Security issues in Cloud

Need for Security and Privacy in Cloud

- Cloud computing - grid + distributed computing, utilizing the Internet as a service delivery network.
- The public Cloud environment is extremely complex when compared to a traditional data center environment.
- Virtual environments are used in Cloud to achieve multi-tenancy.
- Vulnerabilities in virtual machines pose direct threat to the privacy and security of the Cloud services.

Cont..

- Shared and distributed resources in the Cloud systems make it hard to develop a security model for ensuring the data security and privacy.
- Due to transparency issues, no Cloud provider allows its customers to implement intrusion detection or security monitoring systems extending into the management services layer behind virtualized Cloud instances.

Security issues in cloud computing

- Vulnerabilities - the loopholes in the security architecture of Cloud, which can be exploited by an adversary via sophisticated techniques to gain access to the network and other infrastructure resources.
- A threat - a potential (or actual adverse) event that may be malicious or incidental (i.e. failure of a storage device), compromising Cloud resources.
- An attack - an action to harm Cloud resources.
- Exploitation of vulnerabilities would affect the availability and economic benefit of Cloud computing.

Vulnerabilities in Cloud computing

- Virtualization/multi-tenancy is the basis for Cloud computing architecture.
- Mainly three types of virtualization : OS level, application level, and Hypervisor level.
- In OS level virtualization, multiple guest OSs are running on host OS that has visibility and control on each guest OS. In this, an attacker can get control on the entire guest OSs by compromising the host OS.
- In application based virtualization, virtualization is enabled on the top layer of the host OS. In this, each VM has its guest OS and related applications. Application based virtualization also suffers from the same vulnerability as in OS based vulnerabilities.
- Hypervisor or virtual machine monitor (VMM) is just like code embedded to host OS. Such code may contain native errors. This code is available at boot time of the host OS to control multiple guest OSs. If the hypervisor is compromised, then the entire controlled guest OSs can be compromised.
- Vulnerabilities in virtualization or hypervisor allows an attacker to perform cross-VM side-channel attacks and DoS attacks. For instance, a malformed code in Microsoft's Hyper-V run by an authenticated user in one of the VM caused a DoS attack.

Cont..

- Vulnerabilities in Internet protocols may prove to be an implicit way of attacking the Cloud system that include common types of attacks like man-in-the-middle attack, IP spoofing, ARP spoofing, DNS poisoning, RIP attacks, and flooding.
- Vulnerabilities like SQL injection flaw, OS injection flaw, and Lightweight Directory Access Protocol (LDAP) injection flaw are used to disclose application components. Such vulnerabilities are the outcomes of defects in design and architecture of applications. These data may be the organization's applications or private data of other organization's applications residing on the same Cloud.

Cont..

- Cloud providers publish a set of software interfaces (or APIs) that customers can use to manage and interact with Cloud services. Service provisioning, management, orchestration, and monitoring are performed using these interfaces via clients (e.g. Web browser).
- Security and availability of Cloud services depend on the security of these APIs.
- Examples of browser based attacks (HTML based services) are SSL certificate spoofing, attacks on browser caches and phishing attacks on mail clients

Threats to cloud computing

- **Changes to business model -** Cloud computing changes the way in which IT services are delivered. As servers, storage and applications are provided by off-site external service providers, organizations need to evaluate the risks associated with the loss of control over the infrastructure. (A reliable end-to-end encryption and appropriate trust management scheme can simplify such a threat to some extent.)
- **Abusive use of Cloud computing -** Cloud computing provides several utilities including bandwidth and storage capacities. Some vendors also give a predefined trial period to use their services. However, they do not have sufficient control over the attackers, malicious users or spammers that can take advantages of the trials. These can often allow an intruder to plant a malicious attack and prove to be a platform for serious attacks. Areas of concern include password and key cracking, launching dynamic attack points, DDoS, Captcha solving farms, etc. Such threats affect the IaaS and PaaS service models. (For protection, initial registration should be through proper validation/verification and through stronger authentication. In addition to this, the user's network traffic should be monitored comprehensively.)

Cont..

- **Insecure interfaces and API -** Cloud providers often publish a set of APIs to allow their customers to design an interface for interacting with Cloud services. These interfaces often add a layer on top of the framework, which in turn would increase the complexity of Cloud. Such type of threat may affect the IaaS, PaaS, and SaaS service models. (This can be avoided by using a proper security model for Cloud provider's interface and ensuring strong authentication and access control mechanism with encrypted transmission.)

- **Malicious insiders -** Most of the organizations hide their policies regarding the level of access to employees and their recruitment procedure for employees. However, using a higher level of access, an employee can gain access to confidential data and servicesThis type of threat may be relevant to SaaS, PaaS, and IaaS. (To avoid this risk, more transparency is required in security and management process including compliance reporting and breach notification.)

Cont..

- **Shared technology issues/multi-tenancy nature -** In multi-tenant architecture, virtualization is used to offer shared on-demand services. This type of threat affects IaaS. (Implementation of SLA for patching, strong authentication, and access control to administrative tasks are some of the solutions to address this issue.)

- **Data loss and leakage -** This may include data compromise, deletion, or modification. Due to the dynamic and shared nature of the Cloud, such threat could prove to be a major issue leading to data theft. This threat can applicable to SaaS, PaaS, and IaaS. (Solutions include security of API, data integrity, secure storage for used keys, data backup, and retention policies)

Cont..

- **Service hijacking -** Service hijacking may redirect the client to an illegitimate website. User accounts and service instances could in turn make a new base for attackers. This threat can affect IaaS, PaaS, and SaaS. (Some of the mitigation strategies to address this threat include security policies, strong authentication, and activity monitoring.)
- **Risk profiling -** Cloud offerings make organizations less involved with ownership and maintenance of hardware and software. This offers significant advantages. However, this makes them unaware of internal security procedures, security compliance, hardening, patching, auditing, and logging process and expose the organization to greater risk. (To avoid this Cloud provider should disclose partial infrastructure details, logs, and data. In addition to this, there should also be a monitoring and alerting system.)

Cont..

- **Identity theft -** Identity theft is a form of fraud in which someone pretends to be someone else, to access resources or obtain credit and other benefits. The victim (of identity theft) can suffer adverse consequences and losses and held accountable for the perpetrator's actions. Relevant security risks include weak password recovery workflows, phishing attacks, key loggers, etc. This affects SaaS, PaaS, and IaaS. (The solution is to use strong authentication mechanisms.)

Attacks on Cloud computing

- **Zombie attack -** Through the Internet, an attacker tries to flood the victim by sending requests from innocent hosts in the network. These types of hosts are called *zombies*. The Cloud may be overloaded to serve a number of requests, and hence exhausted, which can cause DoS (Denial of Service) or DDoS (distributed denial of service) to the servers. Cloud in the presence of attacker's flooded requests cannot serve valid user's requests. (Better authentication and authorization and IDS/IPS can provide protection against such an attack.)
- **Service injection attack -** Cloud system is responsible for determining and eventually instantiating a free-to-use instance of the requested service. The address for accessing that new instance is to be communicated back to the requesting user. An adversary tries to inject a malicious service or new virtual machine into the Cloud system and can provide malicious service to users. (Service integrity checking module should be implemented. Strong isolation between VMs may disable the attacker from injecting malicious code in the neighbour's VM.)

Cont..

- **Attacks on virtualization -** There are mainly two types of attacks performed over virtualization: VM Escape and Rootkit in hypervisor.
- VM Escape*:* An attacker's program running in a VM breaks the isolation layer in order to run with the hypervisor's root privileges instead with the VM privileges. This allows an attacker to interact directly with the hypervisor. Therefore, VM Escape from the isolation is provided by the virtual layer. By VM Escape, an attacker gets access to the host OS and the other VMs running on the physical machine.

- Rootkit in Hypervisor*:* VM-based rootkits initiate a hypervisor compromising the existing host OS to a VM. The new guest OS assumes that it is running as the host OS with the corresponding control over the resources, however, in reality this host does not exist. (This allows an attacker to control over any VM running on the host machine and to manipulate the activities on the system.)

Cont..

- **Man-in-the Middle attack -** If secure socket layer (SSL) is not properly configured, then any attacker is able to access the data exchange between two parties. In Cloud, an attacker is able to access the data communication among data centers. (Proper SSL configuration and data communication tests between authorized parties can be useful to reduce the risk of Man-in-the-Middle attack.)

- **Metadata spoofing attack -** An adversary modifies or changes the service's Web Services Description Language (WSDL) file where descriptions about service instances are stored. If the adversary succeeds to interrupt service invocation code from WSDL file at delivering time, then this attack can be possible. (To overcome such an attack, information about services and applications should be kept in encrypted form. Strong authentication (and authorization) should be enforced for accessing such critical information.)

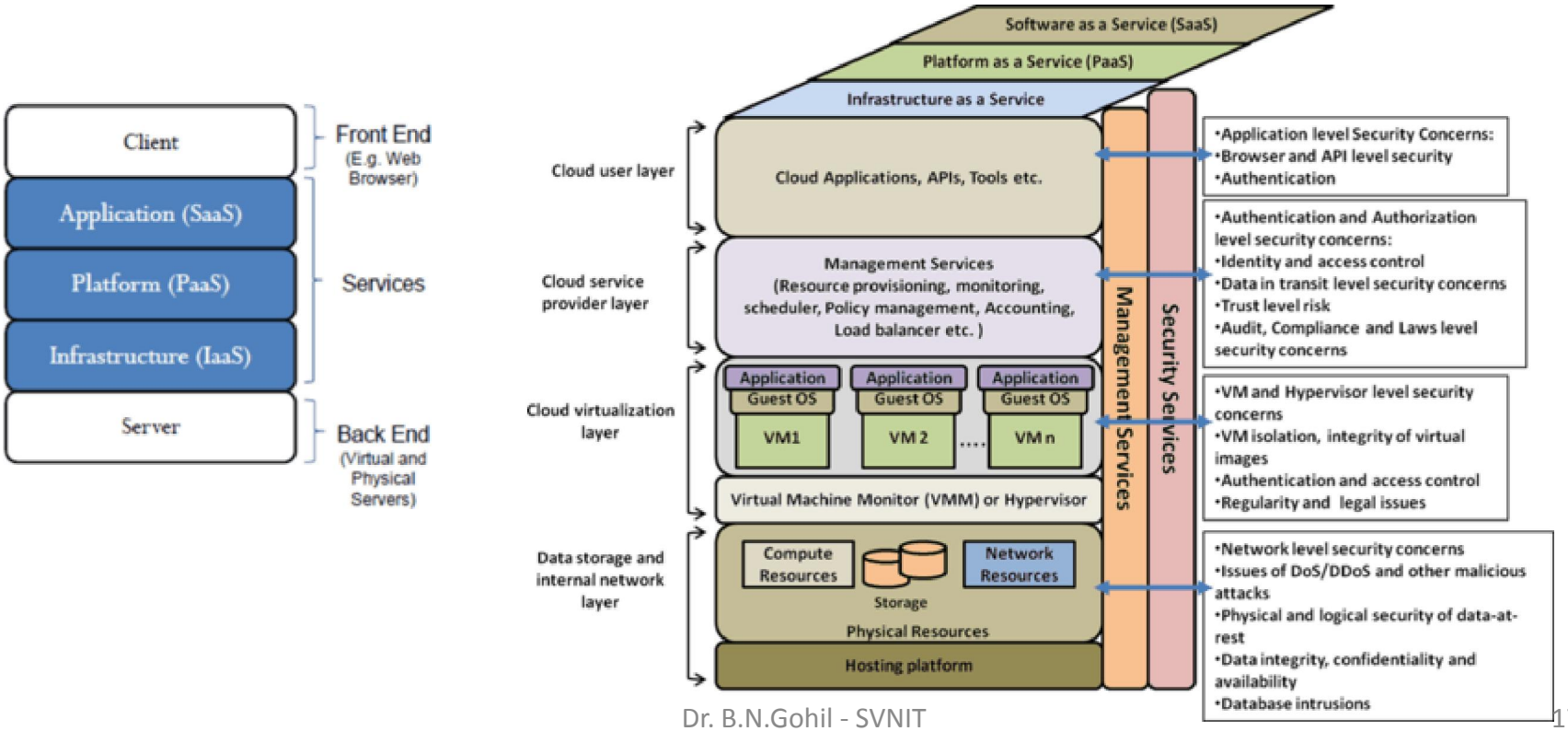
Cont..

- **Phishing attack -** Phishing attacks are well known for manipulating a web link and redirecting a user to a false link to get sensitive data.

- **Backdoor channel attack -** It is a passive attack, which allows hackers to gain remote access to the compromised system. Using backdoor channels, hackers can be able to control victim's resources and can make it a *zombie* for attempting a DDoS attack. (Better authentication and isolation between VMs can provide protection against such attacks.)

Security issues at different layers in Cloud

- Different layers with associate security concerns in cloud enabled system:



Application level security issues

- It refers to the usage of software and hardware resources for providing security to applications such that the attackers are not able to get control over applications and make desirable changes to their format.
- Since Web applications and SaaS are tightly coupled with providing Cloud services, the security and availability of general cloud services are dependent upon the security of Web browsers, APIs and vulnerability free applications.
- A Web browser is the platform independent client program that is mostly used to access the Cloud services (SaaS), web applications, web pages, or web 2.0. It uses SSL/TLS protocols for secure transmission and authentication of data.
- Therefore, attacks on browser based Cloud authentication directly affect the security of Cloud applications. Any attacker can get access to other user's XML tokens (authentication related credentials in the browser) and accesses the services of the victim. One of the solutions viz; XML signature and XML encryption can be used to enhance browser security.

Cont..

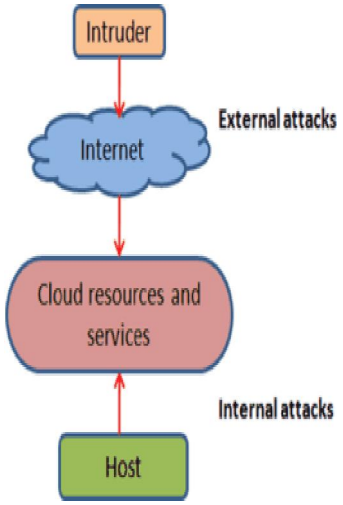
- **Service availability -** Temporary or permanent loss of services and DoS/DDoS attacks are the main threats affecting availability of Cloud services. For better QoS, services should be available as promised when they are requested.
- One such incident is the database cluster failure caused at Salesforce.com.
- In February 2011, Gmail went down for a few hours and due to service disruption, 0.29 % of Gmail users were affected and lost their previous emails and other data.
- On March 28, 2011, thousands of users registered at Intuit (which offers financial and tax preparation software and related services) experienced an outage for 2 to 5 days during the network configuration update and scheduled maintenance. As a result, customers were blocked to access offered services. To address such issues, proper configuration of an IDS/IPS can be investigated.

Cont..

- **Integrity of workload state -** The integrity for the state of a workload should be preserved to ensure expected results. Applications involving workflows are required to store temporary results of computation at different levels. There is no standard mechanism used to secure such sensitive files. If these sensitive files are disclosed to an attacker, he/she may be able to threaten the expected behavior of the application.

Network level security issues

- The network is the backbone of Cloud, and hence vulnerabilities in network directly affect the security of Cloud.
- Security issues at network level should be considered in terms of both external and internal networks.
- An adversary outside the Cloud network often performs DoS or DDoS attacks to affect the availability of Cloud services and resources.
- DoS/DDoS attacks reduce the bandwidth and increases the congestion causing poor service to the users.
- Due to the distributed nature of the Cloud, it is hard to prevent DoS/DDoS and Economic Denial of Sustainability (EDoS can be called as HTTP and XML based DDoS) attacks.



Cont..

- Some common attacks at the network layer are DNS poisoning attack, Sniffer attack, Port scanning, Cross site scripting, ARP spoofing, IP spoofing, and phishing attack, which are executed to gain access of Cloud resources.
- Internal network attacker (authorized users or users within the cloud network) can easily get access to other user's resources without being detected. An insider has higher privileges and knowledge (related to network, security mechanism, and resources to attack) than the external attacker. Therefore, it is easy for an insider to penetrate an attack than external attackers.
- Major security issues at network level include vulnerabilities in Internet protocols, authorization, and authentication, intrusions, backdoor attack, session hijacking, and clear data transmission.
- To address some of the issues at the network level, major Cloud providers (like Amazon, Window Azure, Rack Space, Eucalyptus, etc.) are running their applications behind firewall. It only provides security at boundary of network and cannot detect the internal attacks. Network based intrusion detection system (NIDS) can be integrated to address some of the security issues.
- NIDS should be configured for detecting external intrusions as well as internal intrusions. It should also be capable of detecting intrusions from encrypted traffic.

Data storage level security issues

- Security issues during data-in-transit, data-at-rest, data lineage, data eminence, data provenance, data recovery, data location, data breaches, and investigative support.
- In data-in-transit, adversary in network affects the confidentiality and integrity of data. The biggest risks for data-in-transit include poor encryption technology and network protocols.
- Data at rest (stored in Cloud storage) needs physical, logical, and personnel access control policies.

Cont..

- Tracing the data path is known as data lineage and it is important for auditing purposes in the cloud. Due to the shared environment, maintaining the integrity of data is the most challenging task in the Cloud.
- Data-Remanence refers to the data left out in case of data transfer or data removal. It causes minimal security threats viz; disclosure of sensitive information, data sold to others, etc.
- Data recovery is one of the most challenging problems. Data can be lost due to accidental damage or natural disaster to storage. It poses a risk to data availability for users.
- Tracing location of data is difficult in the Cloud since user's data are dynamically migrated from one region (or country) to another region (or country). It increases risk of data privacy and security since data owner loses the control over his/her data.

Virtualization level security issues

- In the virtualized (multi-tenant) environment, multiple OSs run concurrently on a host computer using hypervisor.
- As the number of guest operating systems (OSs) running on a hypervisor increase, the security concerns with that newer guest OSs also increase. Because it is not possible to keep track of all guest OSs, and hence maintaining the security of those OSs is difficult.
- It may happen that a guest system tries to run a malicious code on the host system and bring the system down or take full control of the system and block access to other guest OSs.

Cont..

- Isolation between two VMs is not completely adequate by current virtual machine monitors (VMMs).
- By compromising the lower layer hypervisor vulnerabilities, an attacker can gain control over installed VMs, for example, Bluepill, SubVirt, and DKSM are some well-known attacks on the virtual layer.

Cont..

- Virtualization based malware and rootkit: New generation of rootkits that benefit from the processor technology that allows an attacker to insert an additional hypervisor between the hardware and the software.
- The hypervisor takes control of the system and converts the original operating system into a virtual guest on the fly.
- In contrast to software-based virtualization, this kind of hijacking does not need a restart, and that makes it all the more difficult to detect the intrusion.

Cont..

- Sharing of VM images in Cloud introduces security risks.
- The owner of an image is concerned about confidentiality (e.g. unauthorized accesses to the image). The user of an image is concerned about safety (e.g. a malicious image that is capable of corrupting or stealing the user's own private data).

Authentication and access control level security issues

- In Cloud, client's information is transmitted over the Internet, which poses data ownership issues. As this information is processed outside the enterprise, it brings an inherent level of risk.
- This issue is addressed by providing support for security assertion markup language (SAML) federation protocol (which contains authentication credentials in the form of SAML assertions) with their own authentication protocol.
- SAML is issued to exchange information, such as assertions related to a subject or authentication information between the cooperating domains. The request and response messages of it are mapped over Simple Object Access Protocol (SOAP) relying on XML.
- Using a Signature Wrapping Attack, it is possible to modify an eavesdropped message despite of it being digitally signed. Thus, an attacker may be able to execute arbitrary machine commands on behalf of a legitimate user.
- To address such issues, data should be transmitted via secured channel and fine-grained authentication and authorization techniques can be used for preventing data from unauthorized access.

Trust level security issues

- This is one of the serious problems in the Cloud.
- Since users have lack of control over resources, they have to rely on trust mechanisms and contracts in conjunction with mechanisms that provide a compensation.
- Trust is a very fuzzy concept and very difficult to calculate in a heterogeneous environment that is assessed by a human or social trust.
- Contractors may be sub-contracting without user's knowledge.
- Limiting visibility of network and system monitoring to user poses major trust issues.
- Contract requirements may not be propagated down the sub-contract chain.
- Employees (authorized users) or malicious insiders of organizations often perform attacks that affect the confidentiality and privacy of other users' data as well as resources.

Cont..

- Lack of public relations poses a trust issue.
- Data processing outside the organizations poses an inherent level of risk. There is no direct control on some service components outside the organization.
- Limiting visibility of network and system monitoring to user may also pose a trust issue.
- This issue can be addressed by providing an adequate means of visibility of the monitoring system.
- Cross-site scripting, access control weaknesses, insecure storage, and insecure configuration are some of the threat examples.
- Advanced cryptographic techniques and signature techniques can be used to address trust issues when outsourcing data.

Security issues related to auditing, regulatory compliance and laws

- Audit and compliance to internal processes and external processes must be met with classified requirement and customer agreements, laws, and regulations. Therefore, such policies should be monitored.
- The multi-tenancy nature of Cloud increases the difficulty of monitoring and logging process of VMs.
- Due to the dynamic nature of the Cloud, it is difficult to audit and manage compliance by coordination with external auditing and regulatory bodies.
- There are different types of compliance.

Cont..

- Privacy compliance*:* Only owners of the data are responsible for the security and privacy of their outsourced data even if the data is held by a service provider. This is due to the various laws and regulations in different countries. It poses a risk of data security, confidentiality, and availability. This is an open problem for providing transparency and controlled environment to owners about their data.

- Geographic compliance*:* If the tenant or cloud customer operates in the United States, Canada, or the European Union, they are subject to numerous regulatory requirements. These include control objectives for information and related technology. These laws might relate to where the data is stored or transferred, as well as how well this data is protected from a confidentiality aspect.

- Industry compliance*:* Industry compliance considerations are typically seen as an area where many Cloud migrations flounder. Typical regulatory requirements can include: Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), Federal Information Processing Standard (FIPS) 140-2, and Trusted Internet Connections (TIC) compliance.

Security standards

- It defines the processes, procedures, and practices necessary for implementing a security program.
- These standards also apply to cloud related IT activities and include specific steps that should be taken to ensure a secure environment is maintained that provides privacy and security of confidential information in a cloud environment.

Security Assertion Markup Language (SAML)

- SAML is an XML-based standard for communicating authentication, authorization, and attribute information among online partners.
- It allows businesses to securely send assertions between partner organizations regarding the identity and entitlements of a principal.
- The Organization for the Advancement of Structured Information Standards (OASIS) Security Services Technical Committee is in charge of defining, enhancing, and maintaining the SAML specifications.
- SAML is built on a number of existing standards, namely, SOAP, HTTP, and XML.
- SAML relies on HTTP as its communications protocol and specifies the use of SOAP.
- SAML assertions and protocols are specified using XML schema.
- Both SAML 1.1 and SAML 2.0 use digital signatures(based on the XMLSignature standard) for authentication and message integrity.

Open Authentication (OAuth)

- OAuth is an open protocol, initiated by Blaine Cook and Chris Messina, to allow secure API authorization in a simple, standardized method for various types of web applications.
- OAuth is a method for publishing and interacting with protected data.
- For developers, OAuth provides users access to their data while protecting account credentials.
- OAuth allows users to grant access to their information, which is shared by the service provider and consumers without sharing all of their identity.
- The Core designation is used to stress that this is the baseline, and other extensions and protocols can build on it.
- OAuth by itself provides no privacy at all and depends on other protocols such as SSL to accomplish that.
- With Oauth, sites use tokens coupled with shared secrets to access resources.
- Secrets, just like passwords, must be protected.

OpenID

- OpenID is an open, decentralized standard for user authentication and access control that allows users to log onto many services using the same digital identity.
- It is a single-sign-on (SSO) method of access control.
- It replaces the common log-in process (i.e., a log-in name and a password) by allowing users to log in once and gain access to resources across participating systems.
- An OpenID is in the form of a unique URL and is authenticated by the entity hosting the OpenID URL.
- The OpenID protocol does not rely on a central authority to authenticate a user's identity.
- Neither the OpenID protocol nor any web sites requiring identification can mandate that a specific type of authentication be used; nonstandard forms of authentication such as smart cards, biometrics, or ordinary passwords are allowed.
- A typical scenario for using OpenID might be something like this: A user visits a web site that displays an OpenID log-in form somewhere on the page. Unlike a typical log-in form, which has fields for user name and password, the OpenID log-in form has only one field for the OpenID identifier (which is an OpenID URL). This form is connected to an implementation of an OpenID client library. A user will have previously registered an OpenID identifier with an OpenID identity provider. The user types this OpenID identifier into the OpenID log-in form.