Cloud Computing and Data Security

BASICS OF CLOUD COMPUTING AND DATA SECURITY

@MOHAMMED FAZULUDDIN

Topics

- Overview of Cloud Computing
- Cloud Computing Providers
- Cloud Computing Deployment Models
- Cloud Computing Models
- Cloud Computing Sub-services Models
- Cloud Data Security

Overview of Cloud Computing

- Cloud computing provides the ability to scale to tens of thousands of systems, as well as the ability to massively scale bandwidth and storage space.
- Cloud computing might be confused with distributed system, grid computing, utility computing, service oriented architecture, web application, web 2.0, broadband network, browser as a platform, Virtualization and free/open software.
- Cloud computing is a natural evolution of the widespread adoption of virtualization, service-oriented architecture, autonomic and utility computing.
- Cloud services exhibit five essential characteristics that demonstrate their relation to, and differences from, traditional computing approaches such as on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.
- Cloud computing often leverages massive scale, homogeneity, virtualization, resilient computing (no stop computing), low cost/free software, geographic distribution, service orientation software and advanced security technologies.

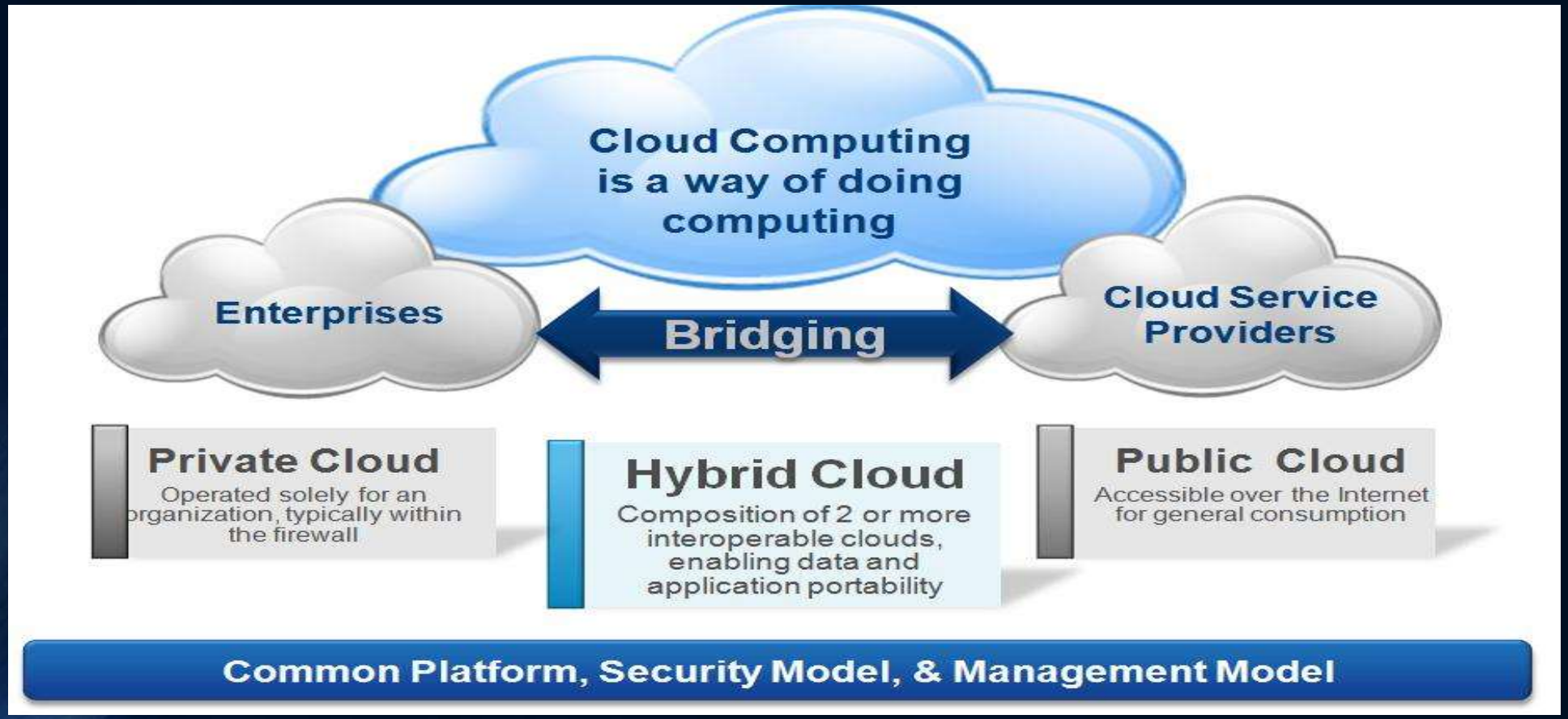
Overview of Cloud Computing

- Lower computer costs, improved performance, reduced software costs, instant software updates, improved document format compatibility, unlimited storage capacity, device independence, and increased data reliability.
- Cloud computing is based on five attributes…
  - Multi-tenancy (shared resources).
  - Massive scalability.
  - Elasticity.
  - Pay as you go .
  - Self-provisioning of resources.
- It makes new improvements in processors, Virtualization technology, disk storage, broadband Internet connection, and combined fast, inexpensive servers to make the cloud to be a more compelling solution.

Overview of Cloud Computing

- **Multi-tenancy (shared resources):** Cloud computing is based on a business model in which resources are shared (i.e., multiple users use the same resource) at the network level, host level and application level.
- **Multi-tenancy (shared resources):** Cloud computing is based on a business model in which resources are shared (i.e., multiple users use the same resource) at the network level, host level and application level.
- **Massive scalability:** Cloud computing provides the ability to scale to tens of thousands of systems, as well as the ability to massively scale bandwidth and storage space.
- **Elasticity:** Users can rapidly increase and decrease their computing resources as needed; Pay as you used: Users to pay for only the resources they actually use and for only the time they require them.
- **Self-provisioning of resources:** Users' self-provision resources, such as additional systems (processing capability, software, storage) and network resources.

Overview of Cloud Computing



Cloud Computing Providers

- Following are the list of cloud computing providers…
  - AWS (amazon web services)—include Amazon S3, Amazon EC2, Amazon Simple-DB, Amazon SQS, Amazon FPS, and others.
  - Salesforce.com—Delivers businesses over the internet using the software as a service model.
  - Google Apps—Software-as-a-service for business email, information sharing and security.
  - And others providers such as
    - Microsoft Azure Services Platform
    - Proof-point
    - Sun Open Cloud Platform
    - Workday, etc..

Cloud Computing Deployment Models

- Private cloud :
  - This model doesn't bring much in terms of cost efficiency, it is comparable to buying, building and managing your own infrastructure.
  - It brings in tremendous value from a security point of view.
  - Security concerns are addressed through secure-access VPN or by the physical location within the client's firewall system.
- Community cloud:
  - In the community deployment model, the cloud infrastructure is shared by several organizations with the same policy and compliance considerations.
  - This helps to further reduce costs as compared to a private cloud, as it is shared by larger group.

Cloud Computing Deployment Models

- Public cloud:
  - The public cloud deployment model represents true cloud hosting.
  - In this deployment model, services and infrastructure are provided to various clients, google is an example of a public cloud.
  - This service can be provided by a vendor free of charge or on the basis of a pay-per-user license policy.
- Hybrid cloud:
  - This deployment model helps businesses to take advantage of secured applications and data hosting on a private cloud, while still enjoying cost benefits by keeping shared data and applications on the public cloud.
  - This model is also used for handling cloud bursting, which refers to a scenario where the existing private cloud infrastructure is not able to handle load spikes and requires a fallback option to support the load.

Cloud Computing Models

- Cloud SaaS (software as a service):
  - Application and information clouds.
  - Use provider's applications over a network, cloud provider examples Zoho, Salesforce.com, and Google Apps.
- Cloud PaaS (platform as a service):
  - Development clouds.
  - Deploy customer-created applications to a cloud, cloud provider examples Windows Azure, Google App Engine and Aptana Cloud.
- Cloud IaaS (infrastructure as a service):
  - Infrastructure clouds.
  - Rent processing, storage.
  - network capacity.
  - Other fundamental computing resources like Dropbox, Amazon Web Services, Mozy and Akamai.

Cloud Computing Sub-services Models

- IaaS: DBaaS (database-as-a-service): DBaaS allows the access and use of a database management system as a service.
- PaaS: STaaS (storage-as-a-service): STaaS involves the delivery of data storage as a service, including database-like services, often billed on a utility computing basis, e.g., per gigabyte per month.
- SaaS: CaaS (communications-as-a-service): CaaS is the delivery of an enterprise communications solution, such as Voice over IP, instant messaging, and video conferencing applications as a service.
- SaaS: SECaaS (security-as-a-service): SECaaS is the security of business networks and mobile networks through the Internet for events, database, application, transaction, and system incidents.

Cloud Computing Sub-services Models

- SaaS: MaaS (monitoring-as-a-service): MaaS refers to the delivery of second-tier infrastructure components, such as log management and asset tracking, as a service.
- PaaS: DTaaS (desktop-as-a-service): DTaaS is the decoupling of a user's physical machine from the desktop and software he or she uses to work.
- IaaS: CCaaS (compute capacity-as-a-service): CCaaS is the provision of "raw" computing resource, typically used in the execution of mathematically complex models from either a single "supercomputer" resource or a large number of distributed computing resources where the task performs well .

Cloud Data Security

- Cloud computing, all your data is stored on the cloud, so cloud users ask some questions like: How secure is the cloud? Can unauthorized users gain access to your confidential data?.
- Cloud computing companies say that data is secure, but it is too early to be completely sure of that. Only time will tell if your data is secure in the cloud.
- Cloud security concerns arising which both customer data and program are residing in provider premises.
- While cost and ease of use are two great benefits of cloud computing, there are significant security concerns that need to be addressed when considering moving critical applications and sensitive data to public and shared cloud environments.

Cloud Data Security

- To address these concerns, the cloud provider must develop sufficient controls to provide the same or a greater.
- level of security than the organization would have if the cloud were not used.
- There are three types of data in cloud computing
  - Data in transit (transmission data)
  - Data at rest (storage data)
  - Data in processing (processing data).
- Clouds are massively complex systems can be reduced to simple primitives that are replicated thousands of times and common functional units.
- These complexities create many issues related to security as well as all aspects of Cloud computing.

Cloud Data Security

- Security of data and trust problem has always been a primary and challenging issue in cloud computing.
- focuses on enhancing security by using…
  - OTP authentication system.
  - Check data integrity by using hashing algorithms.
  - Encrypt data automatically with the highest strong/ fast encryption algorithm and finally ensure the fast recovery of data.
- Most cloud computing providers..
  - Authenticates (e.g., Transfer usernames and password) via secure connections and secondly,
  - Transfer (e.g., via HTTPS) data securely to/from their servers (so-called "data in transit encrypts stored data (so-called "data at rest") automatically.
- The authorization, the process of granting access to requested resources, is pointless without suitable authentication.

Cloud Data Security

- In cloud computing, to ensure correctness of user data, in first, user must be make authentication.
- Authentication is the process of validating or confirming that access credentials provided by a user (for instance, a user ID and password) are valid.
- When organizations begin to utilize applications in the cloud, authenticating users in a trustworthy and manageable manner becomes an additional challenge.
- Organizations must address authentication-related challenges such as credential management, strong authentication, delegated authentication, and trust across all types of cloud delivery models (SPI).

Cloud Data Security

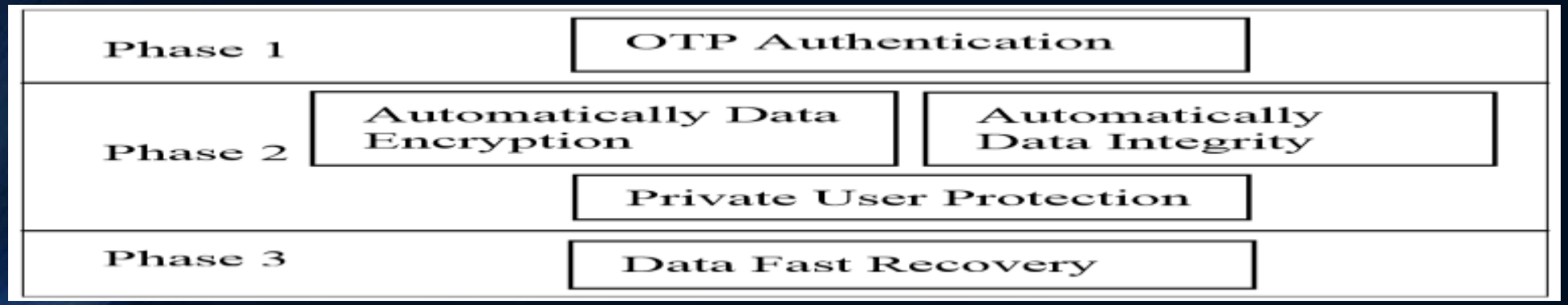
- data security model must ensure…
  - Data must be encrypted automatically
  - Use a strong encryption algorithm.
  - Use the strong encryption algorithm that must be fast to retrieve data faster.
  - Use strong authentication.
  - Ensure file integrity.
- Amazon web services encourage user's to encrypt sensitive data by using TrueCrypt software.
- TrueCrypt is an outstanding encryption solution for anyone familiar with managing volumes and a slight knowledge of encryption technology.

Cloud Data Security

- Any organization planning to deploy TrueCrypt as a cloud-data protection solution must consider the cost and logistics of training and supporting users, managing versions, and recovering damages.
- TrueCrypt is a computer software program whose primary purposes are to…
  - Secure data by encrypting it before it is written to a disk.
  - Decrypt encrypted data after it is read from the disk.
- TrueCrypt uses only three methods (AES, Serpent and Twofish) to encrypt data.

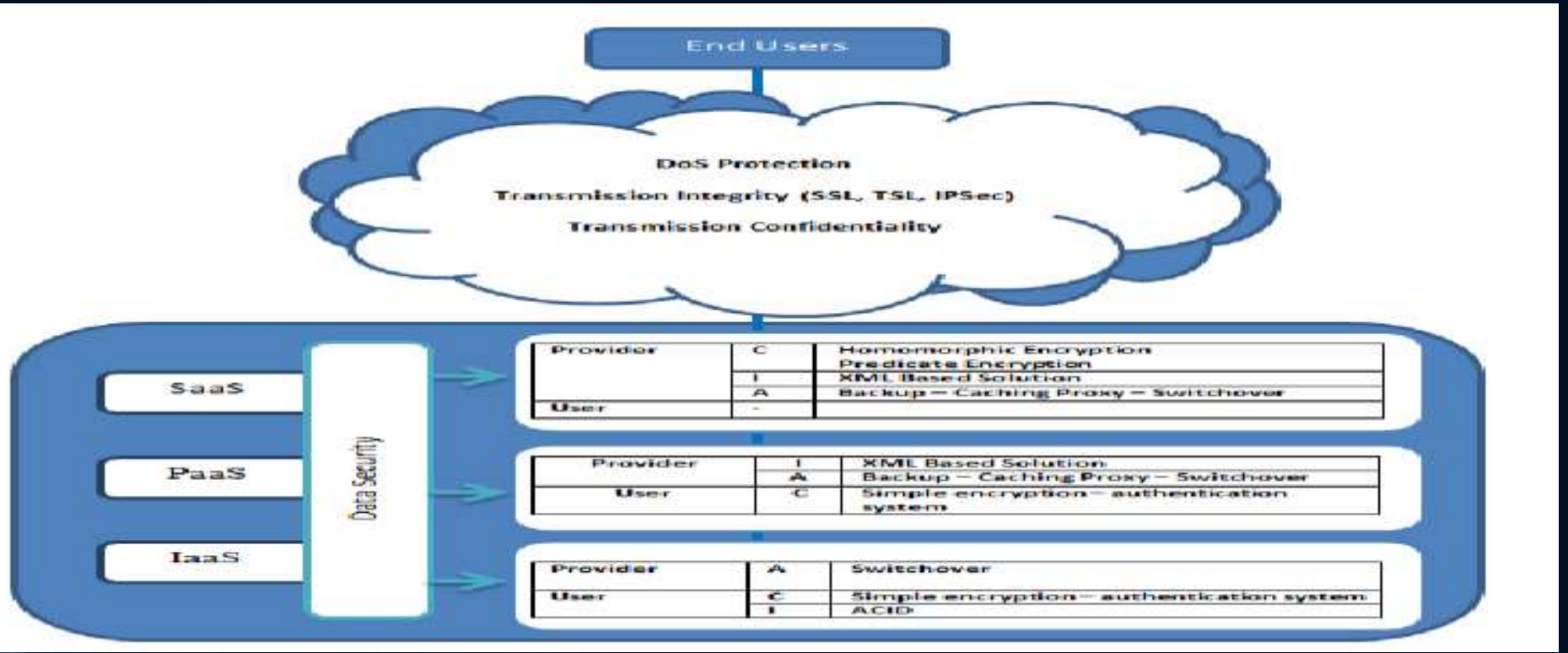
Cloud Data Security

- The proposed data security model uses three-level defense system structure…
  - Strong authentication is achieved by using OTP.
  - Data are encrypted automatically by using strong/fast encryption algorithm.
  - Fast recovery of user data.



Cloud Data Security

Data Security Model In Cloud Computing

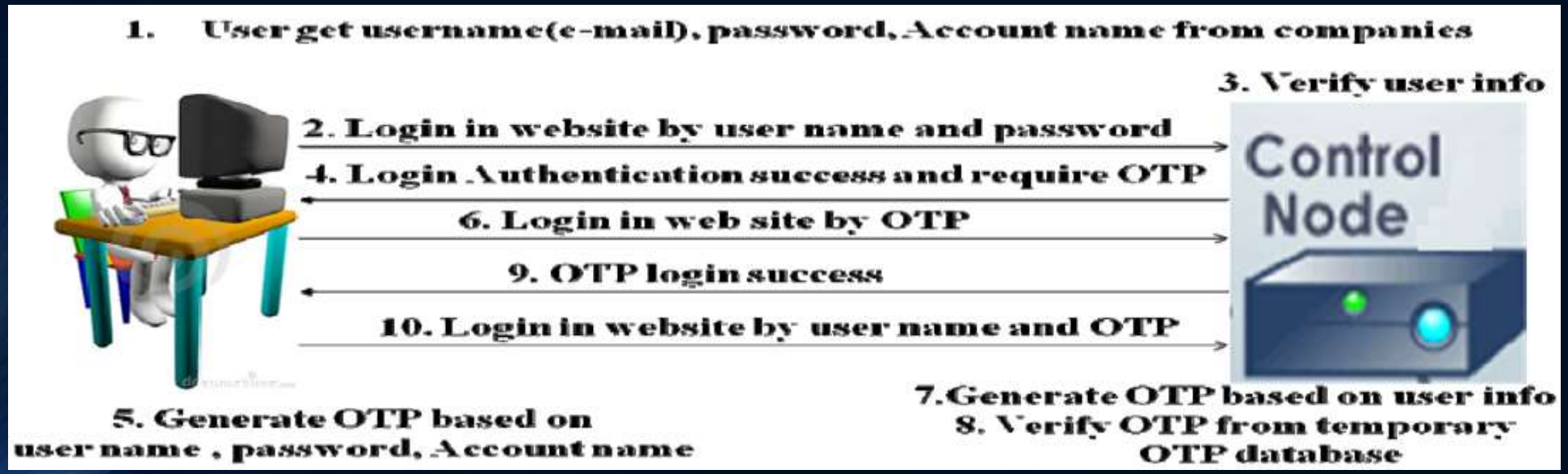


Cloud Data Security

- OTP Authentication:
  - The users connect to the cloud provider. Then the user gets the username (e-mail), password and finally account password.
  - Users login to the cloud provider website by getting username (e-mail), password and account password. Cloud node controller verifies user info.
  - If user info is true, controller-node send that login authentication success and require OTP.
  - Users generate OTP by using MD5 hash function and sequence number based on user name, password and account password.
  - Then users login to cloud website with OTP .
  - The cloud controller node generates 1000 OTP based on user info by using the MD5 hash function. Then the cloud controller saves 1000 OTP in the temporary OTP database.

Cloud Data Security

- OTP Authentication:
  - The cloud controller verifies user OTP from the temporary OTP database.
  - If OTP is true, send OTP login success.

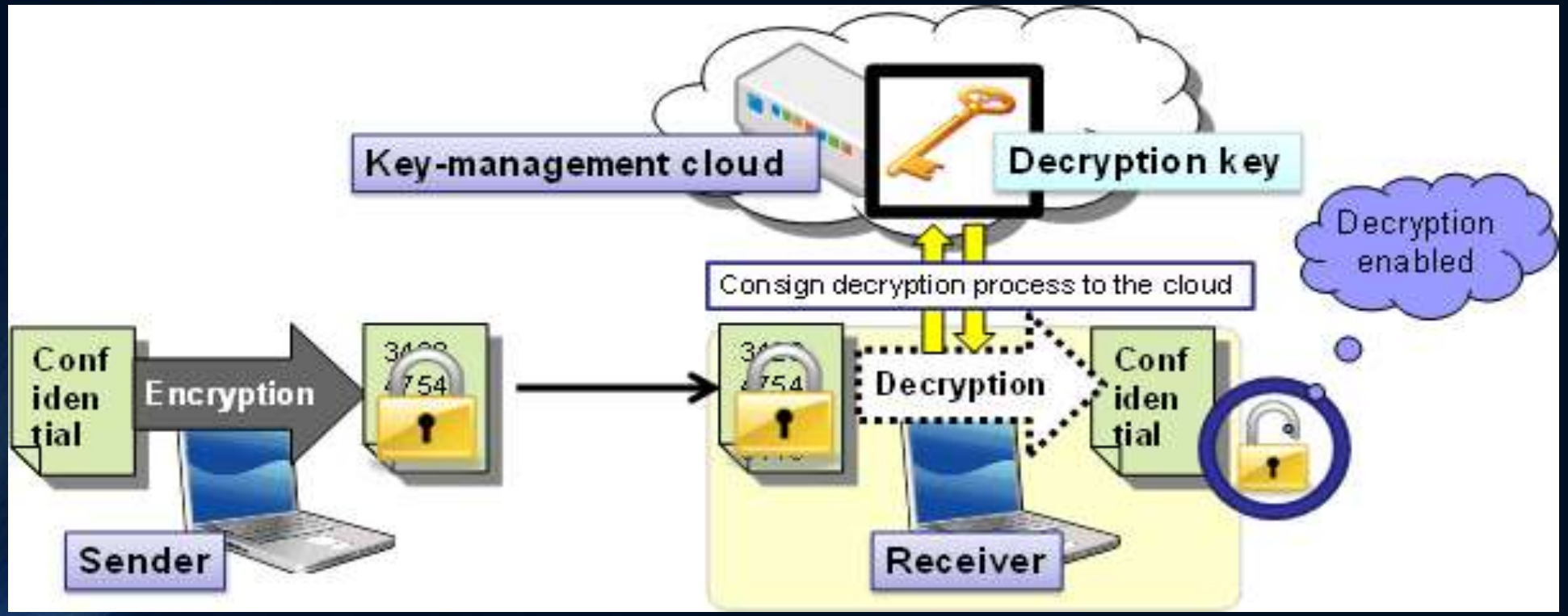


Cloud Data Security

- Evaluation Algorithm Results:
  - Select the strongest and the fastest encryption algorithm by proposing algorithm called "Evaluation algorithm".
  - This algorithm used for selecting eight modern encryption techniques namely: RC4, RC6, MARS, AES, DES, 3DES, Two-Fish and Blowfish.
  - The evaluation has performed for those encryption algorithms according to randomness testing by using NIST statistical testing.
  - This evaluation algorithm performed at Amazon EC2 Micro Instance cloud computing environment.
  - RC4 has an advantage over other DES, RC6, MARS, 3DES and Twofish in terms of time consumption.
  - Twofish has low performance when compared with other algorithms.

Cloud Data Security

Encryption and Decryption Process



Cloud Data Security

- Ensuring Integrity:
  - This is an extra concern for customers that now they have to worry about how to keep data hidden from auditors.
  - This integrity check can be done by using cryptographic hash functions.
  - For integrity check, we have to think about a simple solution that is feasible and easy to implement for a common user.
  - The trust problem between Cloud storage and customer can be solved, if users can check the integrity of data themselves instead of renting an auditing service to do the same.
  - This can be achieved by hashing the data on user's side and storing the hash values in the cloud with the original data.

Cloud Data Security

- Ensuring Integrity:
  - Hashing technique steps…
    - The program takes file path which has to be accessed through cloud.
    - The program computes a four-hash values in this file based on the four hash functions (MD4, MD5, SHA-1 and SHA-2).
    - When users store data in cloud storage devices, server stores four hash values.
    - When a user retrieve data file from cloud, server generate four hash values.
    - Server check integrity by comparing new four hash values with stored four hash values.

Cloud Data Security

High Level Summary of Cloud Data Security Features

Features	Description
Authentication	OTP Authentication System (mathematical generation).
Provider encryption	Software implemented to select the highest security and faster encryption algorithm based on NIST statistical tests.
Private user encryption	TrueCrypt system or proposed software CloudCrypt v.10.
Data integrity	Hashing-MD5-MD4-SHA-1-SHA-2.
Data fast recovery	Based on decryption algorithm speed.
Key management	User keys not stored in provider control domain.

THANKS