Application of Active Bundles

Bharat Bhargava

A. Identity Management (IDM) Service-Oriented Architecture (SOA)

- IDM in traditional application-centric IDM model
    - ➢ Each application keeps trace of identities of the entities it uses.

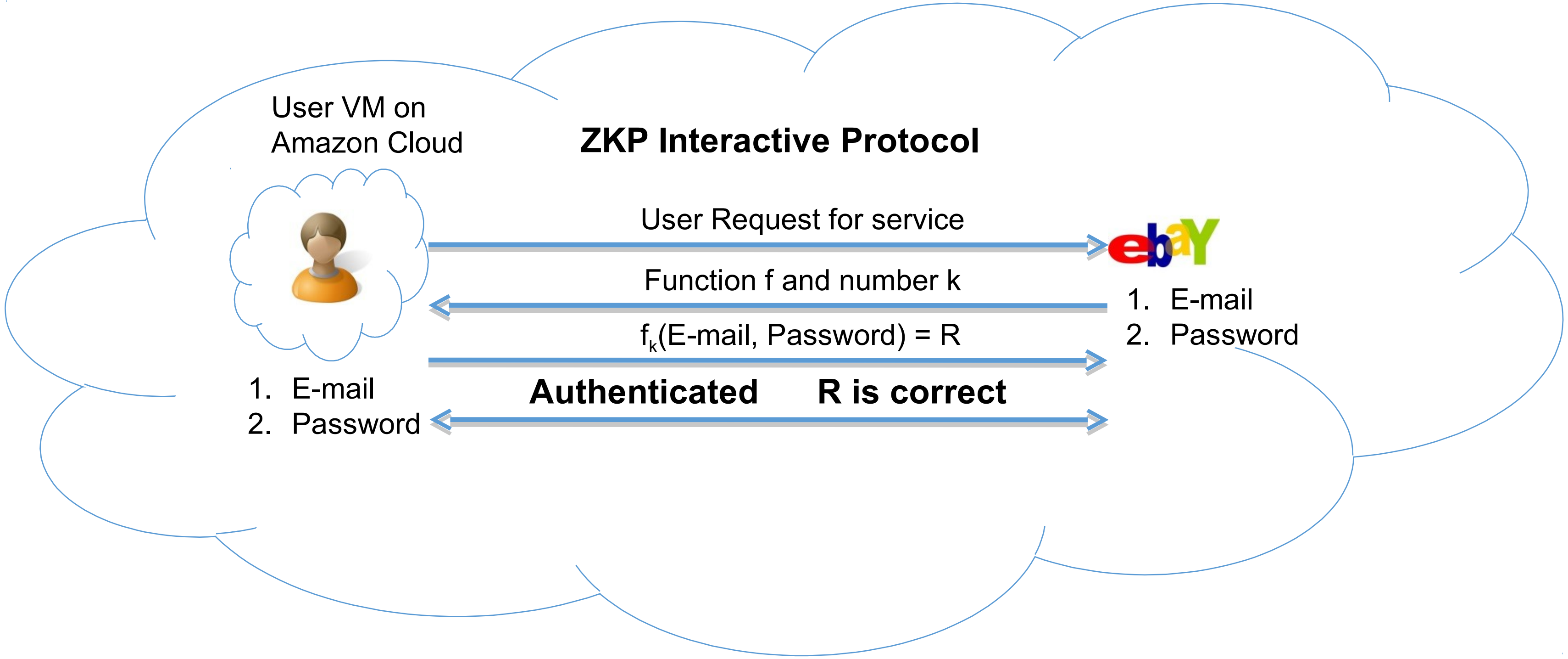
- IDM in SOA
    - ➢ Entities have multiple accounts associated with a single or multiple service providers (SPs).
    - ➢ Sharing sensitive identity information along with associated attributes of the same entity across services can lead to ***mapping of the identities to the entity.***

Goals of IDM

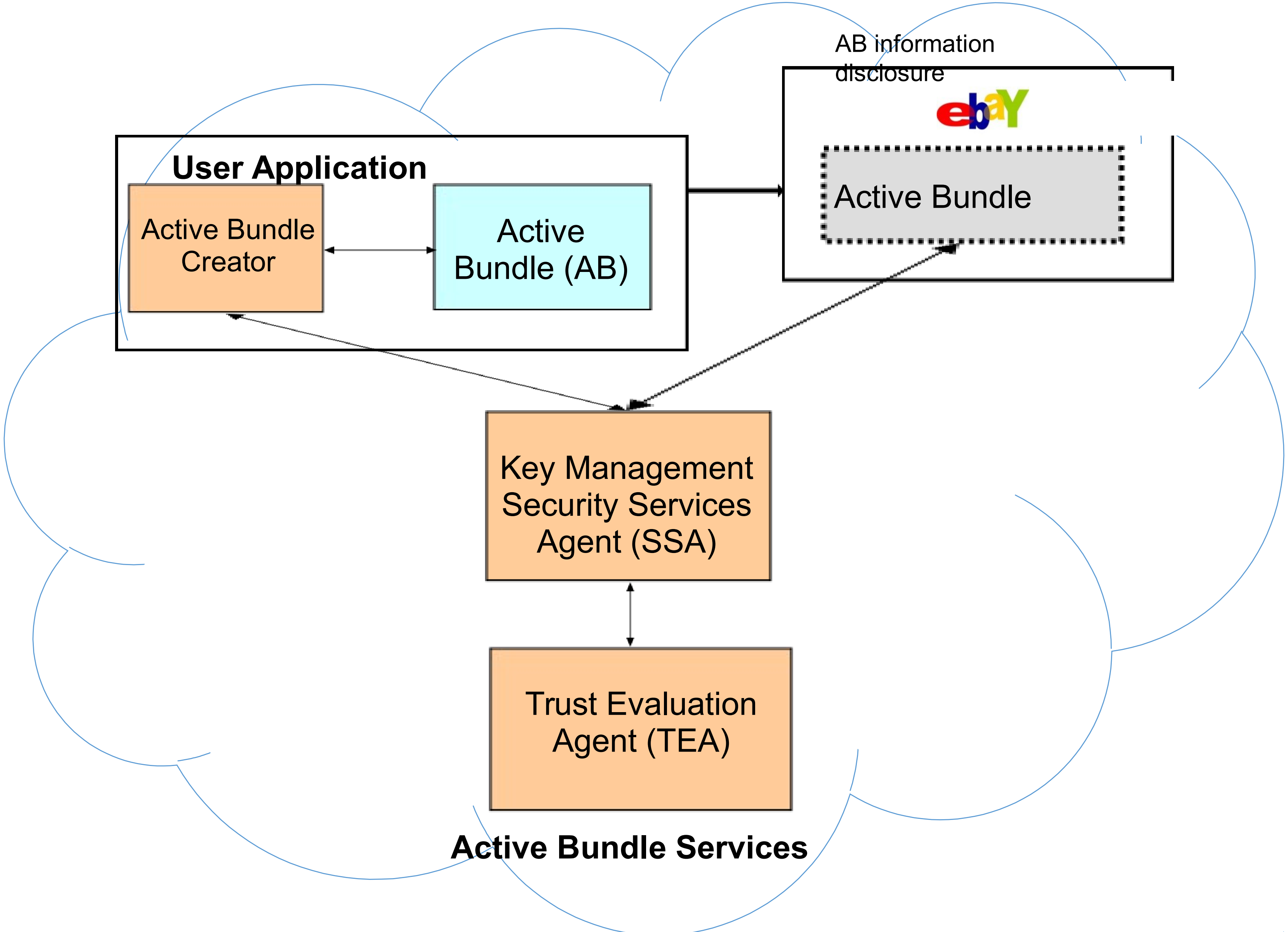
1. Authenticate without disclosing data (Unencrypted data)
2. Use service on untrusted hosts (hosts not owned by user)
3. Minimal disclosure and minimize risk of disclosure during communication between user and service provider (Man in the Middle, Side Channel and Correlation Attacks)
4. Independence of Trusted Third Party

Anonymous Identification

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

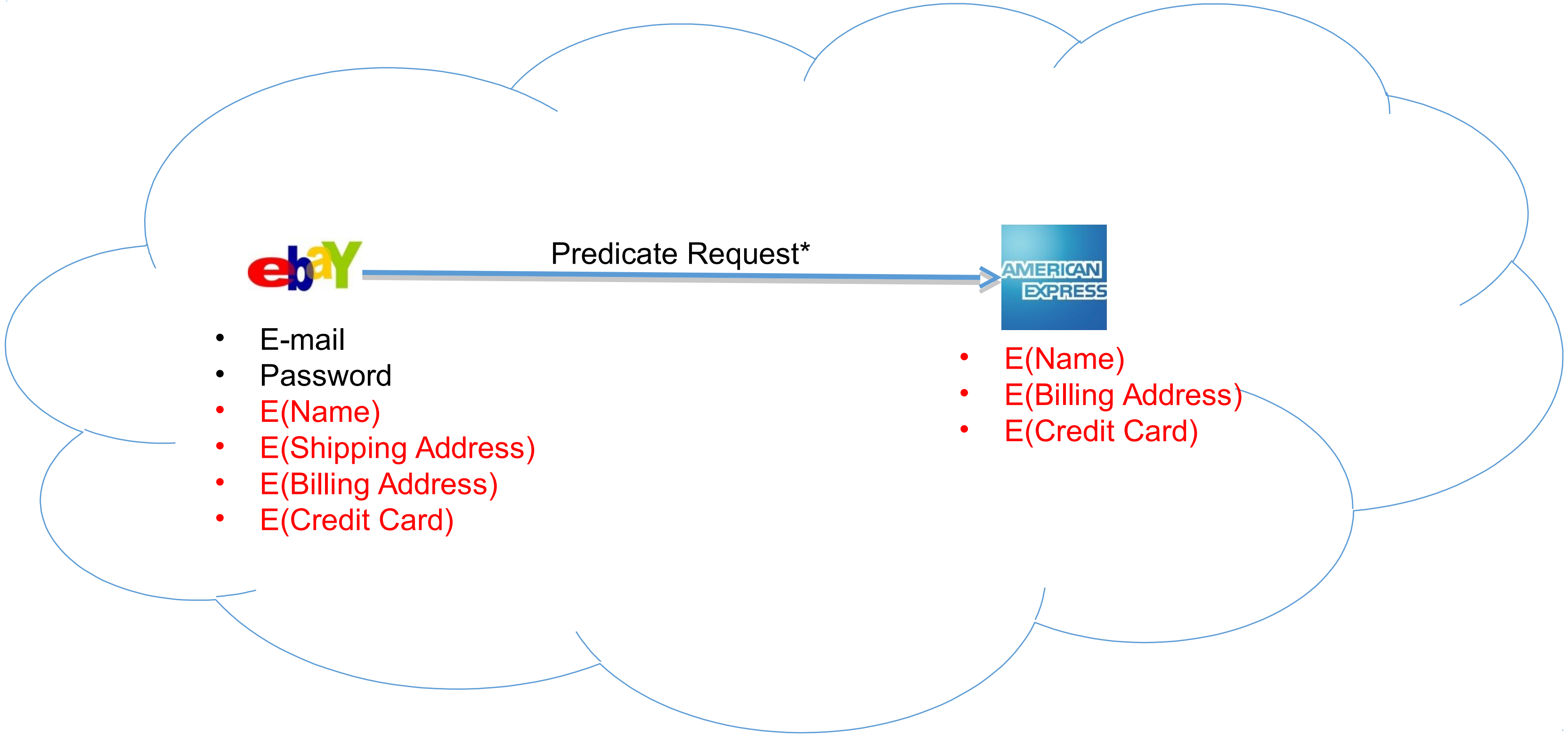


Interaction using Active Bundle


AB information disclosure
ebay
User Application
Active Bundle Creator
Active Bundle (AB)
Active Bundle
Key Management Security Services Agent (SSA)
Trust Evaluation Agent (TEA)
Active Bundle Services

Predicate over Encrypted Data

- Verification without disclosing unencrypted identity data.



Predicate Request*

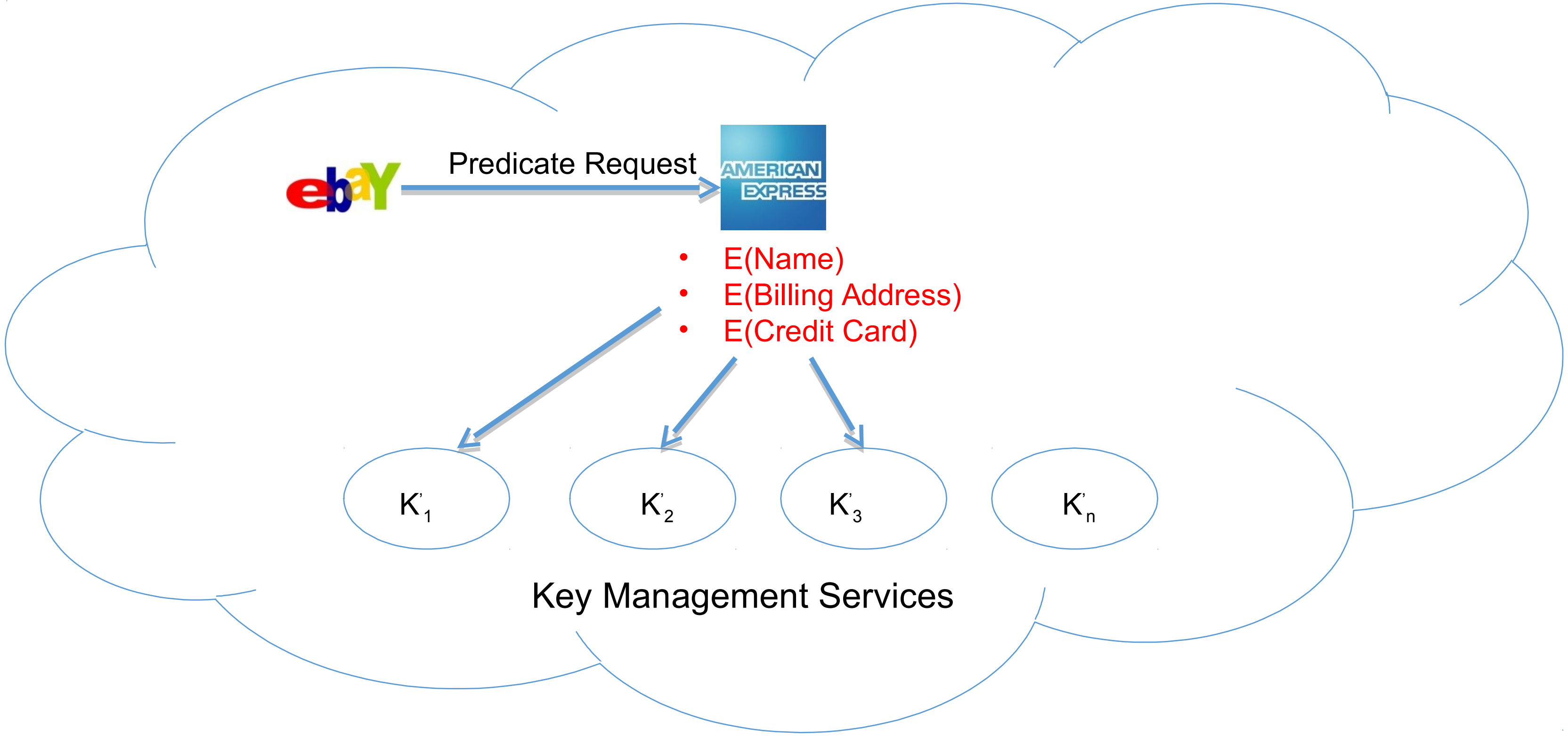
- E-mail
- Password
- E(Name)
- E(Shipping Address)
- E(Billing Address)
- E(Credit Card)

- E(Name)
- E(Billing Address)
- E(Credit Card)

*Credit Card Verification Request

Multi-Party Computation

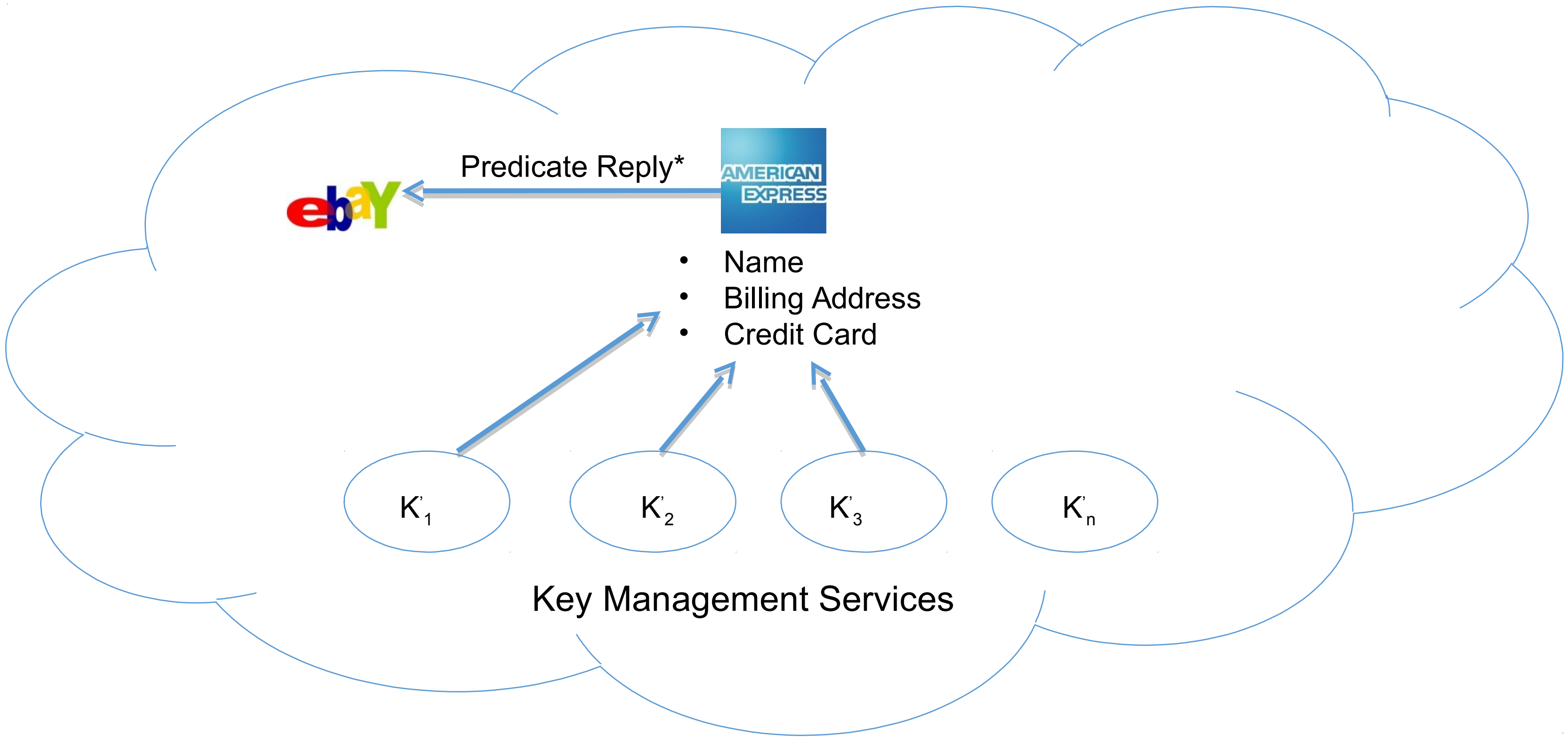
- To become independent of a trusted third party
  - Multiple Services hold shares of the secret key
  - Minimize the risk



* Decryption of information is handled by the Key Management services

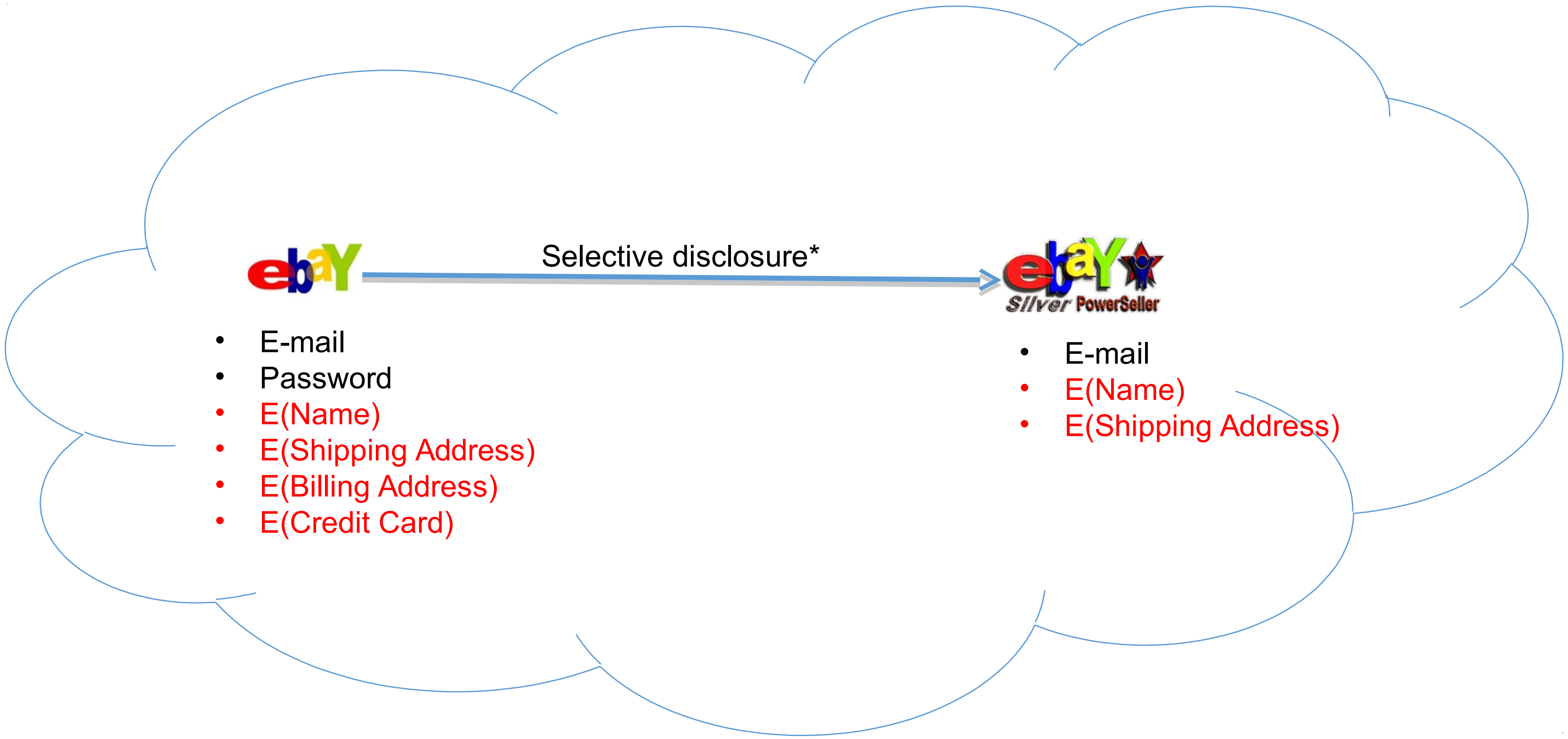
Multi-Party Computation

Credit Card Verified



Selective Disclosure

- User Policies in the Active Bundle dictate dissemination

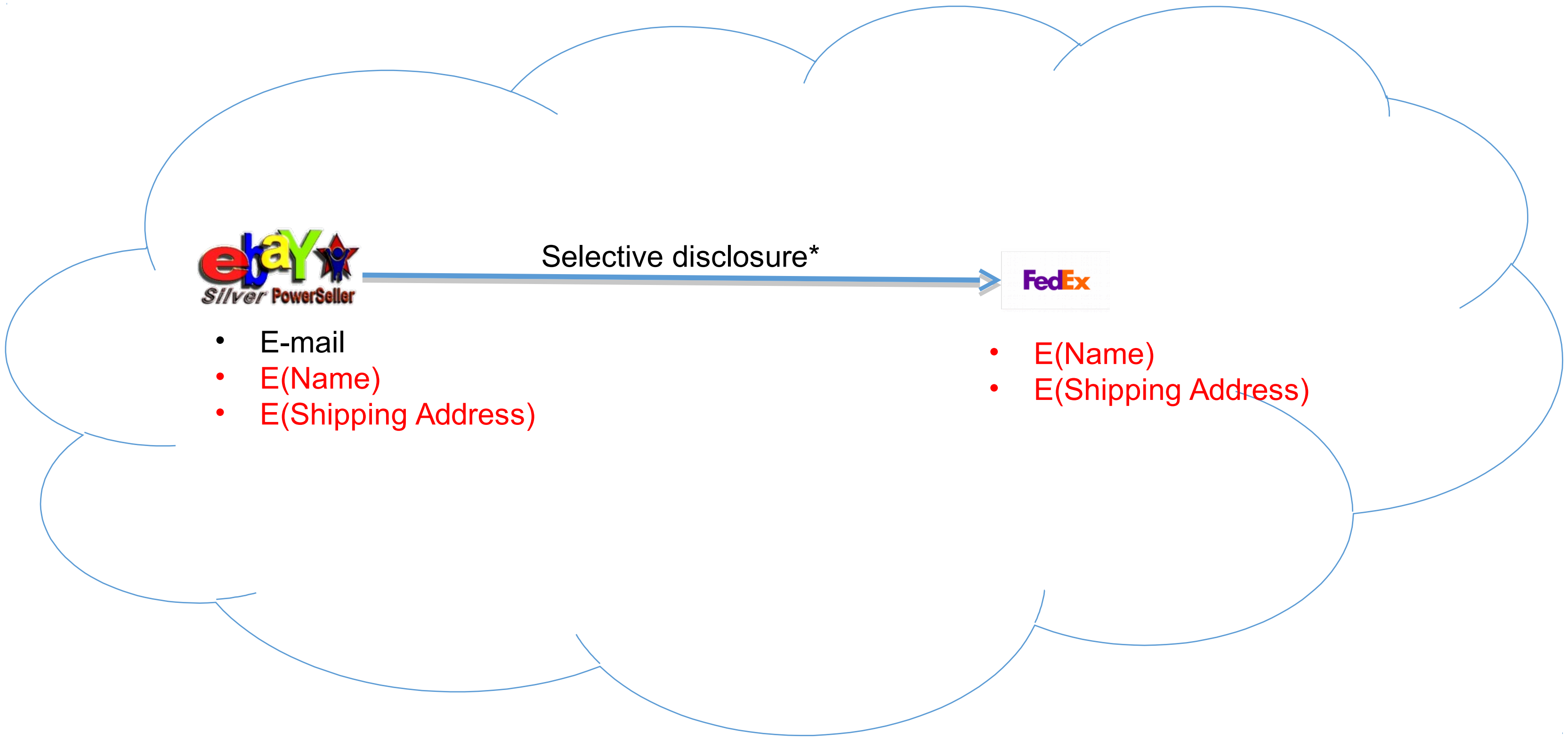


- E-mail
- Password
- E(Name)
- E(Shipping Address)
- E(Billing Address)
- E(Credit Card)

- E-mail
- E(Name)
- E(Shipping Address)

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

Selective Disclosure



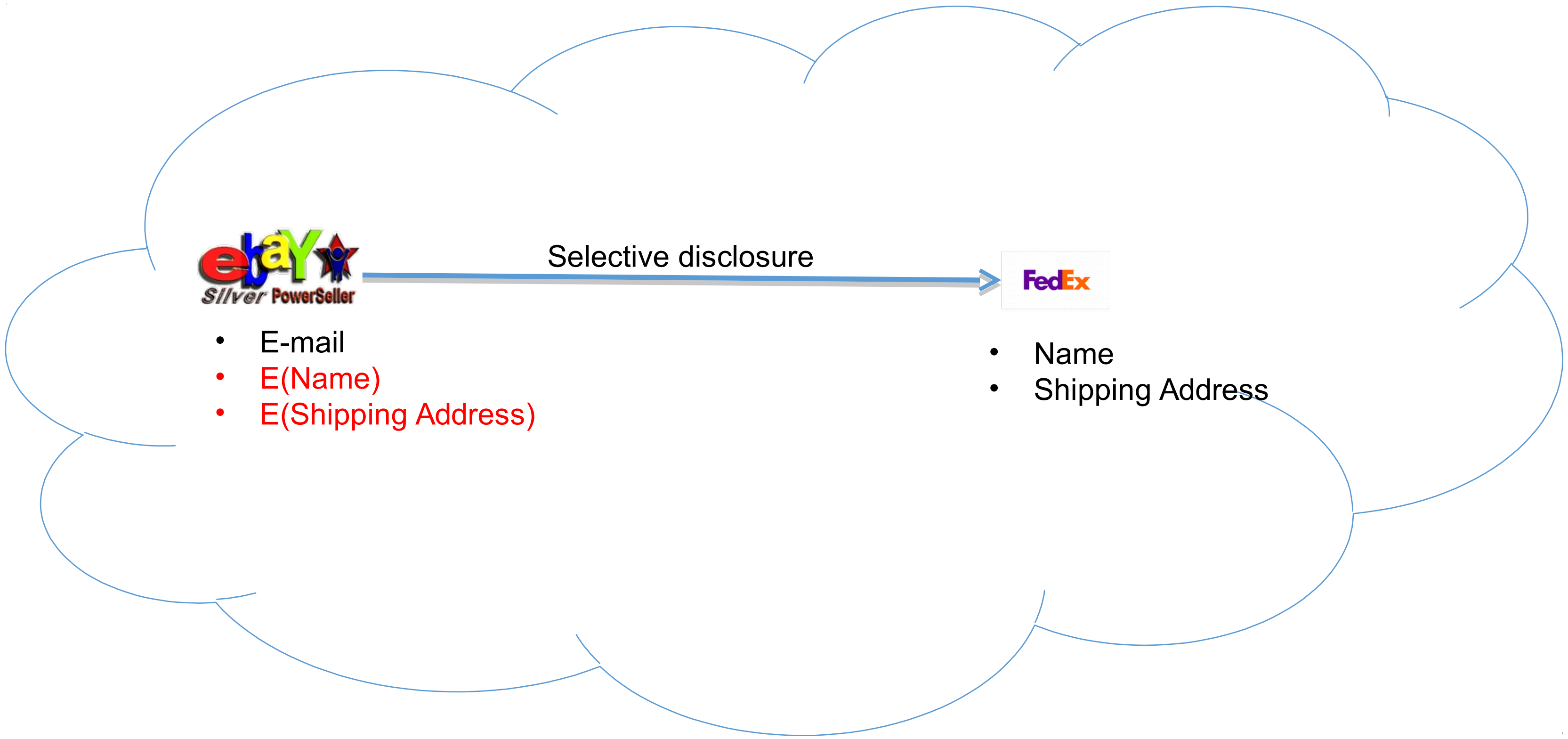
Selective disclosure*

- E-mail
- E(Name)
- E(Shipping Address)

- E(Name)
- E(Shipping Address)

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

Selective Disclosure

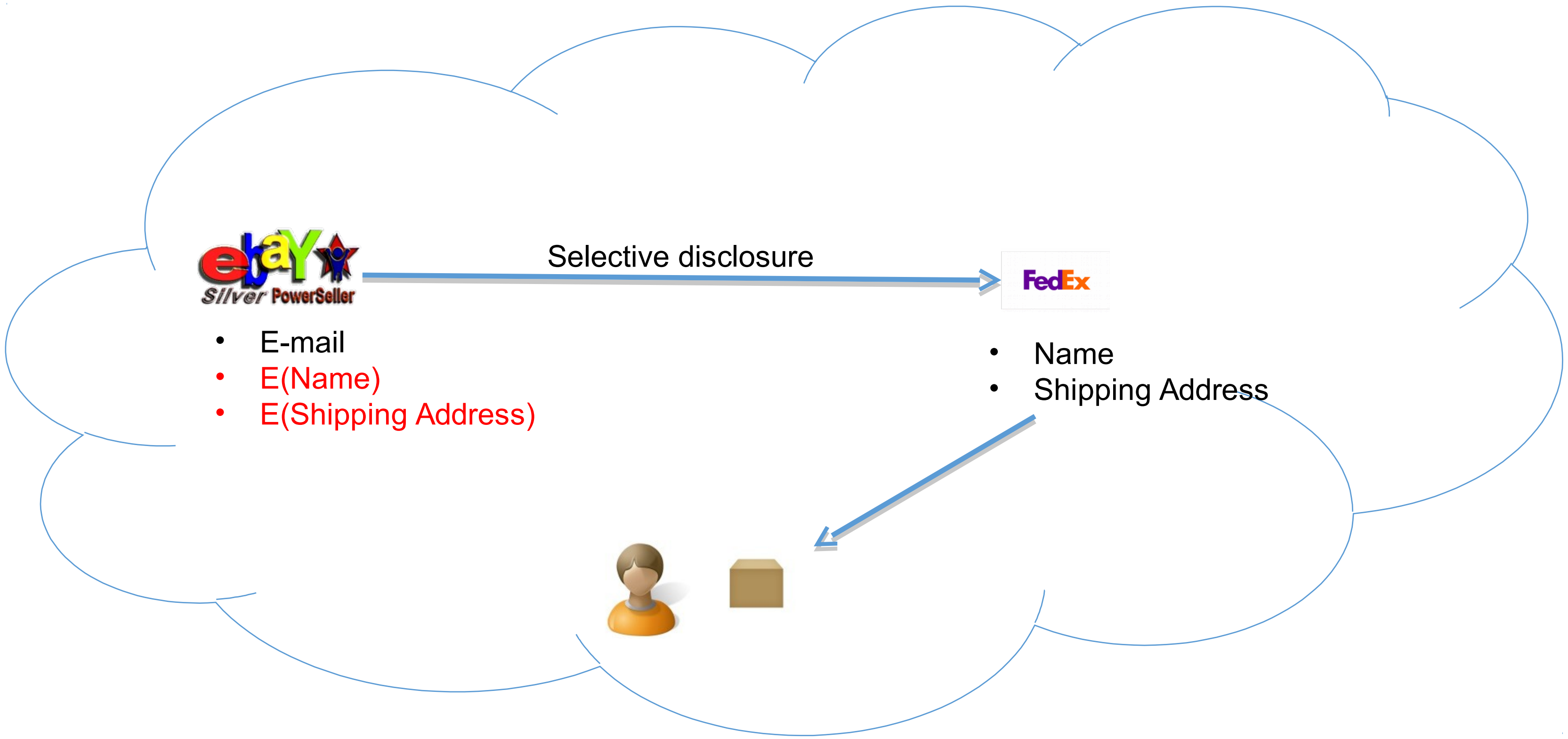


- E-mail
- E(Name)
- E(Shipping Address)

- Name
- Shipping Address

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

Selective Disclosure



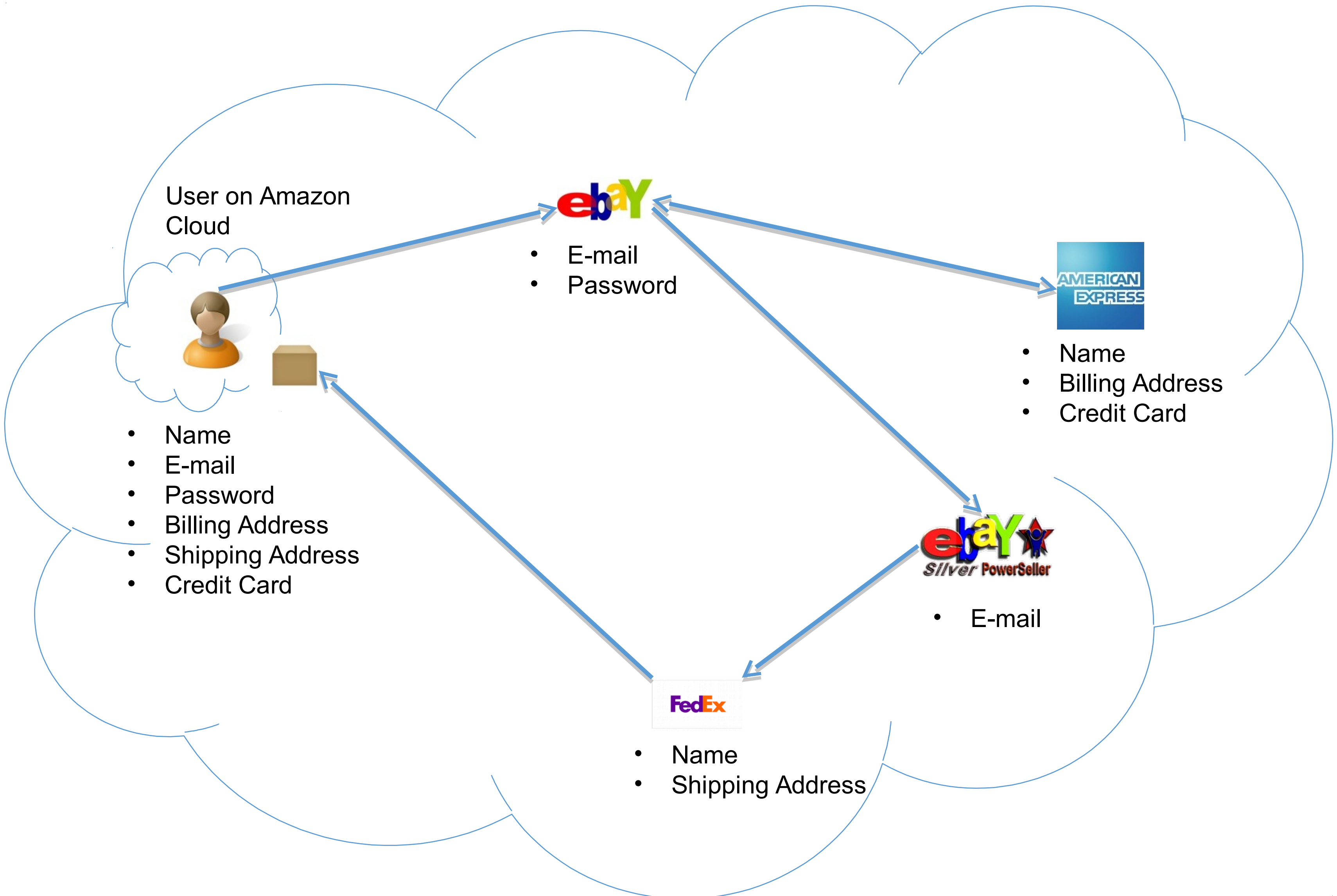
Selective disclosure

- E-mail
- E(Name)
- E(Shipping Address)

- Name
- Shipping Address

- Fed-Ex can now send the package to the user

Identity revealed to Vendors



User on Amazon
Cloud

- Name
- E-mail
- Password
- Billing Address
- Shipping Address
- Credit Card

- E-mail
- Password

- Name
- Billing Address
- Credit Card

- E-mail

- Name
- Shipping Address

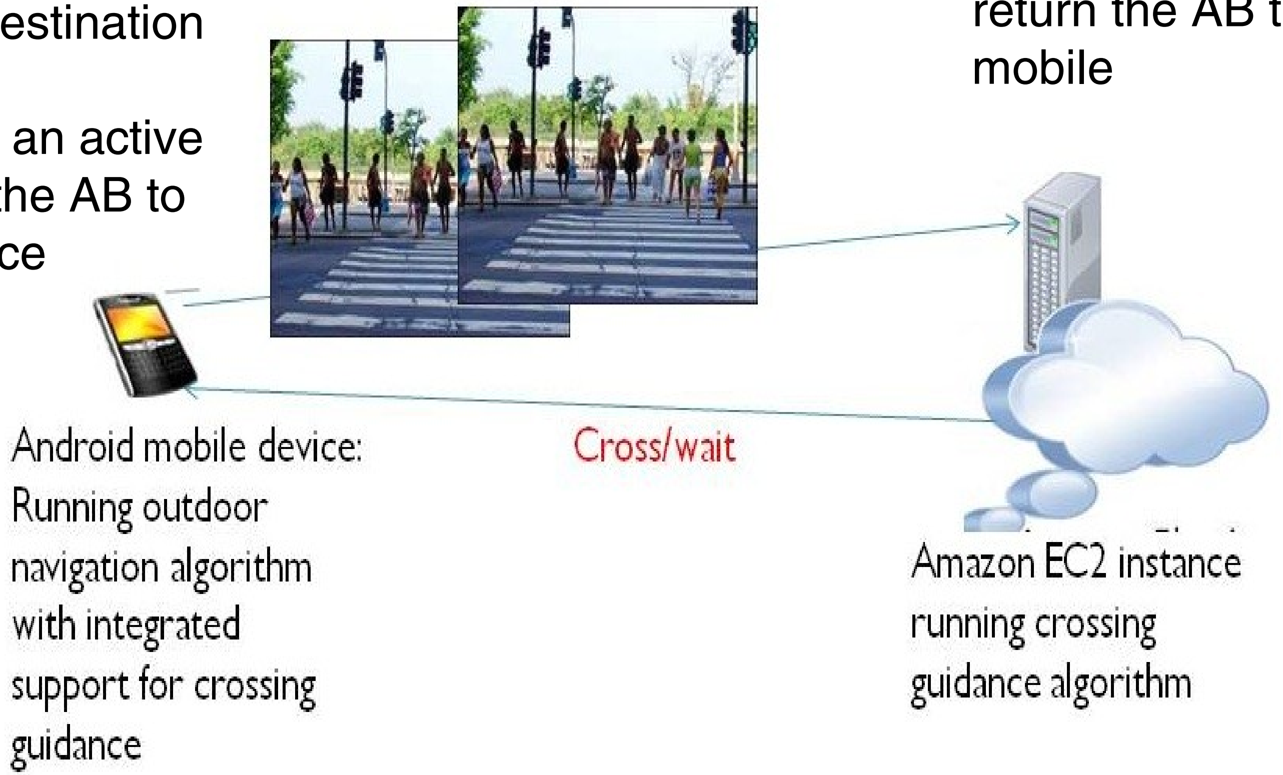
Advantage of AB for IDM

- Ability to use Identity data on untrusted hosts
  - Self Integrity Check against Corruption of AB content
  - Compromised AB leads to apoptosis
- Establishes the trust of users in Requesters
  - Through putting the user in control of who has her data and how it is disseminated
- Independent of Third Party
  - Minimizes identity correlation attacks
- Minimal disclosure to the requester.

B. Mobile-Cloud Pedestrian Crossing Guide for the Blind

Bundle the image, position, and destination as well as the computation in an active bundle; send the AB to the cloud service

Process the code and return the AB to the mobile

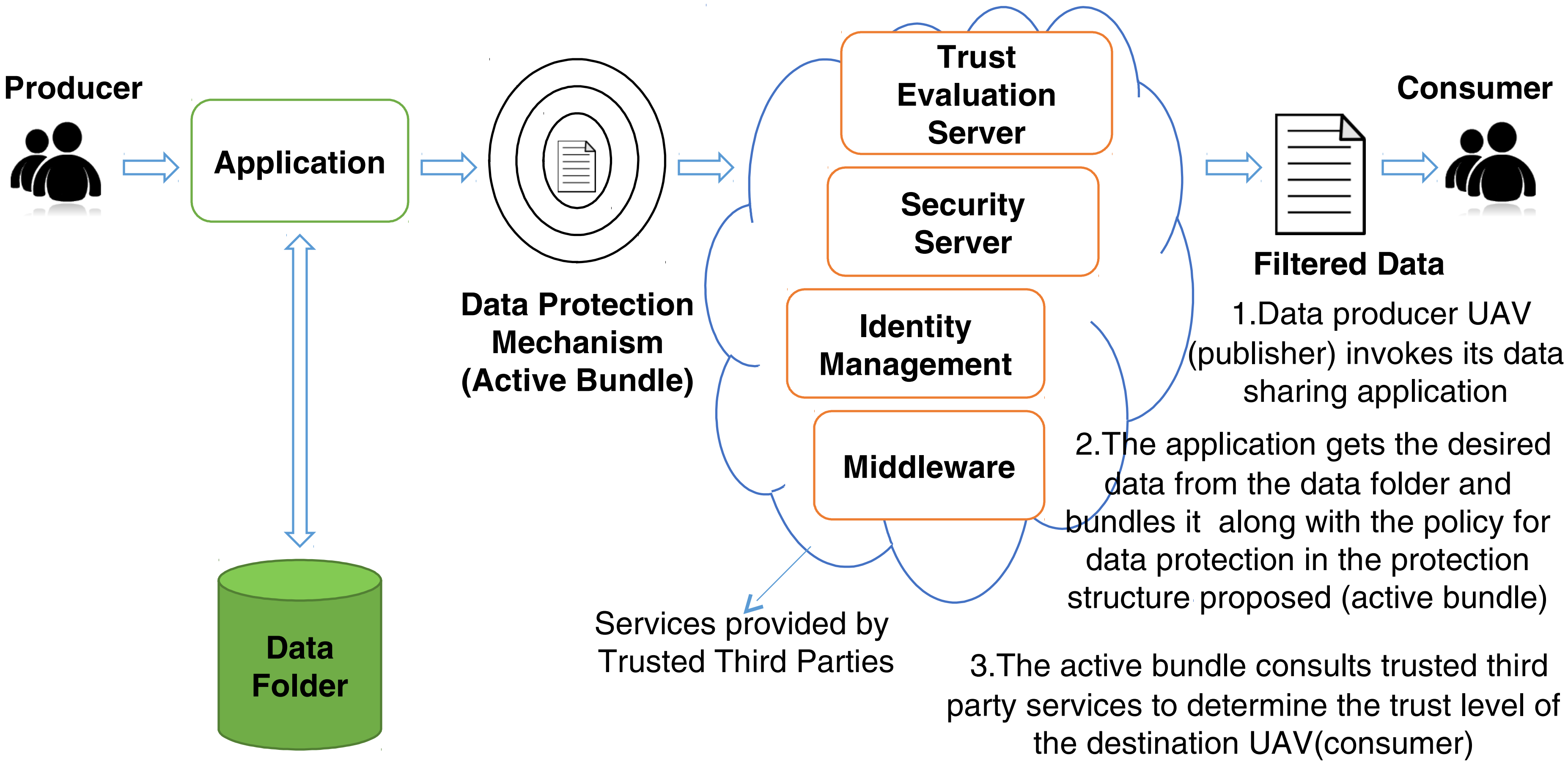

Android mobile device:
Running outdoor navigation algorithm with integrated support for crossing guidance
Cross/wait
Amazon EC2 instance running crossing guidance algorithm

Ensure data are protected; e.g., removed from the cloud when processing finishes.

C. A Trust-based Approach for Secure Data Dissemination in a Mobile Peer-to-Peer Network of UAVs

- Mobile peer-to-peer networks of unmanned aerial vehicles (UAVs) have become significant in collaborative tasks including military missions and search and rescue operations
- Data communication (over shared media) between the nodes in a UAV network makes the disseminated data prone to interception by malicious parties, which could cause serious harm for the designated mission of the network
- A scheme for secure dissemination of data between UAV nodes is needed

Proposed Data Protection Scheme



1.Data producer UAV (publisher) invokes its data sharing application

2.The application gets the desired data from the data folder and bundles it along with the policy for data protection in the protection structure proposed (active bundle)

3.The active bundle consults trusted third party services to determine the trust level of the destination UAV(consumer)

4.The active bundle filters its data based on the trust level of the consumer and the matching of policies between the producer and consumer and presents the filtered data to the consumer.

Dynamic Trust Calculation

- The trust calculation component works like a reputation system, where the trustworthiness of a node is evaluated based on various dynamic parameters
- Trust parameters vary with the scenario in which the UAVs communicate, and have different weights
- Computed trust value is used to determine whether it is safe to share the data and the degree of filtering to apply on the data before sharing
- Trust value *T* for a particular UAV *u* at time *t* also depends on previous interactions with that UAV and is calculated using the below formula, where *a* determines how important previous interactions are and *P* is the trust value determined by the dynamic parameters

$$T_{\boldsymbol{u}}(\boldsymbol{t}) = a \cdot T_{\boldsymbol{u}}(\boldsymbol{t}-1) + (1- a) \cdot P$$

Trust Evaluation

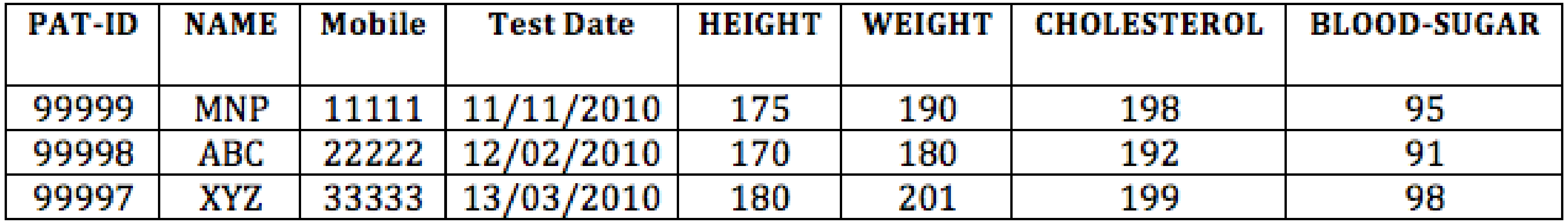
Trust level for the destination UAV (data consumer) can be evaluated and verified by a Trusted Third Party and can be based on different parameters such as:

- **Location**: USA, Middle East, Iraq, etc
- **Security Clearance Level**: Top-secret, Secret, Confidential, Unclassified
- **Bandwidth**: High Bandwidth, Low Bandwidth
- **History of Obligations**: Satisfactory, Unsatisfactory
- **Distance**: Not necessarily based on metric distance, i.e. more trusted entities are closer
- **Authentication Level**: Fully authenticated, Partially authenticated, Not authenticated
- **Context**: Emergency, Disaster, Normal etc.

Example of Data Filtering

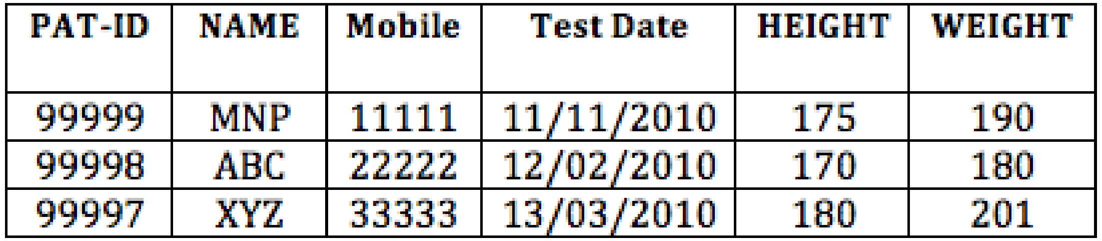
EPHI (Electronic Private Health Information):

Stored in a relational database, data filtering for different data consumers performed through SQL queries run in the Active Bundle VM



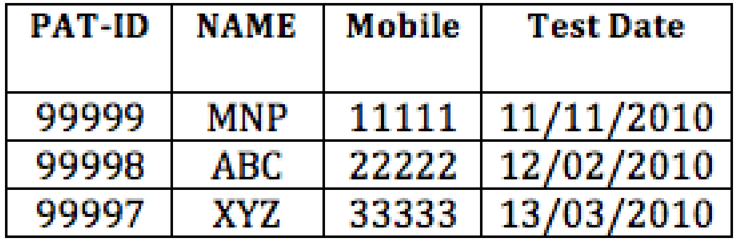
PAT-ID	NAME	Mobile	Test Date	HEIGHT	WEIGHT	CHOLESTEROL	BLOOD-SUGAR
99999	MNP	11111	11/11/2010	175	190	198	95
99998	ABC	22222	12/02/2010	170	180	192	91
99997	XYZ	33333	13/03/2010	180	201	199	98

a. Data consumer verified as doctor at the hospital can get all patient data



PAT-ID	NAME	Mobile	Test Date	HEIGHT	WEIGHT
99999	MNP	11111	11/11/2010	175	190
99998	ABC	22222	12/02/2010	170	180
99997	XYZ	33333	13/03/2010	180	201

b. Hospital Receptionist gets filtered data



PAT-ID	NAME	Mobile	Test Date
99999	MNP	11111	11/11/2010
99998	ABC	22222	12/02/2010
99997	XYZ	33333	13/03/2010

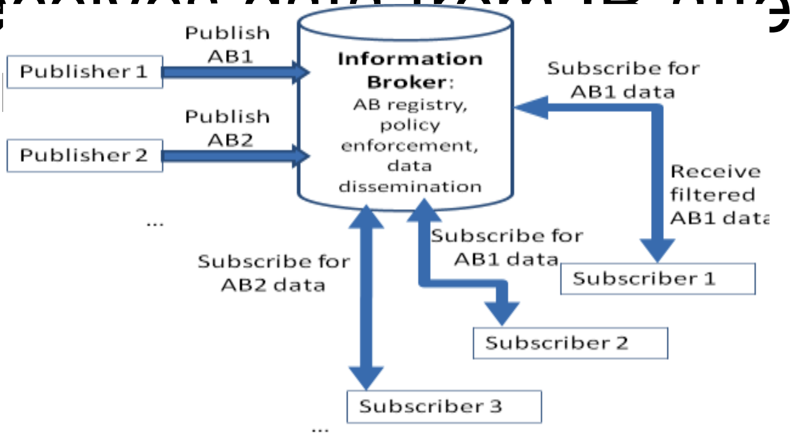
c. Insurance company gets only the minimal required data

Image Data Filtering Techniques

- **Low Dynamic Range Rendering**: This method applies the reverse of high dynamic range rendering on an image to degrade image quality and hide details.
- **Pattern Recognition and Blurring**: This method involves recognition of specific patterns in the image to black out those high sensitivity areas.
- **Data Equivalence Techniques**: Image can be transformed such that the information content of the image remains the same while the fine grain details change (such as replacing the model number of an aircraft with another model's).

Data Dissemination Models

- **Direct Link**: UAVs discover each other through broadcast of ALIVE messages and initiate data transfer without involvement of third-party nodes.
- **Publish-Subscribe**: This model requires a third-party (ground controller) called the *information broker (IB)* to mediate data dissemination between UAVs. The publisher node registers an active bundle with the IB and subscriber receives data from IB after evaluation of its trustwo



Simulation

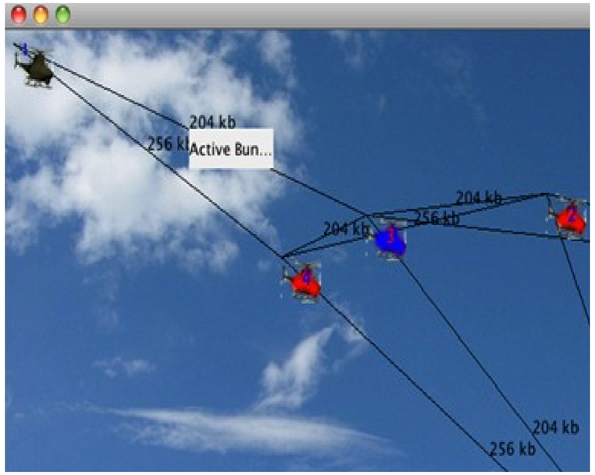
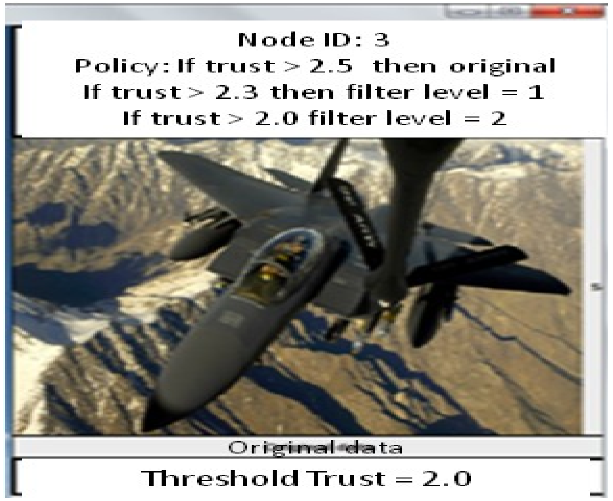


Fig.a. UAV Network. Data transfer is initiated from UAV$_3$ to UAV$_{1.}$ Available bandwidths are displayed on the lines connecting pairs of AVs.



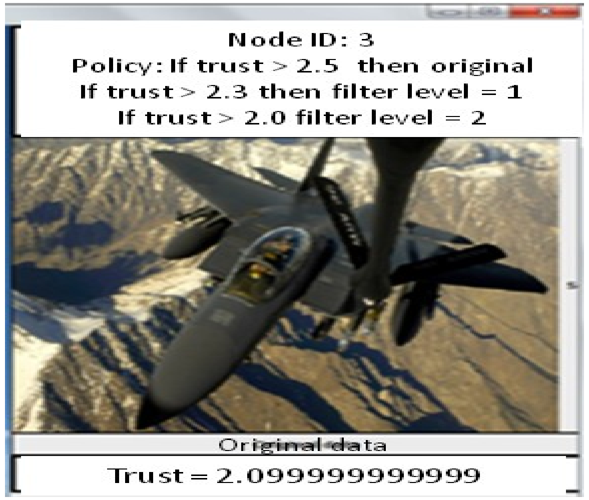
Node ID: 3
Policy: If trust > 2.5 then original
If trust > 2.3 then filter level = 1
If trust > 2.0 filter level = 2

Original data

Threshold Trust = 2.0

Fig.b. Policy of data sharing is at the top, original data in the middle and the virtual machine status at the bottom. Policy is based on the trust level of the AV: If above 2.5, original data is shared; if below 2.5 but above 2.3, minimal filtering is applied; if between 2.3 and 2.0 greater filtering is applied and if below the threshold of 2.0, no data is shared, in which case the active bundle destroys itself.

Simulation (cont.)

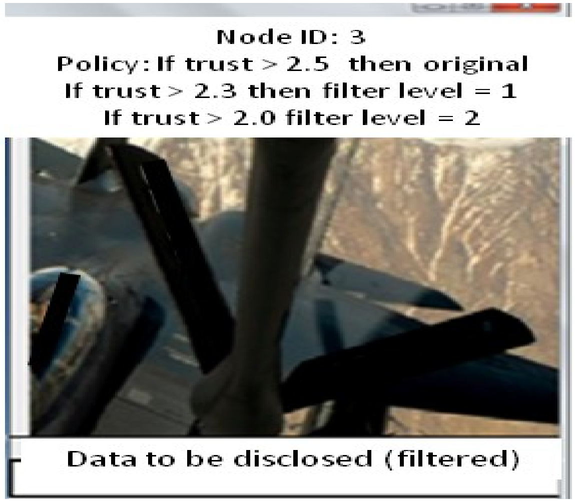


Node ID: 3
Policy: If trust > 2.5 then original
If trust > 2.3 then filter level = 1
If trust > 2.0 filter level = 2

Original data

Trust = 2.0999999999999

Fig.c. The trust level of the receiver AV is calculated as 2.09, which is higher than the threshold trust level, but not high enough to share the original data.



Node ID: 3
Policy: If trust > 2.5 then original
If trust > 2.3 then filter level = 1
If trust > 2.0 filter level = 2

Data to be disclosed (filtered)

Fig.d. Data transformed by the virtual machine according to the policy and the transformed data shared with the receiver node. The data shared provides a narrower view of the environment than the original image.

Simulation