Minimization of Security Issues in Cloud Computing

Razi AHMED
Newports Institute of Communications and Economics, Karachi

Mushtaq HUSSAIN
Newports Institute of Communications and Economics, Karachi

Talat Sharafat RAHMANI
NUST, Karachi

Asif MANSOOR
NUST, Karachi.

Muhammad Liaquat ALI
University of Karachi.

Abstract

Cloud computing is a set of Information Technology (IT) services that are provided to a customer over a network on leased basis and with the ability to scale up or down their service requirements. Cloud services are delivered from data centers located throughout the world. Cloud computing facilitates its consumers by providing virtual resources via internet. General example of cloud services is Google Apps, provided by Google and Microsoft SharePoint. Security has remained a constant issue for Open Systems and internet. Lack of security is the only hurdle in the wide adoption of cloud computing. Cloud computing is surrounded by many security issues like securing data, and examining the utilization of cloud by the cloud computing vendors.

Keywords

Cloud Computing, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Multi-tenancy, Virtual Machines, Risk-adaptable Access Control, Identity management (IDM)

1 Introduction

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable and reliable computing resources (e.g. networks, servers, storage, application and services) that can be rapidly provisional and released with minimal consumer management efforts or service provider interaction. Besides, resources of cloud computing are dynamic and scalable. Cloud computing is independent computing it is totally different from grid and utility computing.

Software as a Service (SaaS):

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure and accessible from various client devices through a thin client interface such as a web browser. In other words, in this model, a complete application is offered to the customer as a service on demand. A single instance of the service runs on the cloud and multiple end users are services. On the customer systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Currently, SaaS is offered by companies such as Google, Salesforce, Microsoft and Zohoetc.

Platform as a Service (PaaS):

In this model, a layer of software or development environment is a side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lower, since only a single application needs to be hosted and maintained. In summary, in this model, the customers do not manage or control the underlying cloud infrastructure, network, servers, operates encapsulated and offered as a service. Upon which other higher levels of service are built. The customer has the freedom to build his own applications, which run on the provider's infrastructure. Hence a capability is provided to the customer to deploy onto the cloud infrastructure, customer-created applications using programming languages and tools supported by the provider (e.g., Java, Python and .Net etc.). Although the customer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, or storage, but he/she has the control over the deployed applications and possibly over the application hosting environment configurations. To meet manageability and scalability requirements of the applications, PaaS providers offer a predefined' combination of operating systems and application servers, such as LAMP (Linux, Apache, MySql and PHP) platform, restricted J2EE, Ruby etc. Some examples of PaaS are: Google's App Engine, Force.com etc.

Infrastructure as a Service (IaaS):

This model provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data center space etc. are pooled and made available to handle workloads. The capability provided to the customer is to rent processing, storage, networks, and other fundamental

computing resources where the customer is able to deploy and run arbitrary software, which can include operating systems and applications. The customer does not manage or control the underlying cloud infrastructure but has the control over operating systems, storage, deployed applications and possibly select networking components (e.g., firewalls, load balancers etc.). Some examples of IaaS are: Amazon, GoGrid, 3 Tera etc. The above information is furnished in Fig. 1

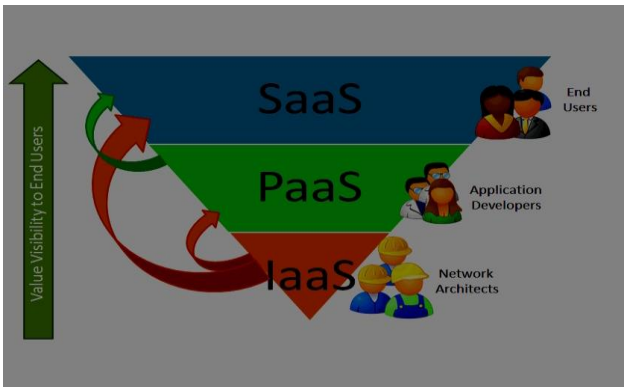


Fig. 1

2 Literature Review:

Cloud Service Deployment and Consumption Models:

Regardless of the delivery model utilized (SaaS, PaaS, IaaS) there are four primary ways in which cloud services are deployed (CSA Security Guidance, 2009). Cloud integrators can play a vital role in determining the right cloud path for a specific organization.

Public Cloud:

Public clouds are provided by a designated service provider and

may offer either a single- tenant (dedicated) or multi-tenant (shared) operating environment with all the benefits and functionality of elasticity and the accountability/utility model of cloud. The physical infrastructure is generally owned by and managed by the designated service provider and located within the provider's data centers (off-premises). All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. One of the advantages of a public cloud is that they may be larger than an enterprise cloud, and hence they provide the ability to scale seamlessly on demand.

Private Cloud:

Private clouds are provided by an organization or their designated services and offer a single-tenant operating environment with all the benefits and functionality of elasticity and accountability/utility model of cloud. The private clouds aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud. There are two variants of private clouds: on-premise private and external hosted private clouds. On-premise private clouds also known as internal clouds are hosted within one's own data center. This model provides a more standardized process and protection, but is limited in aspects of size and scalability. IT departments would also need to incur the capital and operational costs for the physical resources. This is best suited for applications which require complete control and configurability of the infrastructure and security. As the name implies, the externally hosted private clouds are hosted externally with a cloud provider.

Hybrid Cloud:

Hybrid clouds are a combination of public and private cloud offerings that allow for transitive information exchange and possibly application compatibility and portability across disparate cloud service offerings and providers utilizing standard or proprietary methodologies regardless of ownership or location. With a hybrid cloud, service providers can utilize third party cloud providers in a full or partial manner, thereby increasing the flexibility of computing.

The hybrid cloud model is capable of providing on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload. Users and vendor responsibilities are shown in fig.2.

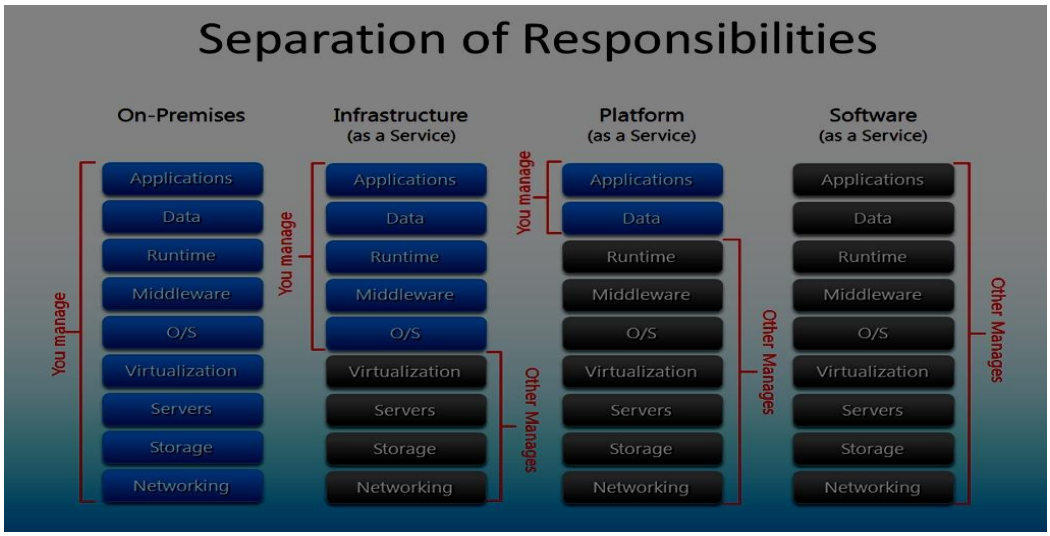


Fig. 2

Generally, SaaS provides a large amount of integrated features built directly into the offering with the least amount of extensibility and

in general a high level of security (or at least a responsibility for security on the part of the service provider).

PaaS offers less integrated features since it is designed to enable developers to build their own applications on top of the platform, and it is therefore, more extensible than SaaS by nature. However, this extensibility features trade-offs on security features and capabilities.

IaaS provides few, if any, application-like features, and provides for enormous extensibility, but generally less security capabilities and functionalities beyond protecting the infrastructure itself, since it expects operating systems, applications and contents to be managed and secured by the customers.

In summary, from a security perspective, in the three service models of cloud computing, the lower down the stack the cloud service provider stops, the more security capabilities and managing the customer are responsible for implementing and managing themselves.

Cloud Computing Security and Privacy Issues:

There are numerous security issues of cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing leads to several security concerns. Mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies, enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure.

One of the more obvious cloud concerns is a separation between a cloud

provider's user (who may be competing companies or even hackers) to avoid inadvertent or intentional access to sensitive information. Typically a cloud provider would use virtual machines (VMs) and a hypervisor to separate customers.

Legal and regulatory issues are extremely important in cloud computing that have security implications. To verify that a cloud provider has strong policies and practices that address legal and regulatory issues, each customer must have its legal and regulatory experts inspect cloud provider's policies and practices to ensure their adequacy. The issues to be considered in this regard include data security and export, compliance, auditing, data retention and destruction, and legal discovery.

The most significant threats to cloud security to identify the top threats for conducting survey of industry experts to compile professional opinion on the greatest security threats within cloud computing. The professional expert finally craft, including the reflection of the industry expert person, mostly industry expert are concerns of the industry identified the following critical threats to cloud security.

- Data Loss
- Data Breaches
- Account Hijacking
- Insecure APIS
- Denial of Service
- Malicious Insiders
- Abuse of Cloud Services
- Insufficient Due Diligence
- Shared Technology Issues

- Data Loss

It is very clear that no one companies are responsible for the security of cloud data different companies are already clear statements are following.

Google Docs. You expressly understand and agree that google, its subsidiaries and affiliates, and its licensors shall not be liable to you for:

- Any direct, indirect, incidental, special, consequential or exemplary damages which may be incurred by you, however caused and under any theory of liability. This shall include, but not be limited to any loss of profit (whether incurred directly or indirectly) any loss of goodwill or business reputation, any loss of data suffered, cost of procurement of substitute goods or services, or other intangible loss.
- Any loss or damage which may be incurred by you, including but not limited to loss or damage as a result of.
- The deletion of, corruption of, or failure to store, any content and other communications data maintained or transmitted by or through your use of the services the limitations on Google's liability to you in paragraph 15.1 above shall apply whether or not Google has been advised of or should have been aware of the possibility of any such losses arising.

Amazon Cloud Drive

We do not guarantee that Your Files will not be subject to misappropriation, loss or damage and we will not be liable if they are. You're responsible for maintaining appropriate security, protection and backup of Your Files.

Microsoft SkyDrive

You’re responsible for backing up the data that you store on the service. If your service is suspended or canceled, we may permanently delete your data from our servers. We have no obligation to return data to you after the service is suspended or canceled. If data are stored with an expiration date, we may also delete the data as of that date. Data that is deleted may be irretrievable.

- Data Breaches

Security and privacy issues over cloud computing are not very different from those surrounding any sort of IT outsourcing and need to be treated that way, security managers and analysts say in the wake of breaches involving.

Unfortunately, while data loss and data leakage are both serious threats to cloud computing, the measures put in place to mitigate one of these threats can exacerbate the other," the report said. Encryption protects data at rest, but lose the encryption key lost the data. The cloud routinely makes copies of data to prevent its loss due to an unexpected die off of a server. The more copies, the more exposure you have to breaches.

Of the 761 data breaches investigated in 2010 by the U.S. Secret Service and Verizon Communications Inc.'s forensics analysis unit, 63% occurred at companies with 100 or fewer employees. And a 2011 survey by security systems provider Symantec Corp. Of more than 2,000 small and mid-size enterprises indicated that 73% had been breached by a cyber-attack, with the average annual cost per organization pegged at $188,242.

- Account Hijacking

Account hijacking sounds too elementary to be a concern in the cloud. Phishing, exploitation of software vulnerabilities such as buffer overflow attacks, and loss of passwords and credentials can all lead to the loss of control over a user account. An intruder with control over a user account can eavesdrop on transactions, manipulate data, provide false and business-damaging responses to customers, and redirect customers to a competitor's site or inappropriate sites.

The alliance offers tips on how to practice defense in depth against such hijackings, but the must-do points are to prohibit the sharing of account credentials between users, including trusted business partners; and to implement strong two-factor authentication techniques "where possible."

- Insecure APIs

In the most recent iteration of the Cloud Security Alliance's (CSA) Top Threats to Cloud Computing report, a number of new risks were presented, while older risks were modified and prioritized. Dubbed The Notorious Nine: Cloud Computing Top Threats in 2013, the report is based on feedback from the cloud computing and security communities.

The cloud era has brought about the contradiction of trying to make services available to millions while limiting any damage all these largely anonymous users might do with the service. The answer has been a public facing application programming interface, or API, that defines how a third party connects an application to the service and providing verification that the third party producing the application is Leading web developers, including ones from Twitter and Google, collaborated on specifying OAuth, an open authorization service for web services that controls third party access. OAuth became an Internet

Engineering Task Force standard in 2010 and Version 2.0 is used for at least some services by

- Denial of Service

There are two types of threats, i.e. Extortionists-Using DDoS attack to exhaust server resources and Competitors-Using known vulnerabilities to interrupt services. When the flood of messages attacks all nodes of different node system at the same time it is known as Distributed Denial of Service (DDoS). Complex and Simple types of DDos attack tools we have, Agobot, Mstream and Trinoo are in complex categories and X-Dos (XML based Denial of service) as well as H-Dos (HTTP based Denial of service) are in simple categories. (Extensible Markup Language)-based Denial of Service (X-DoS) and (Hypertext Transfer Protocol)- based Denial of Service (H-DoS) are used by most attacker as they inclined to use less complicated web based attack tools because of their simple implementation and short of real defences against them. X-DoS with DX-DoS(distributed XML based Denial of Service), it distributed version occurs when message of XML types is sent to a web server with or without wicked content by using their all resources. Coercive Parsing attack is an example of an X-Dos attack in this web Service request is manipulated when content is parsed by SOAP(Simple Object Access Protocol) to transform it into accessible form to the application. A continuous series of open tags are used by Coercive Parsing attack to make CPU usage exhausted on an Axis2 web server. Some 1500 threads are starts up by HTTP Flooder to make HTTP randomized requests to victim web server to make communication channels exhaust in the H-Dos attack. So the point is made that there is no way to filter such traffic and to differentiate between HTTP request that are legitimate and illegitimate.

- Malicious Insiders

Disgruntled Employee

This is usually the employee who feels personally disrespected, possibly due to a missed pay raise that was expected or a negative encounter with supervisors over benefits, time off, demotions, transfers or other similar issues. In this instance, revenge is the employee's motive.

- Profit-seeking employee - This is a simple motivation for many people. They work for a wage; however, by stealing information, they can make more money selling the stolen data to organized criminals or modifying the data to steal an identity.

- An employee moving to a competitor or starting a business - For someone starting a business in the same field, the theft of customer lists, business plans, and even simple forms or templates can be tempting.

- Believe they own the code or product - In this case, employees feel a sense of ownership over code they wrote or a product they developed. Therefore, they take the code for their future use or even for their next job.

- Abuse of Cloud Services:

Infrastructure as a Service (IaaS) providers offer their customers the illusion of unlimited compute, network, and storage capacity often coupled with a 'frictionless' registration process where anyone with a valid credit card can register and immediately begin using cloud services.

- Insufficient Due Diligence

"Due diligence" is an investigation of a business or person prior to signing a contract, or an act with a certain standard of care. It can be a legal obligation, but the term will more commonly apply to voluntary

investigations.

- Shared Technology Issues

Infrastructure as a Service (IaaS) vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure (e.g., CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multi-tenant architecture.

3 Methodology:

- Minimize Lack of Trust
  - Policy Language
  - Certification
- Minimize Loss of Control
  - Monitoring
  - Utilizing different clouds
  - Access control management
  - Identity Management (IDM)
- Minimize Multi-tenancy

Security Issues in the Cloud

- In theory, minimizing any of the issues would help:
  - Third Party Cloud Computing
  - Loss of Control
    - Take back control
      - Data and apps may still need to be on the cloud

        - But can they be managed in some way by the consumer?
    - Lack of trust
        - Increase trust (mechanisms)
            - Technology
            - Policy, regulation
            - Contracts (incentives): topic of a future talk
    - Multi-tenancy
        - Private cloud
            - Takes away the reasons to use a cloud in the first place
        - VPC: it's still not a separate system
        - Strong separation

Third Party Cloud Computing

- Like Amazon's EC2, Microsoft's Azure
    - Allow users to instantiate Virtual Machines
    - Allow users to purchase required quantity when required
    - Allow service providers to maximize the utilization of sunk capital costs
    - Confidentiality is very important
- Known issues: Already exist
    - Confidentiality issues
    - Malicious behavior by cloud provider
    - Known risks exist in any industry practicing outsourcing

- Provider and its infrastructure needs to be trusted

- New Vulnerabilities & Attacks
  - Threats arise from other consumers
  - Due to the subtleties of how physical resources can be transparently shared between VMs
  - Such attacks are based on placement and extraction
  - A customer VM and its adversary can be assigned to the same physical server
  - Adversary can penetrate the VM and violate customer confidentiality
  - Collaborative attacks

Minimize Lack of Trust

- Policy Language
- Certification

Policy Language

- Consumers have specific security needs but don't have a say-so in how they are handled
- Standard language to convey one's policies and expectations.
- Create policy language with the following characteristics:
  - Machine-understandable (or at least processable)
  - Easy to combine/merge and compare
  - Examples of policy statements are, "requires isolation between VMs", "requires geographical isolation between VMs", "requires physical separation between other communities/tenants that are in the same industry," etc.

- Need a validation tool to check that the policy created in the standard language correctly reflects the policy creator's intentions (i.e. that the policy language is semantically equivalent to the user's intentions).

Certification

- Some form of reputable, independent, comparable assessment and description of security features and assurance.
- Sarbanes-Oxley, DIACAP, DISTCAP, etc. (are they sufficient for a cloud environment?).

• Risk Assessment

- Performed by certified third parties.
- Provides consumers with additional assurance.

Minimize Loss of Control

- Monitoring
- Utilizing Different Clouds
- Access Control Management
- Identity Management (Idm)

Minimize Loss of Control: Utilize Different Clouds

- The concept of 'Don't put all your eggs in one basket'
  - Consumer may use services from different clouds through an intra-cloud or multi-cloud architecture.
  - Propose a multi-cloud or intra-cloud architecture in which consumers.

- Spread the risk.
- Increase redundancy (per-task or per-application).
- Increase chance of mission completion for critical applications.

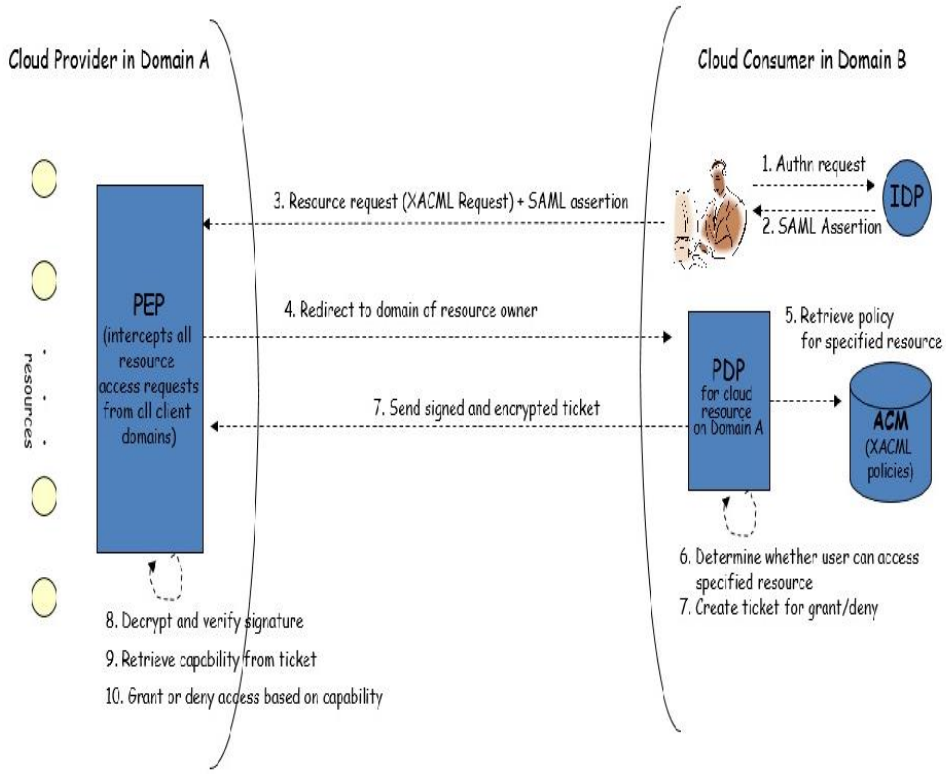
- Possible issues to consider:
  - Policy incompatibility (combined, what is the overarching policy?).
  - Data dependency between clouds.
  - Differing data semantics across clouds.
  - Knowing when to utilize the redundancy feature (monitoring technology).
  - Is it worth it to spread your sensitive data across multiple clouds?
  - Redundancy could increase risk of exposure.

Minimize Loss of Control: Access Control

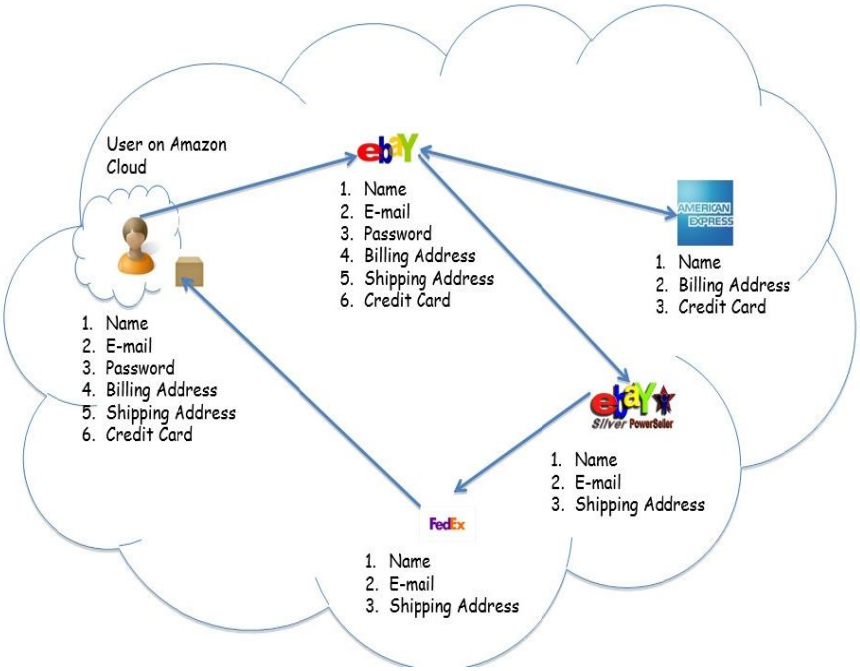
- Regardless of deployment model, provider needs to manage the user authentication and access control procedures to the cloud.
  - Federated Identity Management: access control management burden still lies with the provider.
  - Requires user to place a large amount of trust on the provider in terms of security, management, and maintenance of access control policies. This can be burdensome when numerous users from different organizations with different access control policies, are involved.

- Consumer-managed access control
  - Consumer retains decision-making process to retain some control, requiring less trust of the provider (i.e. PDP is in consumer's domain).
  - Requires the client and provider to have a pre-existing trust relationship, as well as a pre-negotiated standard way of describing resources, users, and access decisions between the cloud provider and consumer. It also needs to be able to guarantee that the provider will uphold the consumer-side's access decisions.
  - Should be at least as secure as the traditional access control model.
  - Facebook and Google Apps do this to some degree, but not enough control.
  - Applicability to privacy of patient health records.

Minimize Loss of Control: Access Control


Cloud Provider in Domain A
Cloud Consumer in Domain B
resources
PEP
(intercepts all resource access requests from all client domains)
3. Resource request (XACML Request) + SAML assertion
1. Authn request
IDP
2. SAML Assertion
4. Redirect to domain of resource owner
5. Retrieve policy for specified resource
PDP
for cloud resource on Domain A
ACM
(XACML policies)
7. Send signed and encrypted ticket
6. Determine whether user can access specified resource
7. Create ticket for grant/deny
8. Decrypt and verify signature
9. Retrieve capability from ticket
10. Grant or deny access based on capability

Minimize Loss of Control: IDM Motivation



Minimize Loss of Control: IDM Identity in the Cloud

Minimize Loss of Control: IDM Present IDMs

- IDM in traditional application-centric IDM model
    - Each application keeps track of identifying information of its users.
- Existing IDM Systems
    - Microsoft Windows CardSpace [W. A. Alrodhan].
    - OpenID [http://openid.net].
    - PRIME [S. F. Hubner].

These systems require a trusted third party and do not work on an untrusted host.

If Trusted Third Party is compromised, all the identifying information of the users is also compromised.

Results and Discussion:

Minimize Loss of Control: IDM Issues in Cloud Computing

- Cloud introduces several issues to IDM
    - Users have multiple accounts associated with multiple service providers.
    - Lack of trust.
        - Use of Trusted Third Party is not an option.
        - Cloud hosts are untrusted.
    - Loss of control.
        - Collusion between Cloud Services
            - Sharing sensitive identity information between services can lead to undesirable mapping of the identities to the user.

Minimize Loss of Control: IDM Goals of Proposed User-Centric IDM for the Cloud

- Authenticate without disclosing identifying information.
- Ability to securely use a service while on an untrusted host (VM on the cloud).
- Minimal disclosure and minimized risk of disclosure during communication between user and service provider (Man in the Middle, Side Channel and Correlation Attacks).
- Independence of Trusted Third Party

Minimize Loss of Control: IDM Approach - 1

- IDM Wallet:
  - Use of AB scheme to protect PII from untrusted hosts.
- Anonymous Identification:
  - Use of Zero-knowledge proofing for authentication of an entity without disclosing its identifier.

Minimize Loss of Control: IDM Components of Active Bundle (Approach - 1)

- Identity data: Data used during authentication, getting service, using service (i.e. SSN, Date of Birth).
- Disclosure policy: A set of rules for choosing Identity data from a set of identities in IDM Wallet.
- Disclosure history: Used for logging and auditing purposes.
- Negotiation policy: This is Anonymous Identification, based on the Zero Knowledge Proofing.
- Virtual Machine: Code for protecting data on untrusted hosts. It

enforces the disclosure policies.

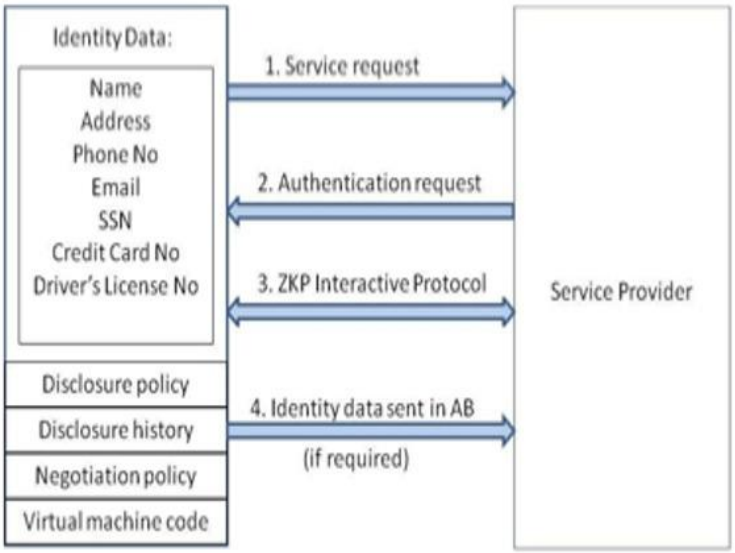
Minimize Loss of Control: IDM Anonymous Identification (Approach - 1)

Anonymous Identification

(Shamir's approach for Credit Cards)

- IDP provides Encrypted Identity Information to the user and SP.
- SP and User interact.
- Both run IDP's public function on the certain bits of the Encrypted data.
- Both exchange results and agree if it matches.

Minimize Loss of Control: IDM Usage Scenario (Approach - 1)



Minimize Loss of Control: IDM Approach - 2

- Active Bundle scheme to protect PII from untrusted hosts.
- Predicates over encrypted data to authenticate without disclosing unencrypted identity data.
- Multi-party computing to be independent of a trusted third party.

Minimize Loss of Control: IDM Usage Scenario (Approach - 2)

- Owner O encrypts Identity Data(PII) using algorithm Encrypt and O's public key PK. Encrypt outputs CT—the encrypted PII.
- SP transforms his request for PII to a predicate represented by function p.
- SP sends shares of p to the n parties who hold the shares of MSK.
- n parties execute together KeyGen using PK, MSK, and p, and return TKp to SP.
- SP calls the algorithm Query that takes as input PK, CT, TKp and produces p(PII) which is the evaluation of the predicate.
- The owner O is allowed to use the service only when the predicate evaluates to "true".

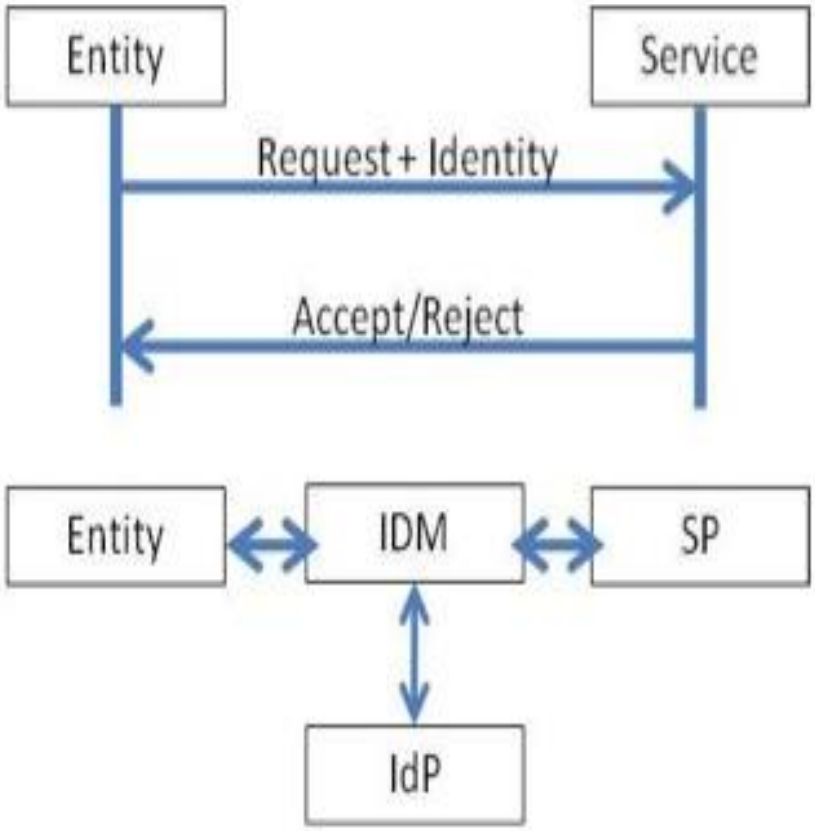
Minimize Loss of Control: IDM Representation of identity information for negotiation

Token/Pseudonym

Identity Information in clear plain text

Active Bundle

Minimize Loss of Control: IDM Motivation-Authentication Process using PII



Problem: Which information to disclose and how to disclose it.

Proposed IDM: Mechanisms

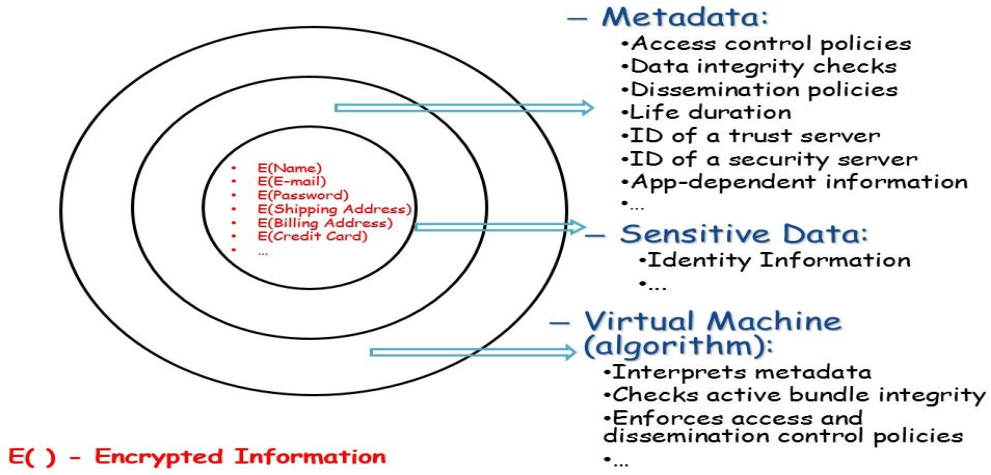
- Active Bundle
- Anonymous Identification
- Computing Predicates with encrypted data
- Multi-Party Computing

- Selective Disclosure

Proposed IDM: Active Bundle

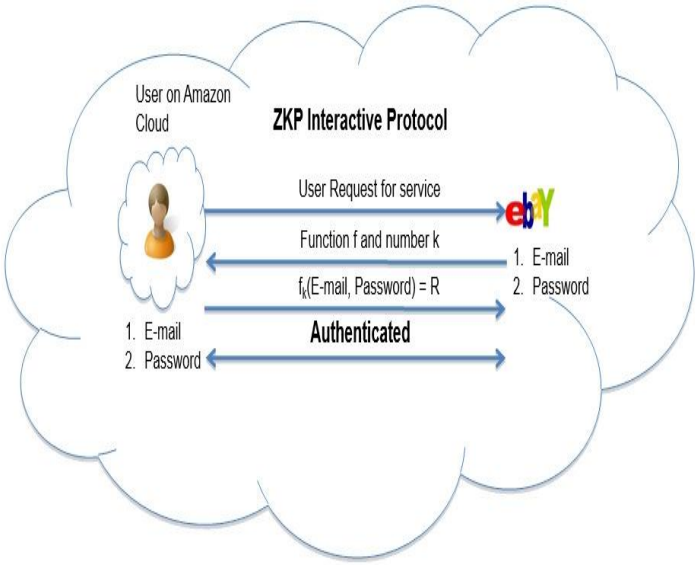
- Active bundle (AB)
    - An encapsulating mechanism protecting data carried within it.
    - Includes metadata used for managing confidentiality.
        - Both privacy of data and privacy of the whole AB
    - Includes Virtual Machine (VM).
        - performing a set of operations
        - protecting its confidentiality
- Active Bundles—Operations
    - Self-Integrity check

Proposed IDM: Active Bundle Scheme

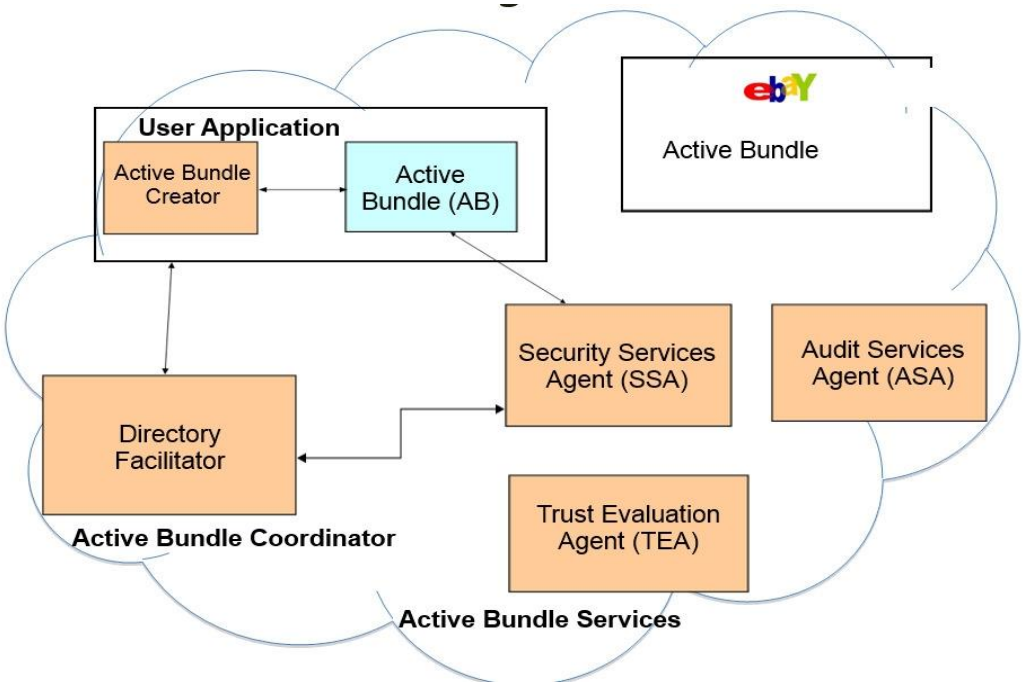


Proposed IDM: Anonymous Identification

- Use of Zero-knowledge proofing for user authentication without disclosing its identity.

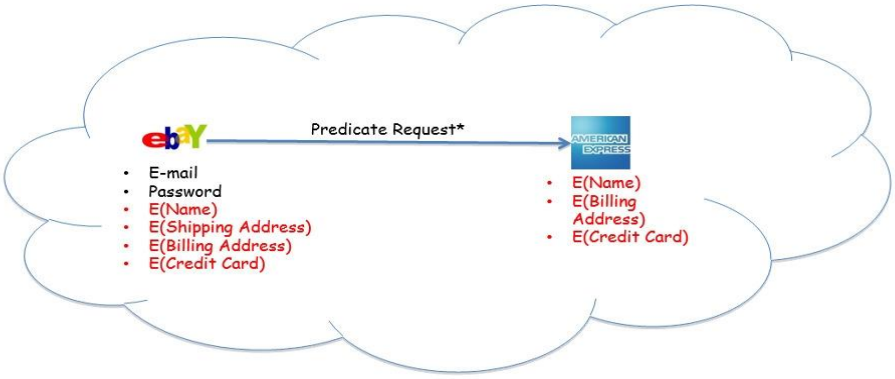


Proposed IDM: Interaction using Active Bundle



Proposed IDM: Predicate over Encrypted Data

- Verification without disclosing unencrypted identity data.

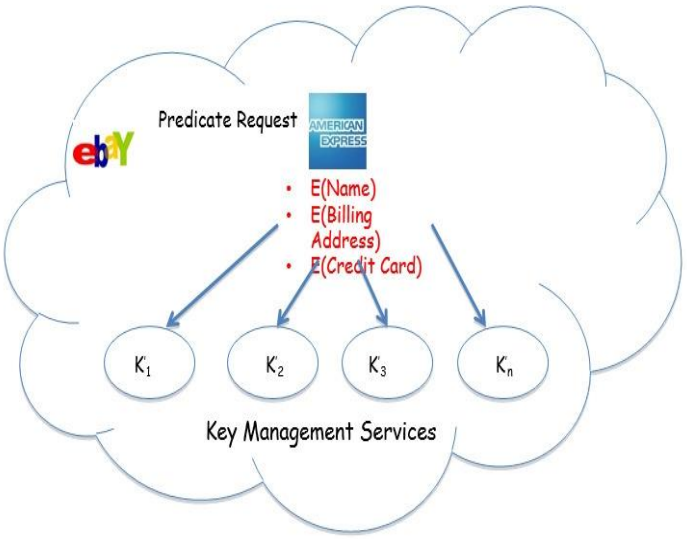


*Age Verification Request

*Credit Card Verification Request

Proposed IDM: Multi-Party Computing

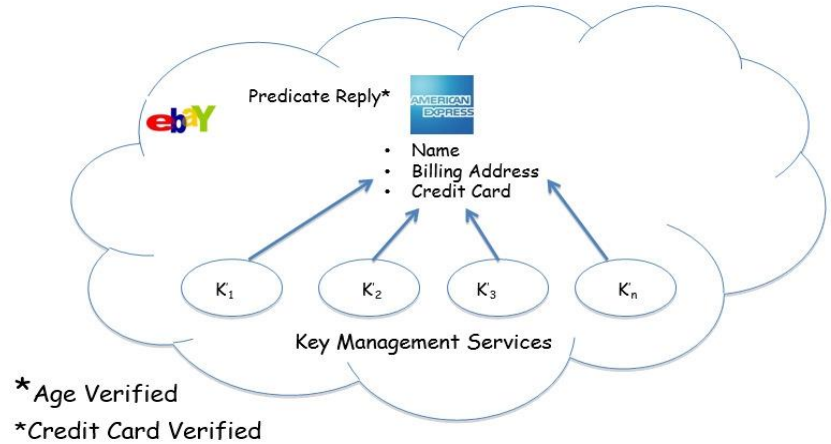
- To become independent of a trusted third party
    - Multiple Services hold shares of the secret key
    - Minimize the risk



* Decryption of information is handled by the Key Management services

Proposed IDM: Multi-Party Computing

- To become independent of a trusted third party
    - Multiple Services hold shares of the secret key
    - Minimize the risk

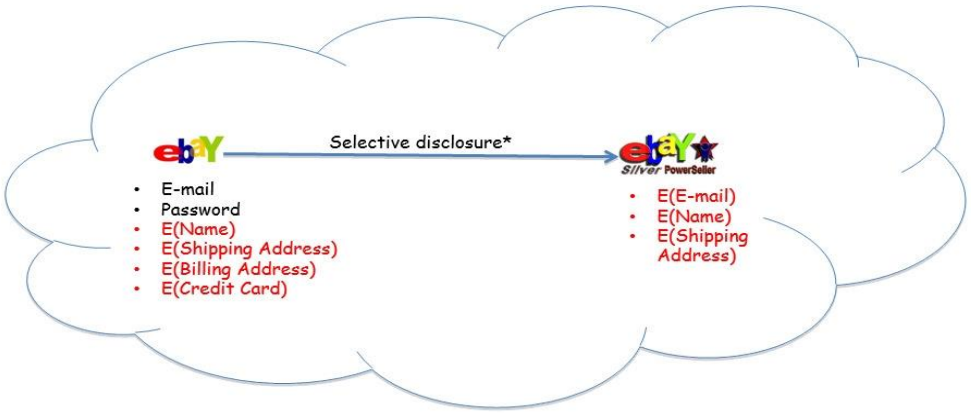


*Age Verified

*Credit Card Verified

Proposed IDM: Selective Disclosure

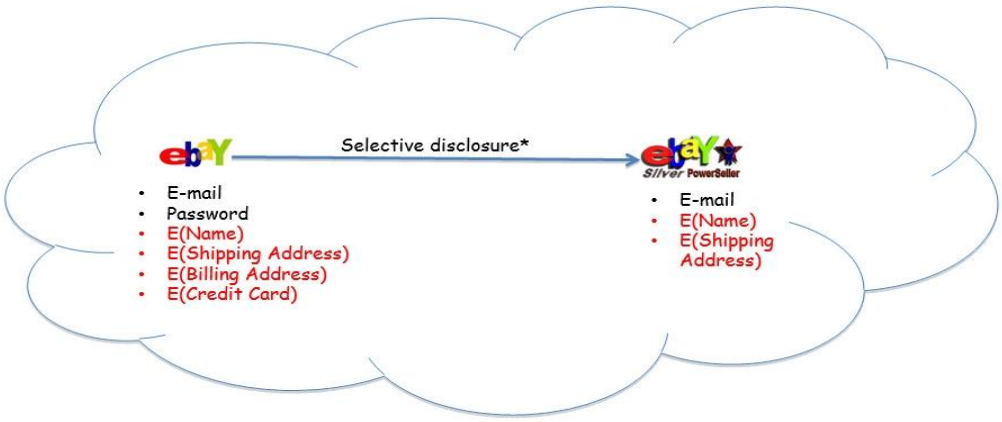
- User Policies in the Active Bundle dictate dissemination.



*e-bay shares the encrypted information based on the user policy

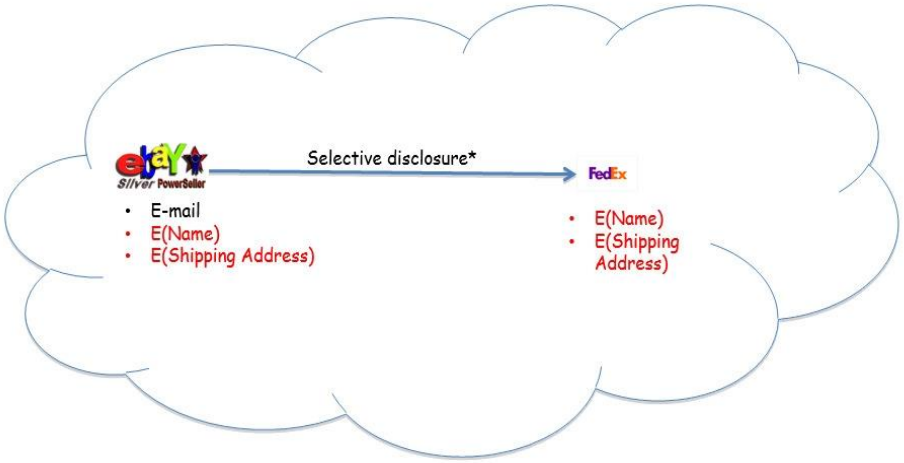
Proposed IDM: Selective Disclosure

- User Policies in the Active Bundle dictate dissemination



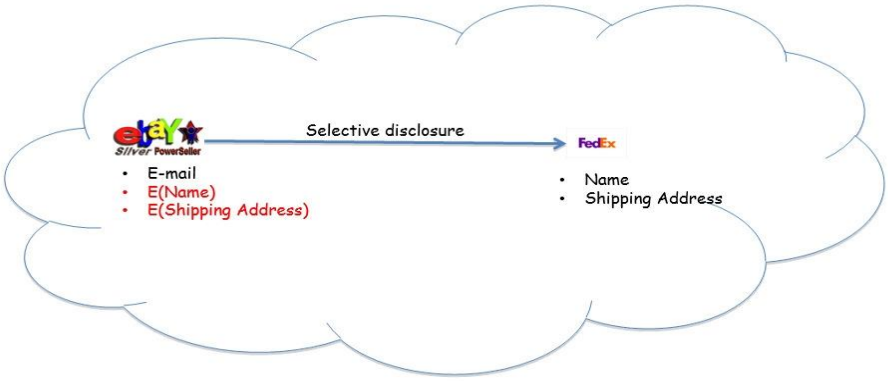
Decryption handled by Multi-Party Computing as in the previous slides

Proposed IDM: Selective Disclosure



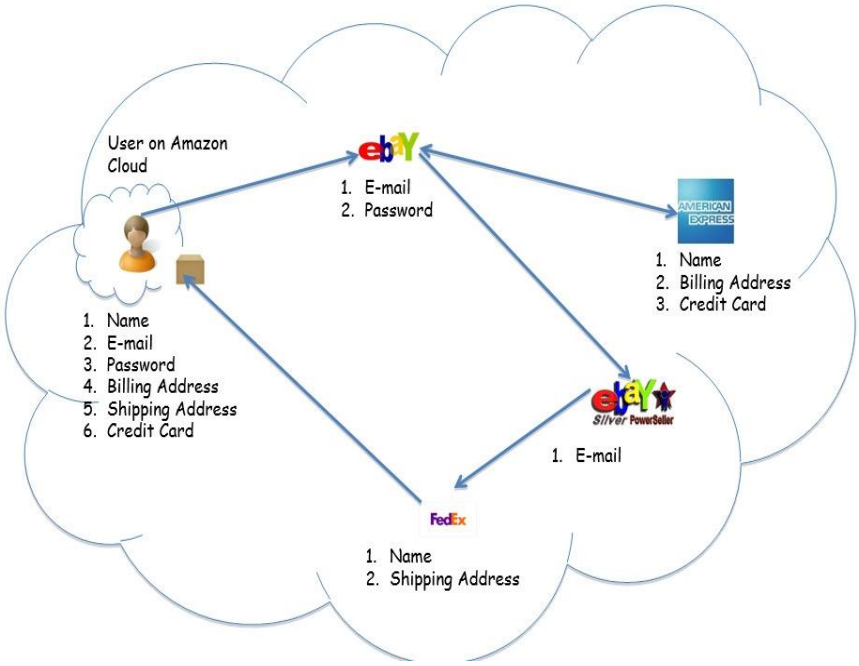
*e-bay seller shares the encrypted information based on the user policy

Proposed IDM: Selective Disclosure



- Decryption handled by Multi-Party Computing as in the previous slides

Proposed IDM: Identity in the Cloud



Proposed IDM: Characteristics and Advantages

- Ability to use Identity data on untrusted hosts
    - Self-Integrity Check, Integrity compromised- apoptosis or evaporation and Data should not be on this host.
- Independent of Third Party.
    - Prevents correlation attacks.
- Establishes the trust of users in IDM.
    - Through putting the user in control of who has his data.
    - Identity is being used in the process of authentication, negotiation, and data exchange.
- Minimal disclosure to the SP.
    - SP receives only necessary information.

Proposed IDM: Conclusion & Future Work

- Problems with IDM in Cloud Computing.
    - Collusion of Identity Information, prohibited untrusted Hosts and usage of Trusted Third Party.
- Proposed Approaches
    - IDM based on Anonymous Identification and Predicate over Encrypted data.
- Future work
    - Develop the prototype, conduct experiments and evaluate the approach.

4 Conclusion

Today, cloud computing is being defined and talked about across the industry under different contexts and with different definitions attached to it. The core point is that cloud computing means having a server firm that can host the services for users connected to it by the network. Technology has moved in this direction because of the advancement in computing, communication and networking technologies. Fast and reliable connectivity is a must for the existence of cloud computing. At least in part to its cost-efficiency and flexibility. However, despite the surge in activity and interest, there are significant, persistent concerns about cloud computing that are impeding the momentum and will eventually compromise the vision of cloud computing as a new information Technology (IT) procurement model. Despite the trumpeted business and technical advantages of cloud computing, many potential cloud users have yet to join the cloud, and those major corporations that are cloud users are for the most part putting only their less sensitive data in the cloud. Lack of control is transparency in the cloud implementation - somewhat contrary to the original promise of cloud computing in which cloud implementation is not relevant. Transparency is needed for regulatory reasons and to ease concern over the potential for data breaches. Because of today's perceived lack of control, larger companies are testing the waters with smaller projects and less sensitive data. In short, the potential of the cloud is not yet being realized.

References

[1]. Alliance for Telecommunications Industry Solutions. Homepage URL: http://www.atis.org.

[2]. Amazon S3 Availability Event: (2008). URL: http://status.aws.amazon.com/s3-20080720.html (Accessed on November 29, 2012).

[3]. AOL Apologizes for Release of User Search Data (2006). URL: news.cnet.com/2010-1030_3-6102793.html. August 7, 2006.

[4]. http://www.businessinsurance.com/article/99999999/NEWS070101/399999805#.

[5]. http://www.digitaltrends.com/computing/upload-at-your-own-risk-most-cloud-storage-services-offer-no-data-guarantee./

[6]. http://www.informationweek.com/cloud/infrastructure-as-a-service/9-worst-cloud-security-threats/d/d-id/1114085.

[7]. CSA, April 2009. Available Online at: https://cloudsecurityalliance.org/csaguide.pdf (Accessedon: November 29, 2012).

[8]. Distributed Management Task Force. Homepage URL: http://www.dmtf.org.

[9]. Don't Cloud Your Vision. URL: http://www.ft.com/cms/s/0/303680a6-bf51-11dd-ae63-0000779fd18c.html?nclick_check=1. (Accessed on: November 29, 2012).

[10]. European Network and Information Security Agency (ENISA) (2009). Cloud Computing: Cloud Computing: Benefits, Risks and recommendations for Information Security. Report No: 2009.

[11]. Sen, J. (2010f). A Trust-Based Robust and Efficient Searching Scheme for Peer-to-Peer Networks. In Proceedings of the 12th International Conference on Information and Communication Security (ICICS), pp. 77-91, December 2010, Barcelona, Spain, Springer LNCS Vol 6476.

[12]. Song, D., Wagner, D., &Perrig, A. (2000). Practical Techniques for Searches on Encrypted Data. In Proceedings of the IEEE Symposium on Research in Security and Privacy, Oakland, California, USA, pp. 44-55, May 2000.

[13]. Storage Networking Industry Association. Homepage URL: http://www.snia.org.Takabi, H., Joshi, J. B. D., &Ahn, G.-J. (2010). Security and Privacy Challenges in Cloud Computing Environments. IEEE Security and Privacy, Vol 8, No 6, pp. 24-31, November-December 2010.

[15]. TM Forum. Homepage URL: http://www.tmforum.org.

[16]. Trusted Computing Group (TCG)'s White Paper (2010). Cloud Computing and Security- A Natural Match. Available online at: http://www.trustedcomputinggroup.org (Accessed on; November 2012).

[17]. Xen Vulnerability. URL: http://secunia.com/advisories/26986/. (Accessed on: November 20, 2012).

[18]. Zetter, K. (2010). Google hackers Targeted Source Code of More Than 30 Companies. Wired Threat Level. January 13 2010. Available online at:

http://www.wired.com/threatlevel/2010/01/google-hackattack/(Accessed on: November 29, 2012).

[19]. http://www.digitaltrends.com/computing/upload-at-your-own-risk-most-cloud-storage-services-offer-no-data-guarantee/#ixzz3.