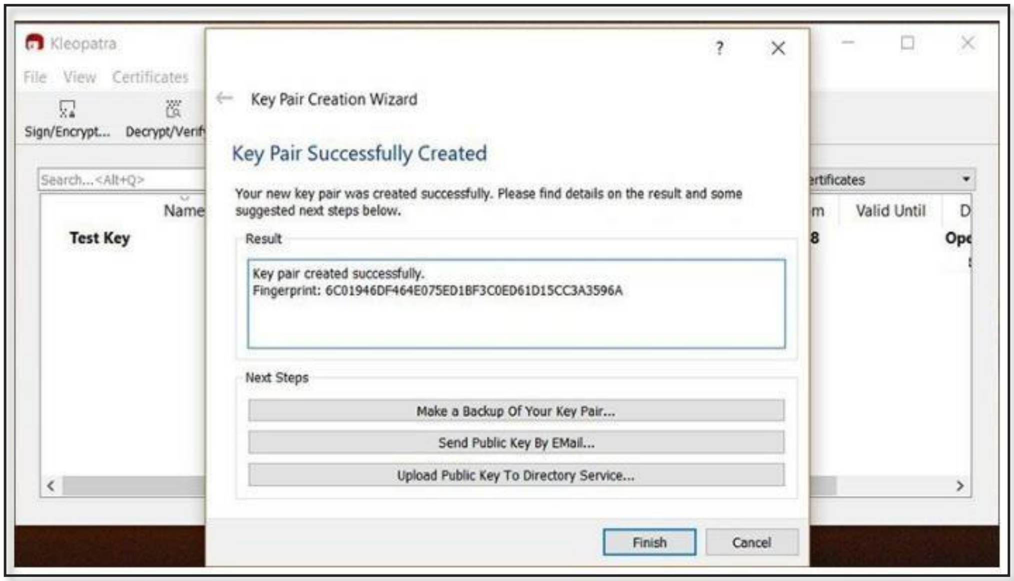
Passphrase: •••••••••

Repeat: •••••••••

Quality: 90%

Figure 19 Setting up Passphrase for new key

Step 9: User now has a public and private key. If user wishes, then he can store the key in a separate file somewhere. Through email or any other form, the public key can be uploaded.



Key Pair Creation Wizard

Key Pair Successfully Created

Your new key pair was created successfully. Please find details on the result and some suggested next steps below.

Result

Key pair created successfully.
Fingerprint: 6C01946DF464E075ED1BF3C0ED61D15CC3A3596A

Figure 20 Successful creation of Key pairs

Step 10: User can generate a file with public key in it by right-clicking the file and clicking "Export." There are several ways to view it, but it is easy to access public key whenever the user wants, without the need to use Kleopatra.

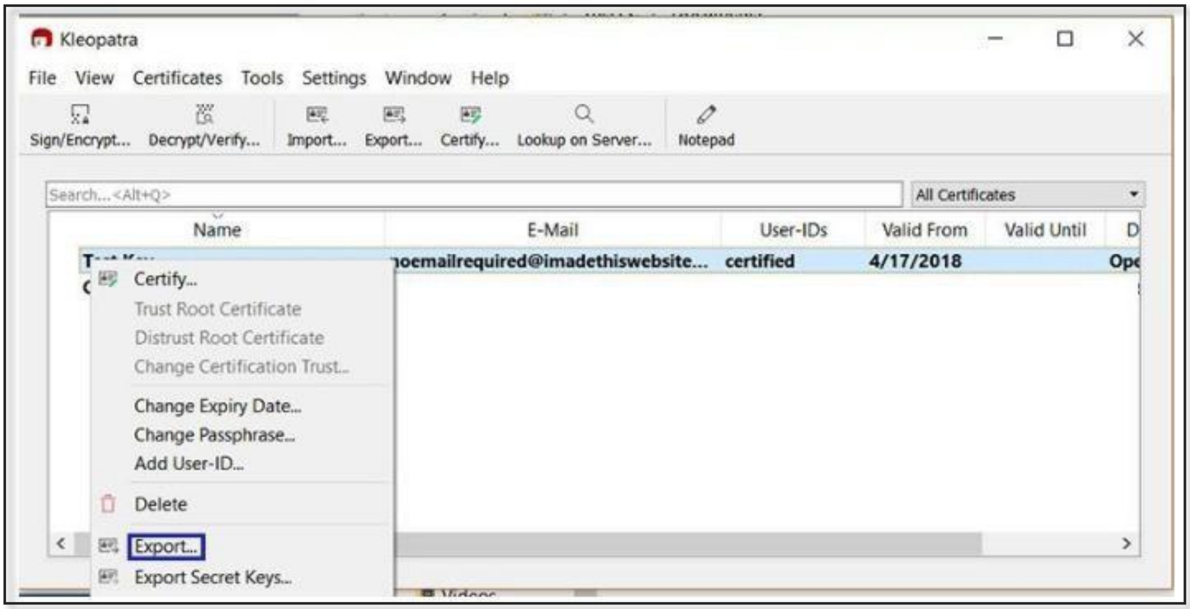
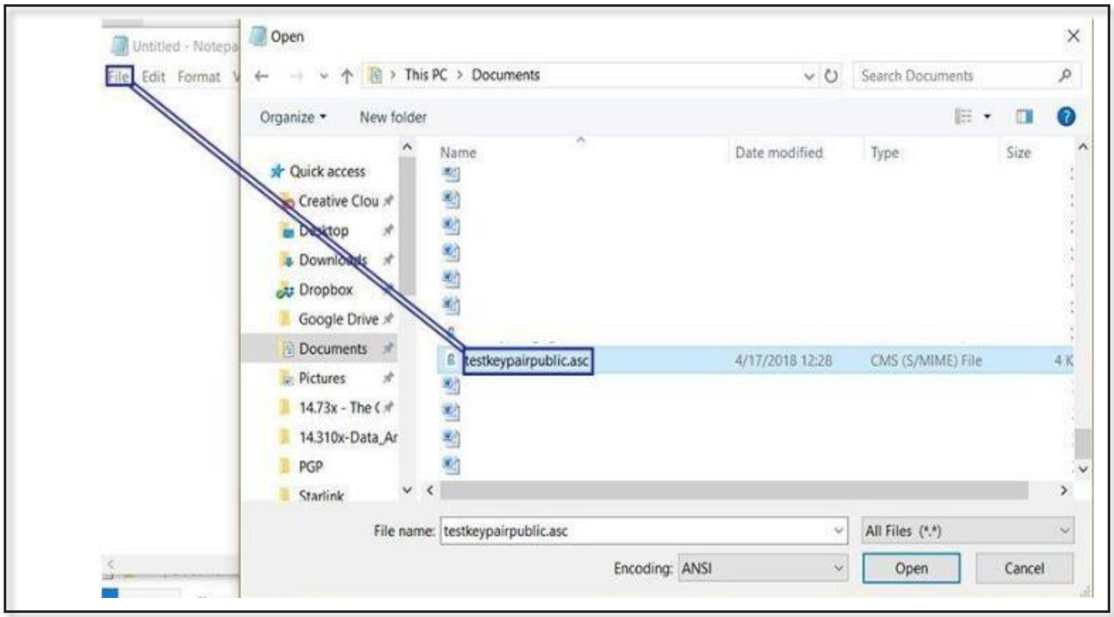


Figure 21 Exporting Public Key

Step 11: Choose the location to save the file. It will save as a .asc ASCII file. Then it can be opened with any text-editing app like Notepad.

Step 12: Go to “File” and then “Open” on time. Set the file type to “All files”. The public key file can be found in the saved location.



testkeypairpublic.asc 4/17/2018 12:28 CMS (S/MIME) File 4 K

File name: testkeypairpublic.asc

All Files (*.*)

Encoding: ANSI

Figure 22 Opening the saved Public key file

Step 13: Open it up with text editor to see the public key.

Step 14: User can export the private key with the same process. Instead of “Export Secret Keys” just “Export” is selected. Make sure this is stored in a safe location, or just keep it inside Kleopatra where it perfectly accessible.

These public and private keys can be used with any program that works with PGP, and Kleopatra itself can encrypt and decrypt files using user keys. If one wants to take them for a test run, encrypting a text file with the public key and decrypting it with their private key can be tried.

PGP is safe only if private key remains private. If it is disabled, then anyone will be able to read the message that is encrypted with public key. Depending on how secure one wants to be, the key should be kept on a hard drive or put them on a secure form of removable storage, like an encrypted USB drive.

7 End user email security best practices

These are practices used for ensuring security to end users who make use of e- mail systems. One of the best practices is educating the employees on handling e-mail security risks. This develops a great impact on the organization by preventing e-mail systems from unwanted exploits. Some of the end user e-mail security practices are as follows,

- Avoiding unwanted links and opening of attachments from unknown e-mail recipients.
- Creating strong passwords and changing them on regular basis.
- There should not be sharing of passwords even with colleagues.
- By checking whether sensitive information is sent only to required recipients with the help of spam filters.
- Using anti-virus software to block vulnerabilities.
- Using private software such as VPN's instead of public Wi-Fi connections to access corporate e-mail over personal remote devices.

A proper implementation of e-mail security measures in the enterprise network, helps the organisation helps in eradicating e-mail security risks. Employees can also prevent their sensitive data from loss or virus if they are provided with proper education and real-time practices.

Following are the tips that can be followed to secure the e-mail from spam or from virus threats that causes unwanted content replications. E-mail accounts can be secured in many ways. Organizations make use of two-combination approach such as educating employee and using comprehensive security protocols. The following are some of the practices to secure enterprise e-mail systems security,

- Educating employees by explaining them to be aware of phishing attacks by engaging them on real-time e-mail security risks.
- Creation of strong passwords by employees based on rules and mandatorily changing them every month strictly.
- Protecting the contents of e-mail and its attachments by implementing encryption techniques.
- Corporate employees wishing to access e-mail on their personal devices must use BYOD security.
- Using secure login using encryption methods on web mail applications.
- Deploying malware scanners and tools to scan and block e-mails that affect the files with malicious contents.

- Data protection solutions must be used in identifying and preventing sensitive data over e-mail transmissions.

3 Cloud Security

Cloud computing is one of the promised leading computing technologies for cloud service providers and cloud consumers. The emergence of cloud users has in IT sectors increase the need for new security standards for the challenges faced by them. Cloud security refers to the process of securing user resources. The cloud security features are different for different cloud models and are similar to any program that is installed and run on IT architecture.

Cloud computing security processes should also address the security controls that the cloud provider will incorporate to maintain the customer's data security, privacy and compliance with necessary regulations. The security process must include business continuity and data backup plan in the case of a security breach. The common security concerns that affect cloud systems are unauthorized exposure, leaking of data, exposure to vulnerable attacks, implementation of poor access controls, and the problems of data availability. Some of the basic cloud security protection measures for any cloud environment can be explained as follows,

- Ensure the safety of data and systems.
- Identify unusual behaviors.
- Examine the latest security state.
- Keep track of and react to unpredicted events.

The basic cloud security protection measures are displayed in figure 3

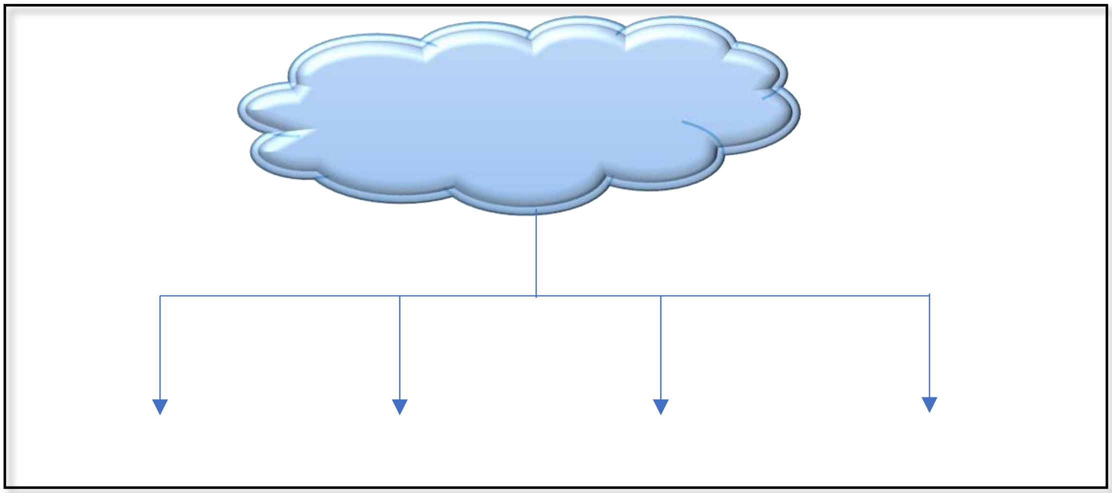


Figure 31 Basic Cloud Security Protection Measures

1 Cloud Deployment Models

As defined by National Institute of Standards and Technology (NIST) standard there are different cloud deployment models available such as Public, Private, Community and Hybrid. These models are designed and deployed to secure the privacy of users accessing the cloud resources. Apart from the standard models, a model named as Virtual Private Cloud (VPC) introduced by Amazon has the advantages of public and private clouds in terms of flexibility and security.

(i) Public Cloud – This type of cloud model is defined by a third-party provider over a public network to offer services and resources to the users present in the network.

(ii) Private Cloud – This cloud model is designed for a particular organization where services are provisioned and managed by a third party making it available to private users.

(iii) Community Cloud – It is a collaborative model where sharing of infrastructure takes place between different organizations having common security concerns.

(iv) Hybrid Cloud – It is a cloud model that uses a mix of above cloud models with co- ordination between two platforms.

(v) Virtual private cloud (VPC) – This type of cloud introduced by Amazon has major advantages over security of private cloud and flexibility of data in public clouds. It works based on the advantages of Virtual Private Network (VPN) by providing resources to customize security settings and network topology.

The different types of cloud deployment models are displayed in figure 3

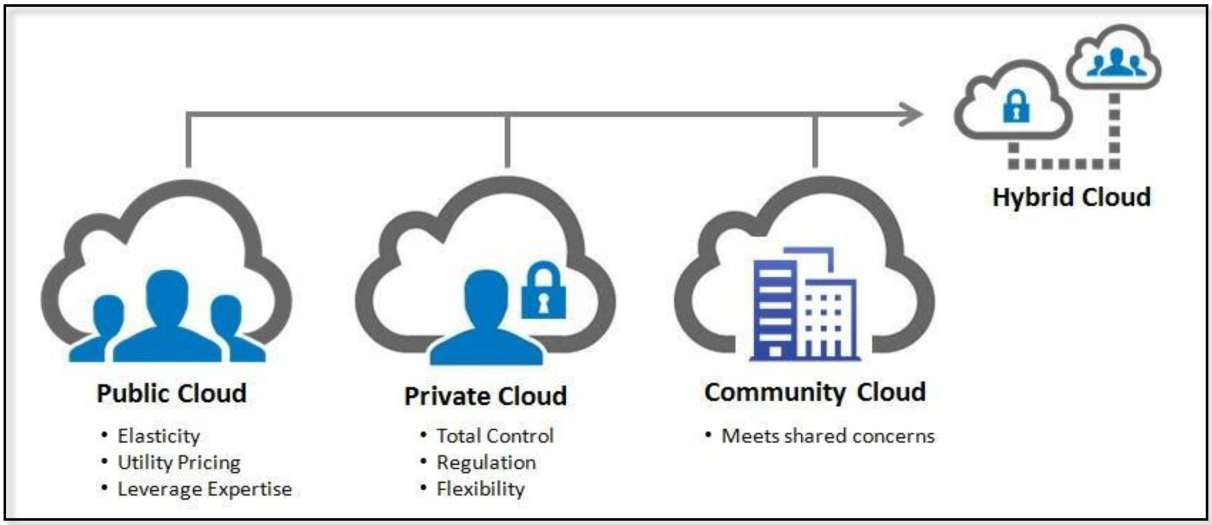


Figure 32 Cloud Deployment Models

2 Cloud Service Models

A cloud service model refers to the types of services provided to the cloud users. There are three main types of cloud services namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Apart from this, there are also other models emerging based upon services. The various cloud service models are displayed in figure 3

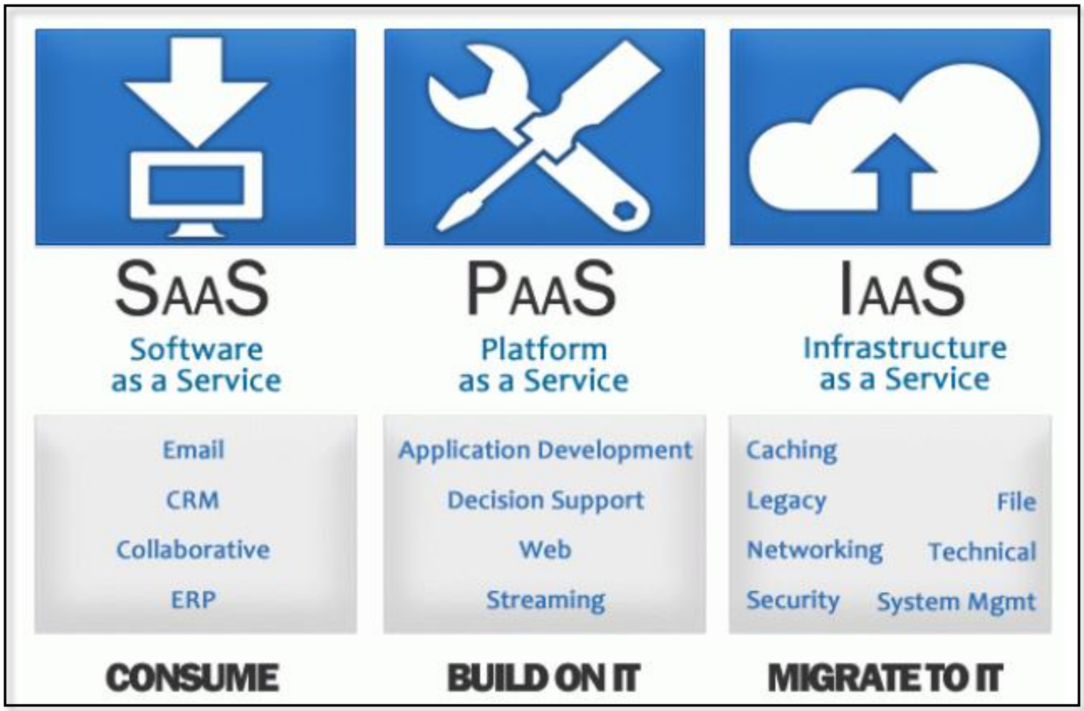


Figure 33 Cloud Service Models

1 Software-as-a-Service (SaaS)

SaaS is associated with software that is deployed on a hosted service and can be accessed globally over the Internet, most often through browser. It provides a complete infrastructure, software and solution stack as the service offering. Facebook and Gmail are some of the widely used SaaS type. SaaS supports multiple users and sharing of data through a single-instance, multi-tenancy model.

2 Platform-as-a-Service (PaaS)

PaaS describes the software environment in which a developer can create customized solutions within the context of the development tools that is provided by the platform. Platforms can be based on specific types of development languages, application frameworks or other constructs. Examples of PaaS includes Google AppEngine,

Windows Azure Platform etc.

6.4.2.3 Infrastructure-as-a-Service (IaaS)

This type of service model provides infrastructure resources as a service to the cloud users. These resources include virtual machines, virtual storage, virtual infrastructure and other hardware assets. It manages all other infrastructure services while the client is requests for it. This can include the operating systems, applications and user interactions with the system. Examples of IaaS are Amazon Elastic Compute Cloud
(EC2), Openstack, etc.

6.4.2.4 Human-as-a-Service (HuaaS)

HuaaS refers to the process of providing human resources as a service to the cloud users for predicting massive-scale data and aggregate their information. They make use of crowdsourcing and Crowdservicing that groups large number of people to investigate and provide information needed by the cloud users through innovative ideas. Examples of Crowdsourcing include community-based design and human-based
_computation.

6.4.2.5 Everything-as-a-Service (XaaS)

It is a service that refers to the approach of providing “everything” as a service and to consume. Nowadays most of the computing systems are stepping towards XaaS service model. Depending on the service requirement the cloud security features vary, and the models can be customized in a dynamic environment. Based upon various demands, customers can choose their own service types.

3 The Key Aspects of Cloud Security

The various aspects of cloud security depend upon the following three key areas,

- Management
- Operation and
- Technology

1 Management

The management aspect

of cloud security includes the following functions,

- Alteration of security policies such as updating and modifying the organization’s comprehensive security policy.
- Cloud security strategy is the organization’s security strategy based on cloud. This should be as whole or be a part in organization’s comprehensive security policy.
- Cloud security governance is the process of believing in and following the practices of cloud security strategy policies and its updates.
- Cloud security processes are those which are associated with cloud to incorporate it with existing amendments.
- Security roles & responsibilities are effective implementation managements which ensure cloud security elements by describing user actions (who and what are they doing).
- Cloud security guidelines are the advices given to organizations. They portrait methods to achieve security based on affecting factors.
- Cloud security assessment is the process of measuring the effectiveness of security offered by the cloud service provider.
- Service integration defines the incorporation of various cloud services at management level.
- IT & procurement security requirements are those that are used to obtain the overall security requirements of specific cloud.
- Cloud security management refers to the overall day-to-day management of cloud security.

2 Operation

Operation is the key aspect of cloud security that renders the following functions,

- Awareness & training programs on cloud security and its impact are to be conducted to educate employees and users by explaining their roles and functions.
- Incident management refers to identifying cloud related problems and provide responses to them.
- Configuration management ensures that the organization’s configuration is correctly configured by ensuring safe and secured services.
- Contingency planning is a pre-planned approach designed to keep track of cloud usage, recover from disaster and to maintain essential functions in a cloud.
- Maintenance refers to the process of up to date preservation of resources and services in cloud security.

- Media protection protects the cloud data surety by maintaining them properly.
- Environmental protection ensures protection of the environmental credentials by cloud service provider.
- System integrity defines the uprightness of cloud security system.
- Information integrity defines the process of ensuring the fairness of the information present in the cloud.
- Personnel security provides security to all personnel of cloud provider (both internal

staff and employees) to prevent them from service compromise.

3 Technology

The technology aspect of the cloud security includes the following functions,

- Access control Technology and software configuration allows only legitimate users to access the data.
- System Protection Technology is a protection mechanism used to prevent the systems from vulnerabilities that may involve a Distributed Denial-of-Service(DDoS) attack. Identification Technology identifies if cloud services are accessed by only authorized personnel.
- Authentication Technology authenticates cloud system access based on claimed users.
- Cloud security audits are auditing mechanisms used to maintain cloud security with the help of tools and processes.
- Identity and key management are the process of controlling the organization’s identity and security keys such as session and encryption keys.
- Physical security protection refers to the process of providing physical security controls in separate buildings for data access.
- Backup recovery and archive are used to maintain the data that is lost by the provider by backing up or recovering them using some tools and procedures. These data can also be archived to ensure data integrity in a cloud security system.
- Core infrastructure is the protection of servers and other core infrastructures.

4 Risks in Cloud Security

When the cloud security is weak, then there are high chances of risks that affect the cloud users in accessing the services. Lack of multi-factor authentication, usage of poor encryption mechanisms while storing the data in cloud are the major causes of risk in cloud security. Apart from this, there are other types of risks that can be,

- Loss or theft of intellectual property
- Compliance of violations and regulatory actions
- Loss of control over under user actions
- Malware infections that unleash a targeted attack
- Contractual breaches with customer or business partners
- Diminished customer trust
- Data breach requiring disclosure and notification to victims
- Increased customer churn
- Revenue losses

The various risks to cloud security are displayed in figure 3

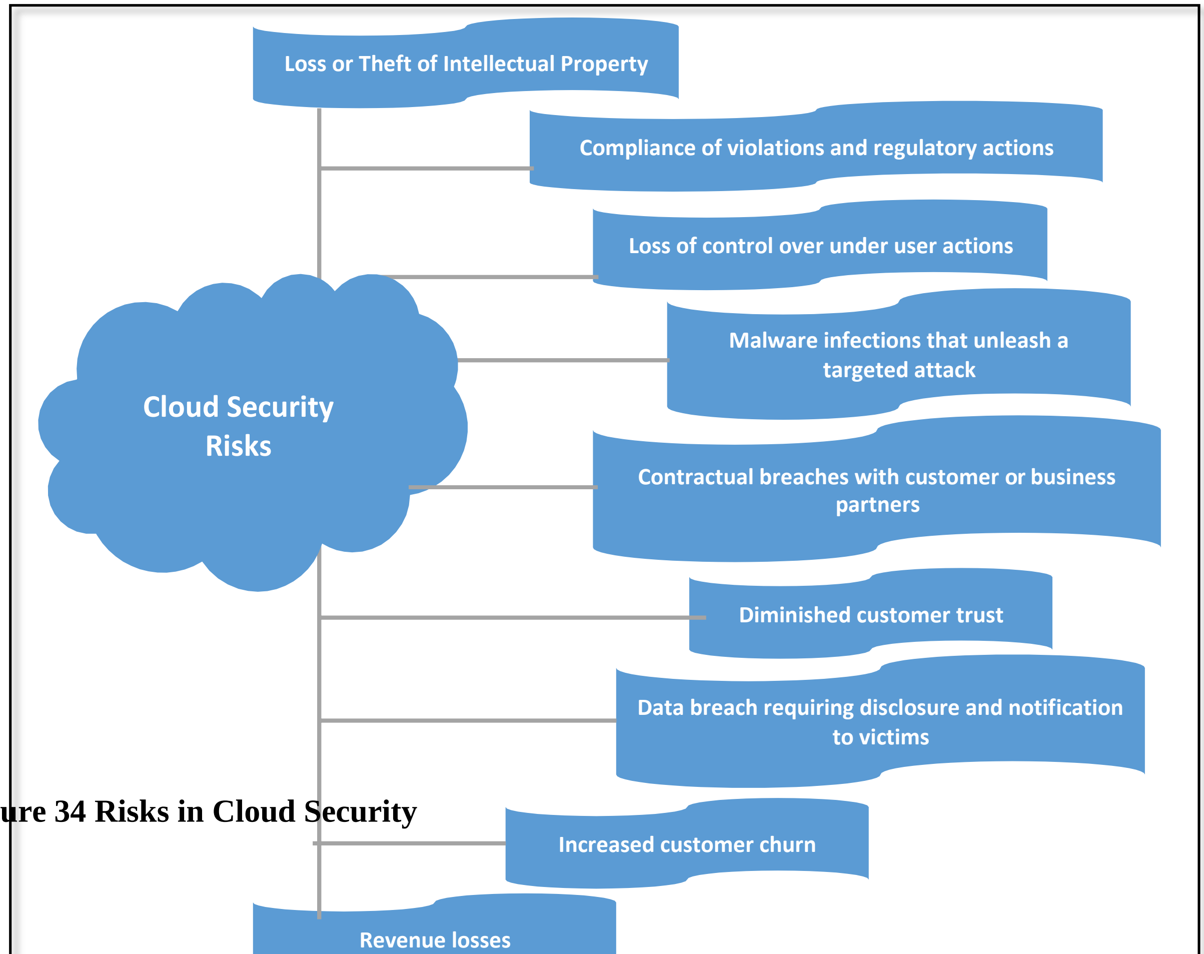

Loss or Theft of Intellectual Property
Compliance of violations and regulatory actions
Loss of control over under user actions
Malware infections that unleash a targeted attack
Cloud Security Risks
Contractual breaches with customer or business partners
Diminished customer trust
Data breach requiring disclosure and notification to victims
Increased customer churn
Revenue losses

Figure 34 Risks in Cloud Security

1 Loss or theft of intellectual property

Intellectual property is those that includes sensitive data of the owners that are intangible and protected with copyrights. Nowadays organizations store most of their confidential data on the cloud that also contains intellectual property. This property can face serious consequences such as being stolen or being lost by attackers. The hacker uses data breach techniques to succeed in their attempt. If the data is breached, then access to cloud data is gained. If access is denied, then other risks are experienced

violating the requirements of uploading owner data into the cloud system.

2 Compliance of violations and regulatory actions

At present, most of the companies follow regulatory control for their information. For example: HIPAA is used for private health information, FERPA is used for maintaining student's confidential records. There are other regulatories related to industry and governance. With the help of these regulations, organizations can identify where data is stored, who are the persons accessing it, how protection methods used. One major example of this risk is the state of non-compliance by Bring Your Own Computer(BYOC) or Bring Your Own Device(BYOD). It violates the regulations thereby putting the organizations to indirect consequences.

3 Loss of control over end user actions

This type of loss can occur when an employee is about to resign the job. At that time, one may take over the organization's confidential data that is stored in the cloud. There is a possibility to perform other actions such as downloading and uploading cloud data and storing them in a private cloud. Later after the resignation, one can access data from the private cloud. This is known as an insider threat and it pushes organizations to severe risks. This attack may be unknown until the company keeps a keen eye on the

_workers.

4 Malware infections that unleash a targeted attack

A major type of malware found in cloud services is data exfiltration. It performs malicious activity by unauthorized copying, transferring or retrieving data from the cloud. It is also used in the process of encoding sensitive data into video or audio files. This type of attack causes dangerous risks to user private data. They are also implemented to cause phishing attacks through sharing of malware infected files and services.

5 Contractual breaches with customers or business partners

Contracts are those which are used to define the rights of user access and authorized parties in an organization. Only employees who adhere to the contract are identified as authorized person and granted access for the data. Sometimes, these contracts can be breached by cybercriminals, violating the access rights and gaining control over business data stored in the cloud. This risk can happen when there is a violation in sharing the data with the users.

6 Diminished customer trust

This type of risks occurs mainly due to data breaches that happen to the user's confidential data stored in the cloud. When the attacker compromise user data, then the customers lack their trust on storing their data on cloud. This diminished customer trust may also happen during credit card frauds where the customer's account is under-taken by the attacker. Because of this risk, customer may lose trust over their cloud security mechanisms.

7 Data breach requiring disclosure and notification to victims

Due to data breach the company's confidential and sensitive information are uncovered. The company must send notifications to the victims. It is a very important approach in data protection related to health care industries. The regulation authorities can levy fine on the company, if proper disclosure is not practiced.

8 Increased customer churn

The customers have every right to change their choice on the cloud type based on the security controls. It is advisable to avoid cloud services if the customer privacy is not provided in a safe manner.

9 Revenue losses

When the customer become aware of data breaches of the organization, then they can move their data to other cloud service provider who ensures proper security. This results in the revenue losses to the service provider thereby leading to all other customers changing their services to other cloud service providers.

5 Tools used in Cloud security

OpenStack is an open source software that is used for creating private and public clouds. It is intended to control the access of the resources in a datacenter through a dashboard or through OpenStack API. With OpenStack, users can create virtual machines to run multiple tasks at the same time using instances.

Users can quickly create a new Virtual Machine (VM) or an instance upon which other cloud components can run. On the platform provided users can develop and deliver applications to the end users.

6 The Steps towards an Effective Cloud Security Team

There are generally seven steps towards an effective cloud security team and they are as follows,

- Developing a cloud security strategy
- Focusing on federated model
- Moving closer to contracts and the business
- Managing multiplicity
- Securing the exit
- Building diverse teams and
- Seeking out security standards

Figure 35 shows the steps towards an effective Cloud Security Team.

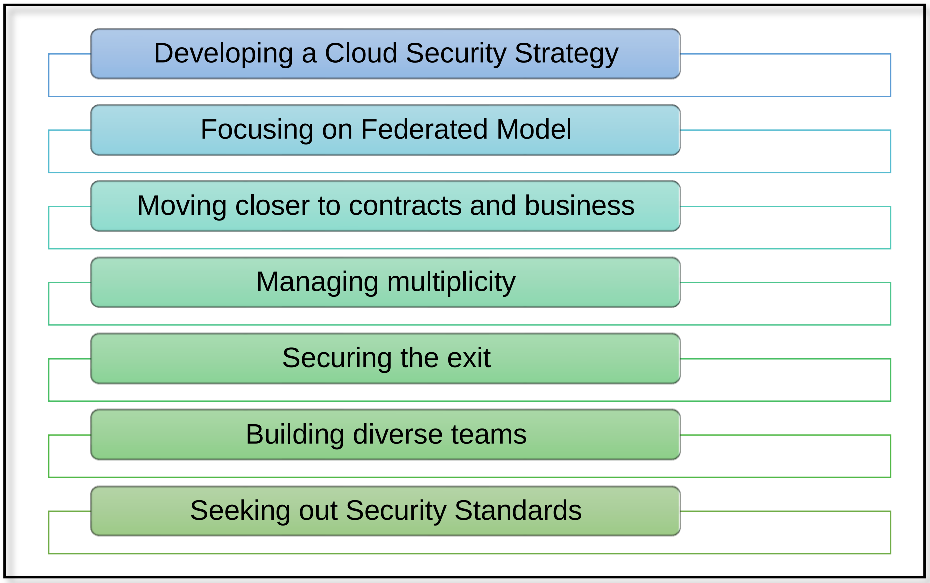

Developing a Cloud Security Strategy
Focusing on Federated Model
Moving closer to contracts and business
Managing multiplicity
Securing the exit
Building diverse teams
Seeking out Security Standards

Figure 35 Step Towards an Effective Cloud Security Team

1 Developing a cloud security strategy

Developing a proper security strategy by security teams is necessary to maintain the organization's information. The security teams are responsible for updating and processing the cloud to provide proper security policies and procedures. This refers to the addition or extending current polices with new security ideas. It also has indirect effects on security teams by examining the violating policies.

2 Focusing on a federated model

Due to the increasing adoption of cloud services, it is important for the security team to focus on creating a combined model that provides various cloud protection mechanisms. For this purpose, a federated model that authenticates and authorizes the services around the organization's boundary should be considered. A cloud model that is centralized is less secured. The security team is responsible for addressing the security issues and to provide methods to overcome risks.

3 Moving closer to contracts and the business

To meet the requirements of the organization's security, the security team should develop policies based on strong contracts. These contracts are useful for ensuring security by providing assessment criteria including assurance and compliance of data and services. Outsourcing of cloud resources require these contracts for effectiveness.

6.4.6.4 Managing multiplicity

It is necessary for the security teams to understand and manage cloud security risks in multiple cloud service providers. When multiple clouds are present, the risks of data availability are larger. Hence the security team should be responsible for managing these issues using multiplicity concepts.

6.4.6.5 Securing the exit

Whenever a cloud service contract is terminated, it is much important to examine the service provider system for left-over sensitive data. The databases, archives and backups are also audited because they are the major data storage places. Secure exit is an important factor to be considered during the procurement stage.

6 Building diverse teams

The cloud security system may be highly compromised due to some risks. The in- house technical staff is one of the reason for causing this risk. The security system must be builtinvolving diverse teams, combining the security representatives of cloud service

Seeking out security standards

It is important to set up security standards for providing cloud data security depending on different types of cloud service providers. These standards are to be provided by the security teams based on the organization’s requirements. Looking out for security standards are increasingly growing. Nowadays due to increasing demands for Cloud Services.