



UNIVERSITY AT ALBANY

State University of New York

SecureCTask: Secure Tasking over Untrusted Third-Party Servers

PRADEEP K ATREY

ALBANY LAB FOR PRIVACY AND SECURITY (ALPS)

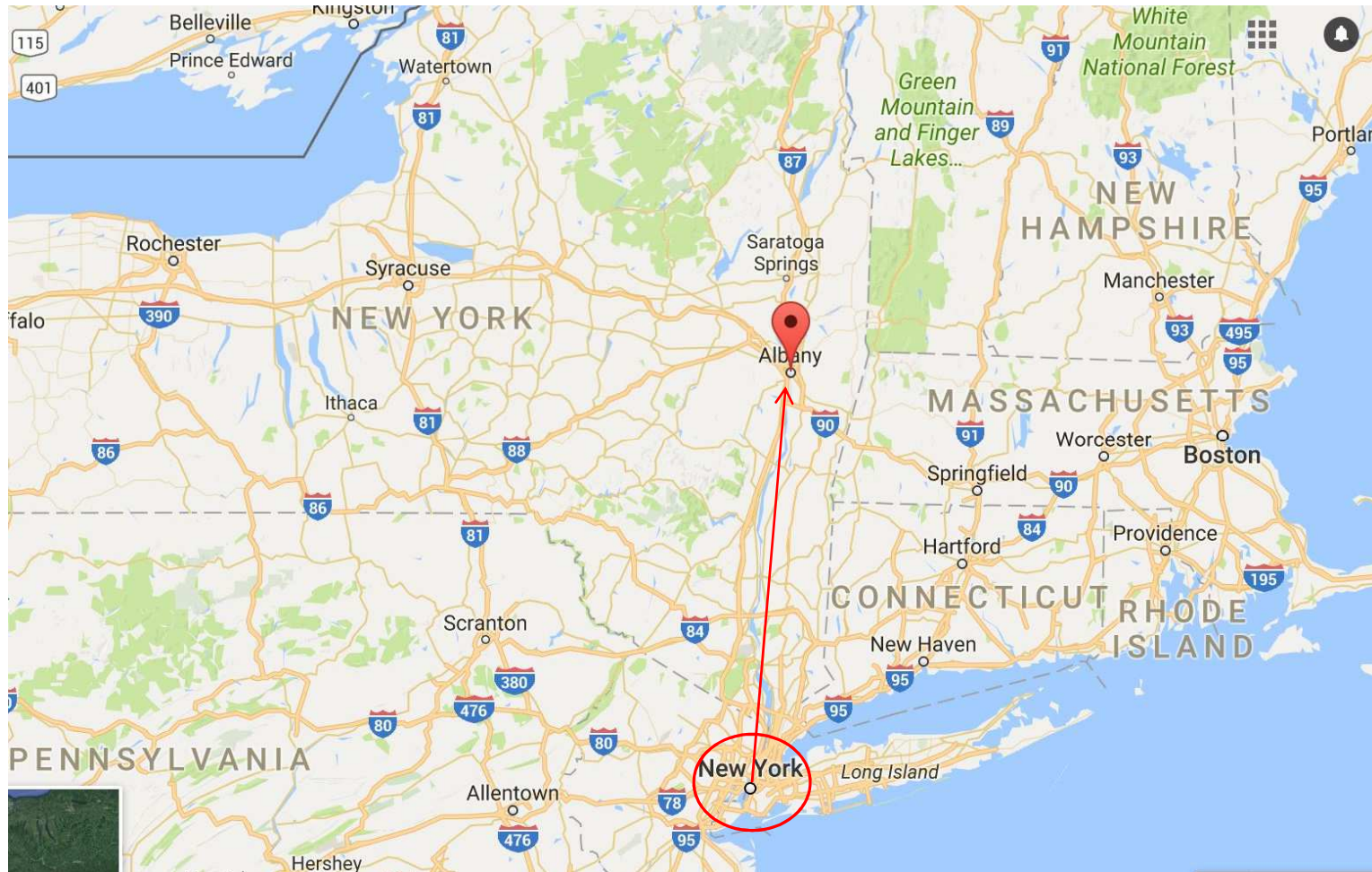
DEPARTMENT OF COMPUTER SCIENCE, COLLEGE OF ENGINEERING AND
APPLIED SCIENCES

EMAIL: PATREY@ALBANY.EDU, URL: WWW.CS.ALBANY.EDU/~PATREY

Where I come from?



Where I come from?



State University of New York at Albany (UAlbany)



[UAlbany Video](#)



UNIVERSITY AT ALBANY
State University of New York

NETSEC 2018, IIT, ROORKEE

4



UNIVERSITY AT ALBANY

State University of New York

SecureCTask: Secure Tasking over Untrusted Third-Party Servers

PRADEEP K ATREY








ALBANY LAB FOR PRIVACY AND SECURITY (ALPS)

DEPARTMENT OF COMPUTER SCIENCE, COLLEGE OF ENGINEERING AND
APPLIED SCIENCES

EMAIL: PATREY@ALBANY.EDU, URL: WWW.CS.ALBANY.EDU/~PATREY

Motivation

Data Per Minute

	510,000 comments, 293,000 status updates, and 136,000 photos
	300 hours of video
	204 million emails
	350,000 tweets
	2.4 million search queries, 12000 GB free Google Drive space
	Terabytes of video
	Gigabytes of audio data

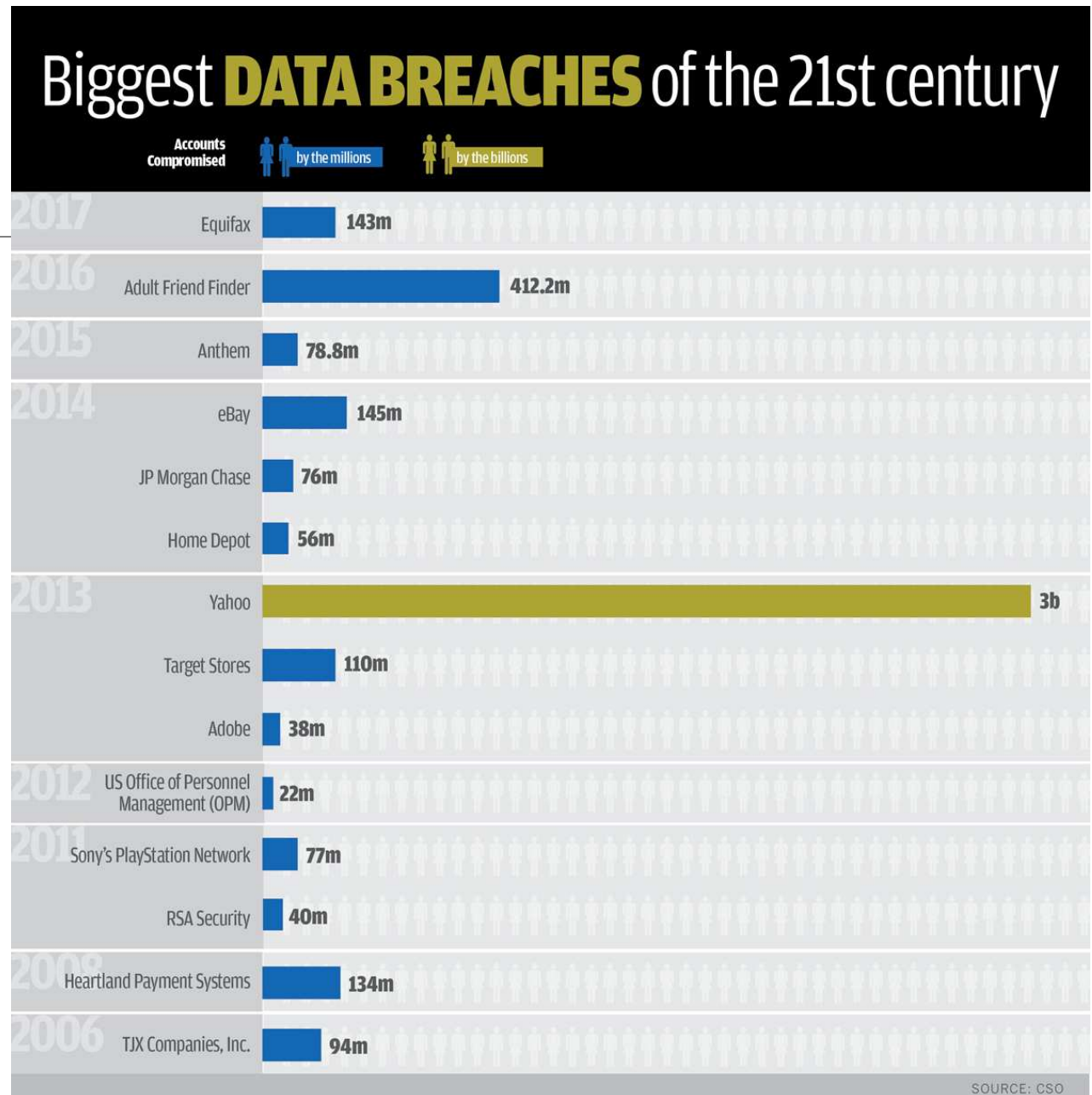
> 2000 TB

STORAGE
&
PROCESSING



Motivation (cont.)

Source: www.csoonline.com
published Oct 11, 2017



Motivation (cont.)

Email Security Breaches

Every single Yahoo account was hacked - 3 billion in all - Oct. 3, 2017
money.cnn.com/2017/10/03/technology/business/yahoo-breach-3.../index.html ▼

Spambot leaks more than 700m email addresses in huge data breach ...
<https://www.theguardian.com> › Technology › Data and computer security ▼
Aug 30, 2017 - Millions of passwords also contained in **breach**, a result of ... that an online **security**



Motivation (cont.)



How many of you
have called to a call
center at least once?

Image source: <http://www.teleware.com/solutions/call-recording/>



Motivation (cont.)



How many of you
have called to a call
center at least once?



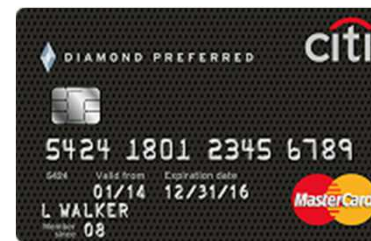
SSN



Passport



**Health
Policy Card**



Credit Card

What is your date of birth?

Day Month Year

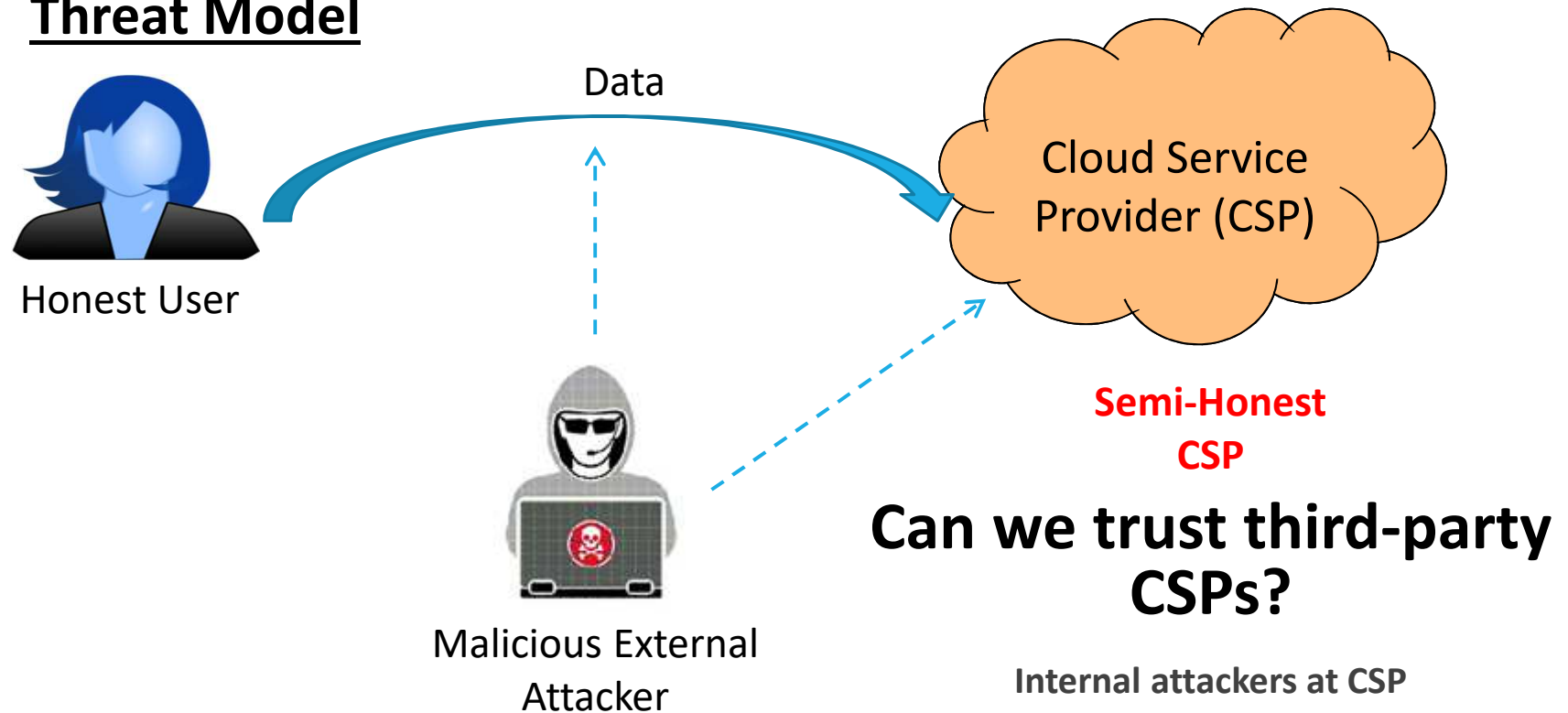
Date of Birth

Image source: <http://www.teleware.com/solutions/call-recording/>



Motivation (cont.)

Threat Model

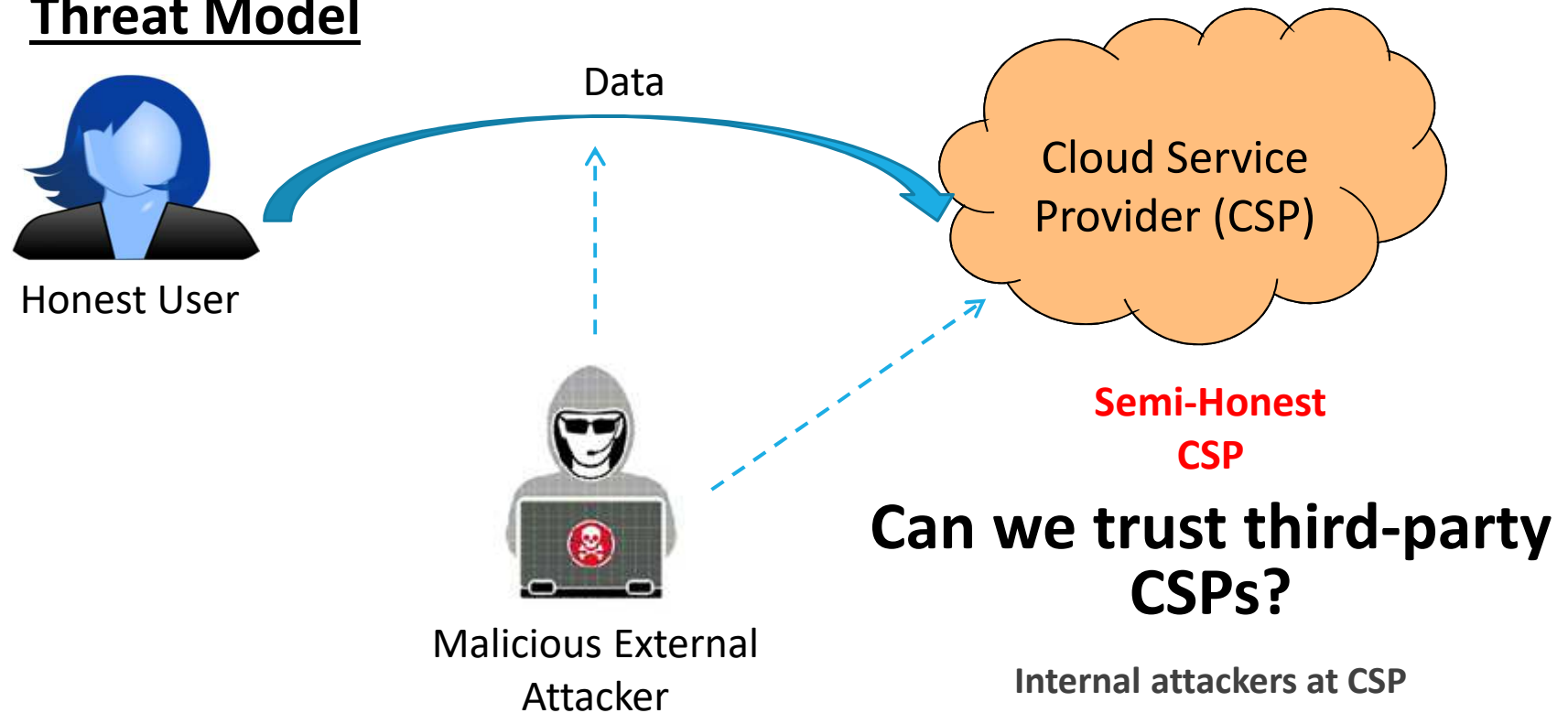


Can We Securely Perform Tasks at Cloud?



Motivation (cont.)

Threat Model



Can We **Securely** Perform **Tasks** at **Cloud**? ➡ **SecureCTask**

SecureCTask

- SecureCScaling
 - Secure Cloud-based Image/Video Scaling
- SecureCEnhance
 - Secure Cloud-based Image/Audio Enhancement
- SecureCMail
 - Secure Cloud-based Emailing
- SecureCMerge
 - Secure Cloud-based PDF merging
- SecureCEdit
 - Secure Cloud-based Document Editing
- SecureCDedup
 - Secure Cloud-based Data Deduplication



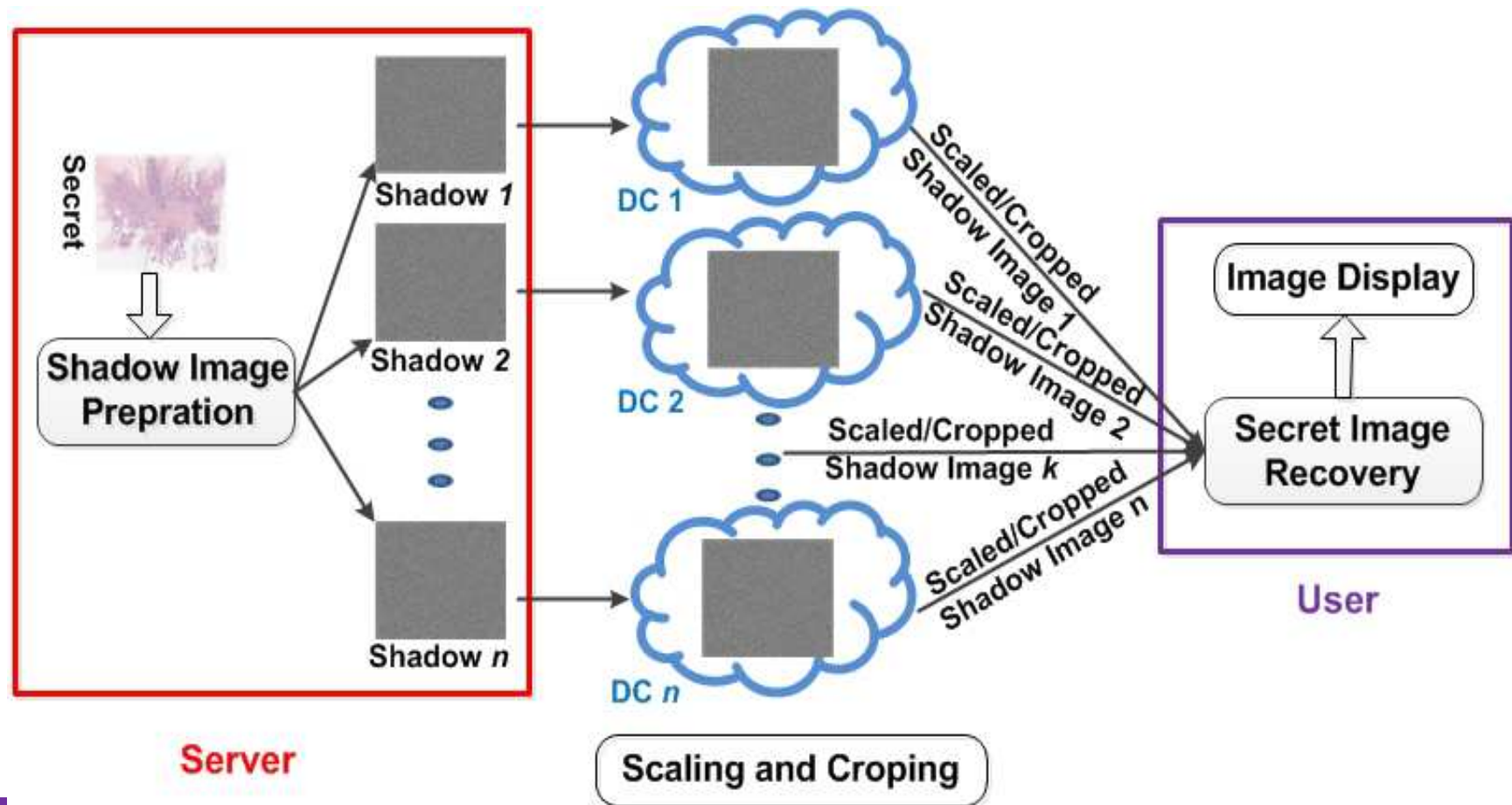
SecureCTask

- **SecureCScaling**
 - Secure Cloud-based Image/Video Scaling
- SecureCEnhance
 - Secure Cloud-based Image/Audio Enhancement
- SecureCMail
 - Secure Cloud-based Emailing
- SecureCMerge
 - Secure Cloud-based PDF merging
- SecureCEdit
 - Secure Cloud-based Document Editing
- SecureCDedup
 - Secure Cloud-based Data Deduplication

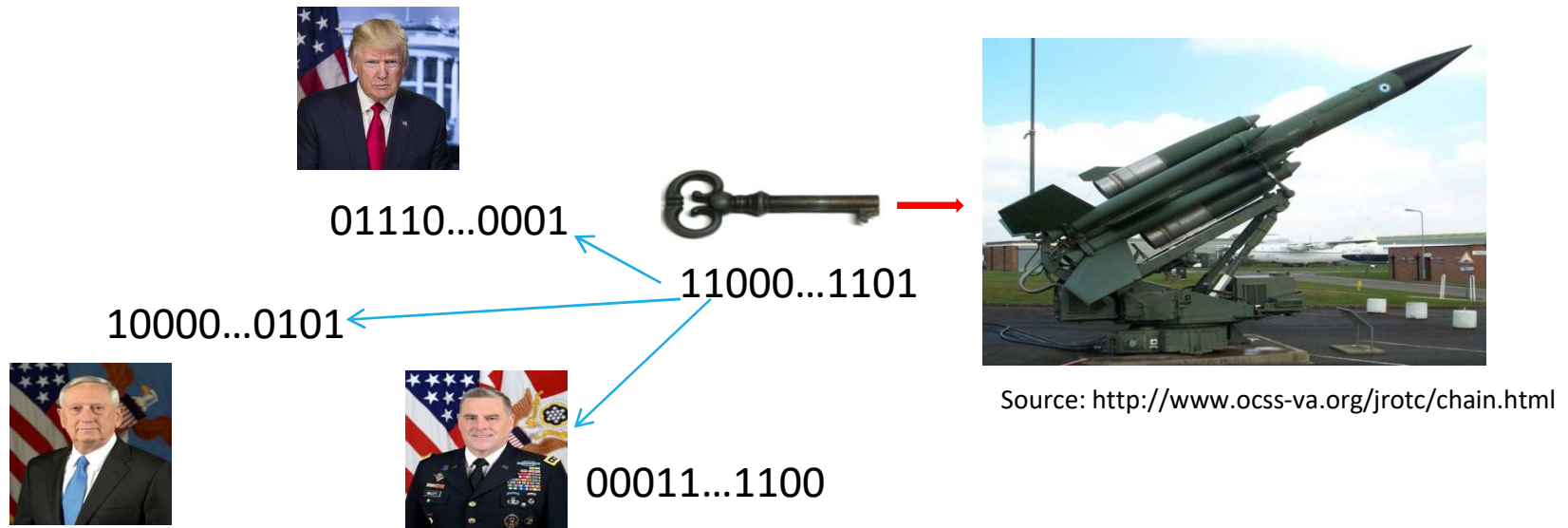
SecureCScaling:

Secure Cloud-based Image/Video Scaling

- Architecture and Workflow



Cryptosystem - Shamir's Secret Sharing

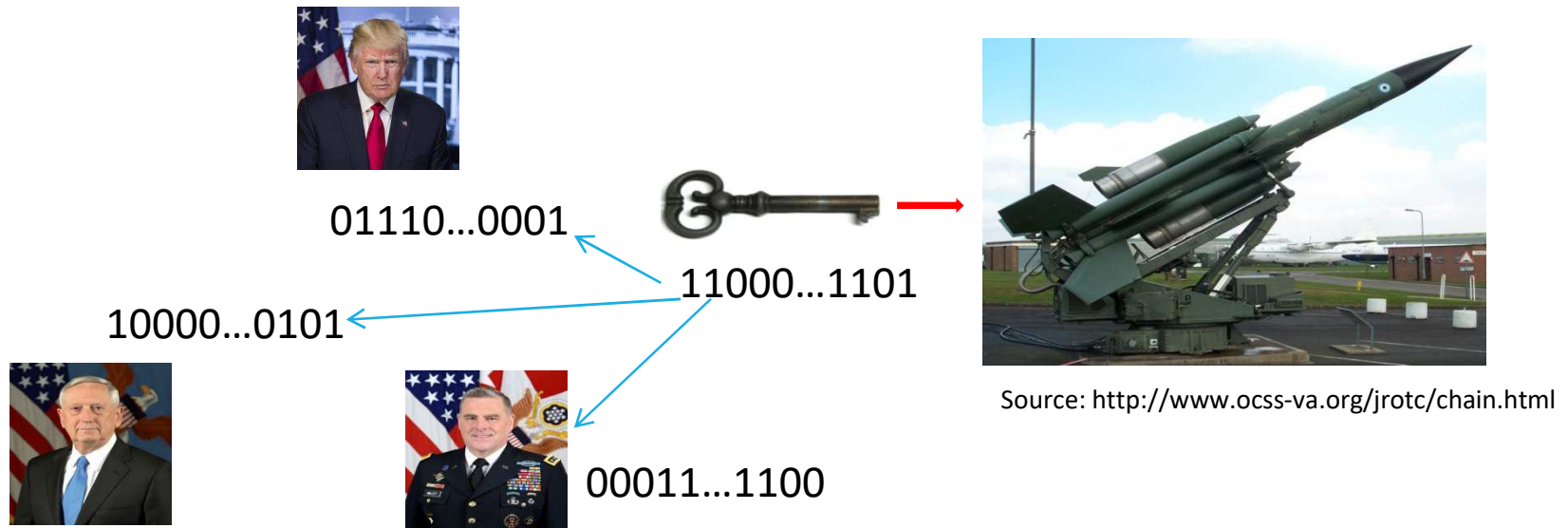


Sharing a Secret

$$F(x) = (\underset{\substack{\downarrow \\ \text{Secret}}}{S} + \sum_{i=1}^{k-1} \underset{\substack{\downarrow \\ \text{Random} \\ \text{Number}}}{a_i} x^i) \bmod \underset{\substack{\downarrow}}{q}$$

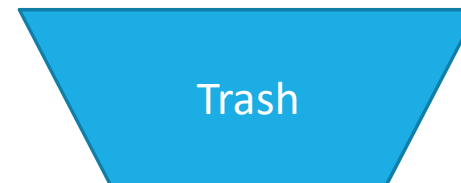


Cryptosystem - Shamir's Secret Sharing

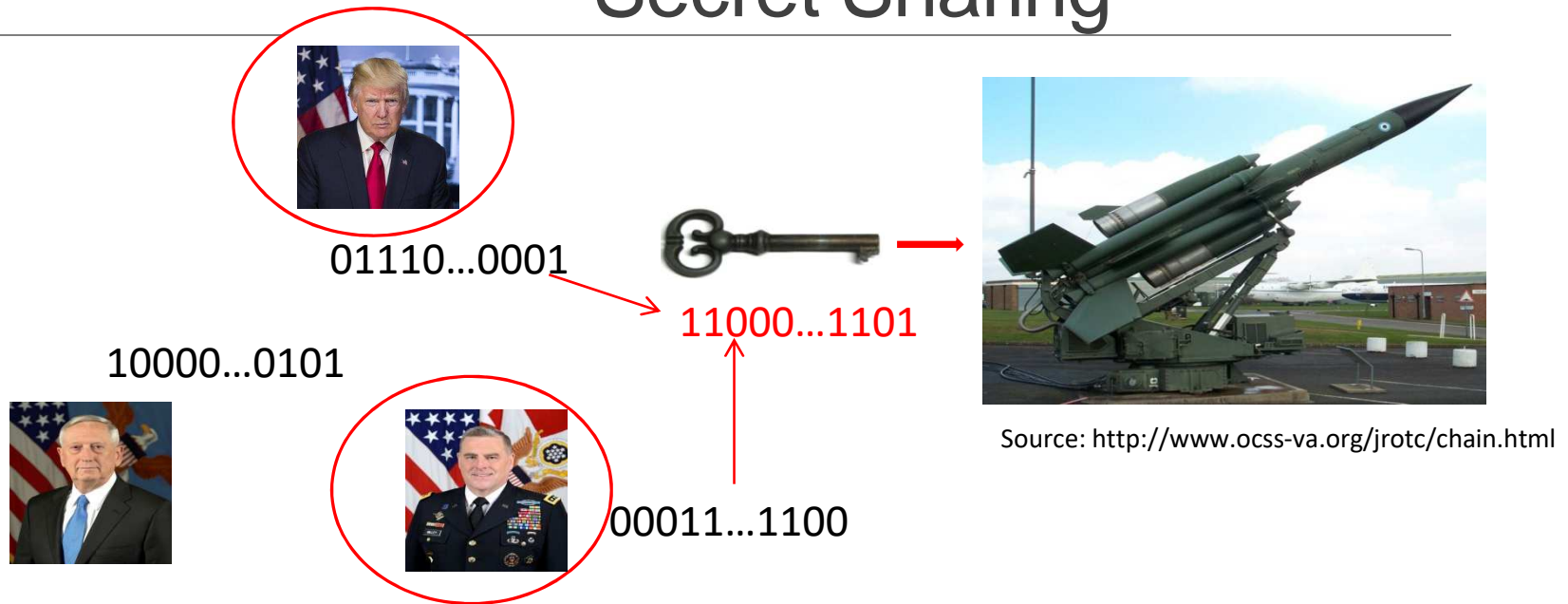


Sharing a Secret

$$F(x) = (\underset{\substack{\downarrow \\ \text{Secret}}}{S} + \sum_{i=1}^{k-1} \underset{\substack{\downarrow \\ \text{Random} \\ \text{Number}}}{a_i} x^i) \bmod \underset{\substack{\downarrow}}{q}$$



Cryptosystem - Shamir's Secret Sharing



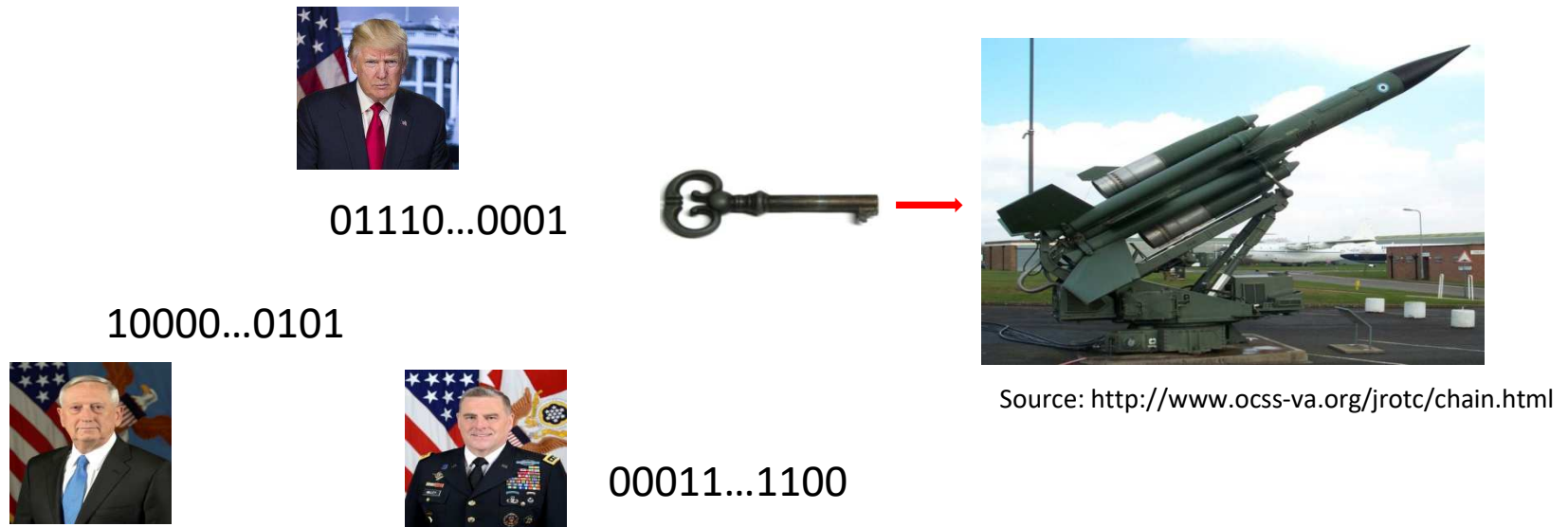
Reconstructing a Secret

$$L(x) = \left(\sum_{i=0}^{k-1} F(i) t_i(x) \right) \bmod q$$

i^{th} Share

$$\prod_{j=0, j \neq i}^{k-1} \frac{x - x_j}{x_i - x_j}$$

Cryptosystem - Shamir's Secret Sharing

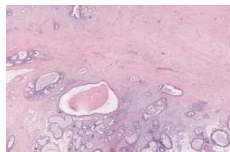


Homomorphic property: $E(A) \circ E(B) = E(A \circ B)$

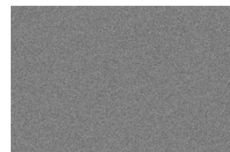
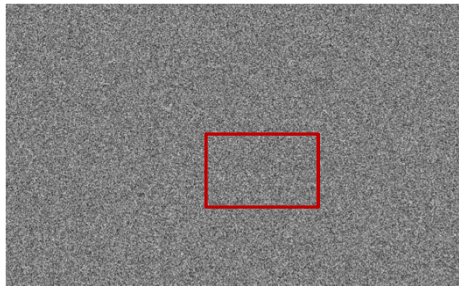
\circ : +, -, *, /, |

SecureCScale: Secure Cloud-based Image Scaling

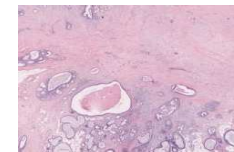
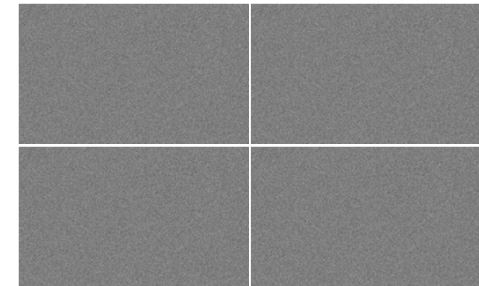
- Results: Scaling



Required



Zoomed Shadow
Image

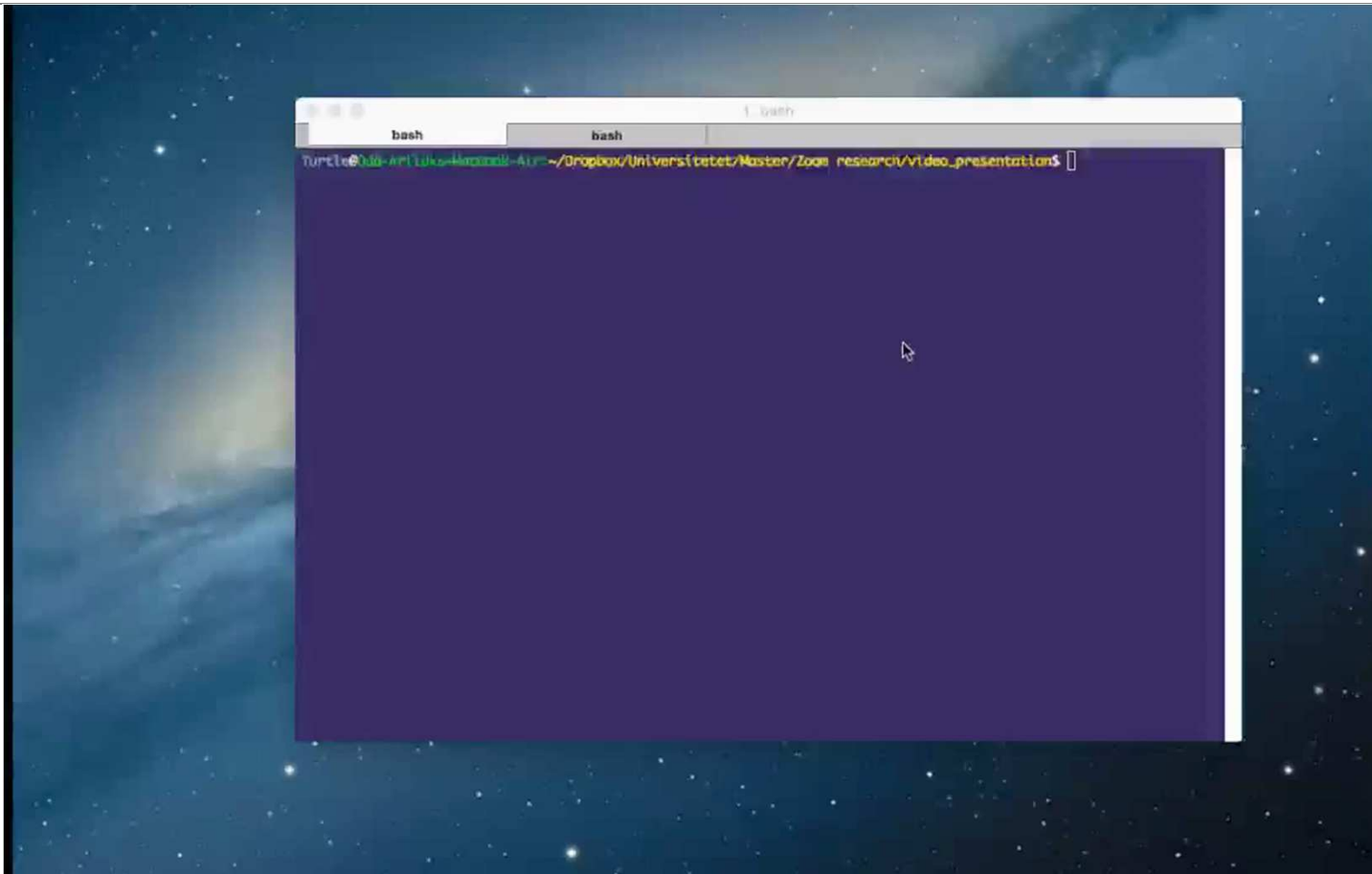


Recovered Zoomed
Image

M. Mohanty, W.-T. Ooi and P. K. Atrey. [Scale me, crop me, know me not: Supporting scaling and cropping in secret image sharing](#). *IEEE International Conference on Multimedia and Expo (ICME'2013)*, July 15-19, 2013, San Jose, CA, USA.



SecureCScaling: Secure Cloud-based Video Scaling



O.-A. Kristensen, M. Mohanty, and P. K. Atrey. **Don't see me, just edit me: Towards secure cloud-based video editing**. The 11th Annual Symposium on Information Assurance ([ASIA'16](#)) with NYS Cyber Security Conference, pp 74-78, June 2016, Albany, NY, USA.



SecureCTask

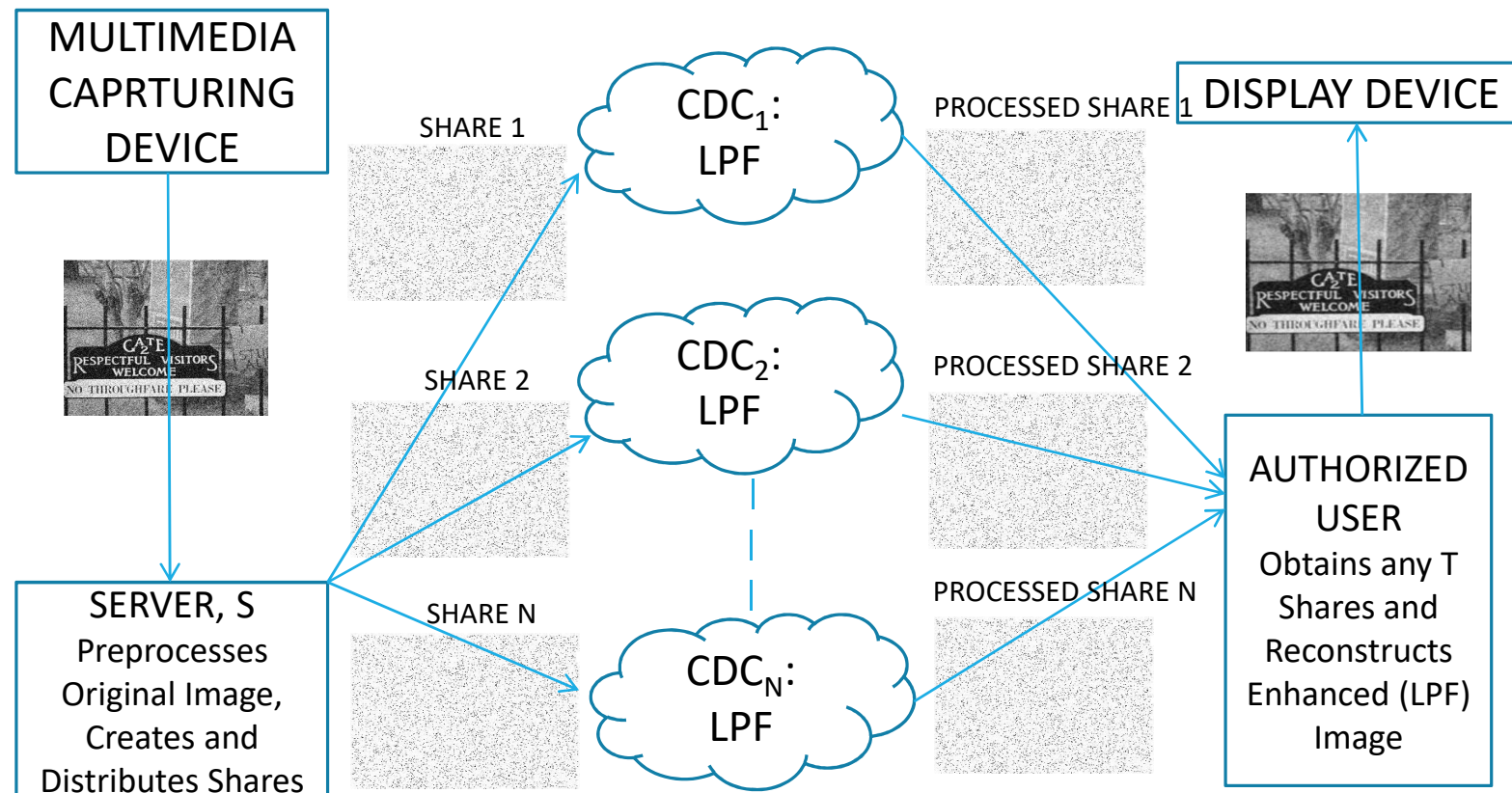
- SecureCScaling
 - Secure Cloud-based Image/Video Scaling
- **SecureCEnhance**
 - **Secure Cloud-based Image/Audio Enhancement**
- SecureCMail
 - Secure Cloud-based Emailing
- SecureCMerge
 - Secure Cloud-based PDF merging
- SecureCEdit
 - Secure Cloud-based Document Editing
- SecureCDedup
 - Secure Cloud-based Data Deduplication



SecureCEnhance:

Encrypted-domain Image Quality Enhancement over Cloud

Architecture and Workflow



A. Lathey, P. K. Atrey and N. Joshi. **Homomorphic low pass filtering on encrypted multimedia over cloud**. *IEEE International Conference on Semantic Computing (ICSC'2013)*, September 2013, Irvine, CA, USA.



SecureCEnhance:

Encrypted-domain Image Quality Enhancement over Cloud

The proposed method is demonstrated to work for

- Noise removal and anti-aliasing
 - Results – Scheme 1 ([Demo](#))
 - Results – Scheme 2 ([Demo](#))
- Edge and contrast enhancement ([Demo](#))
- Dehazing ([Demo](#))

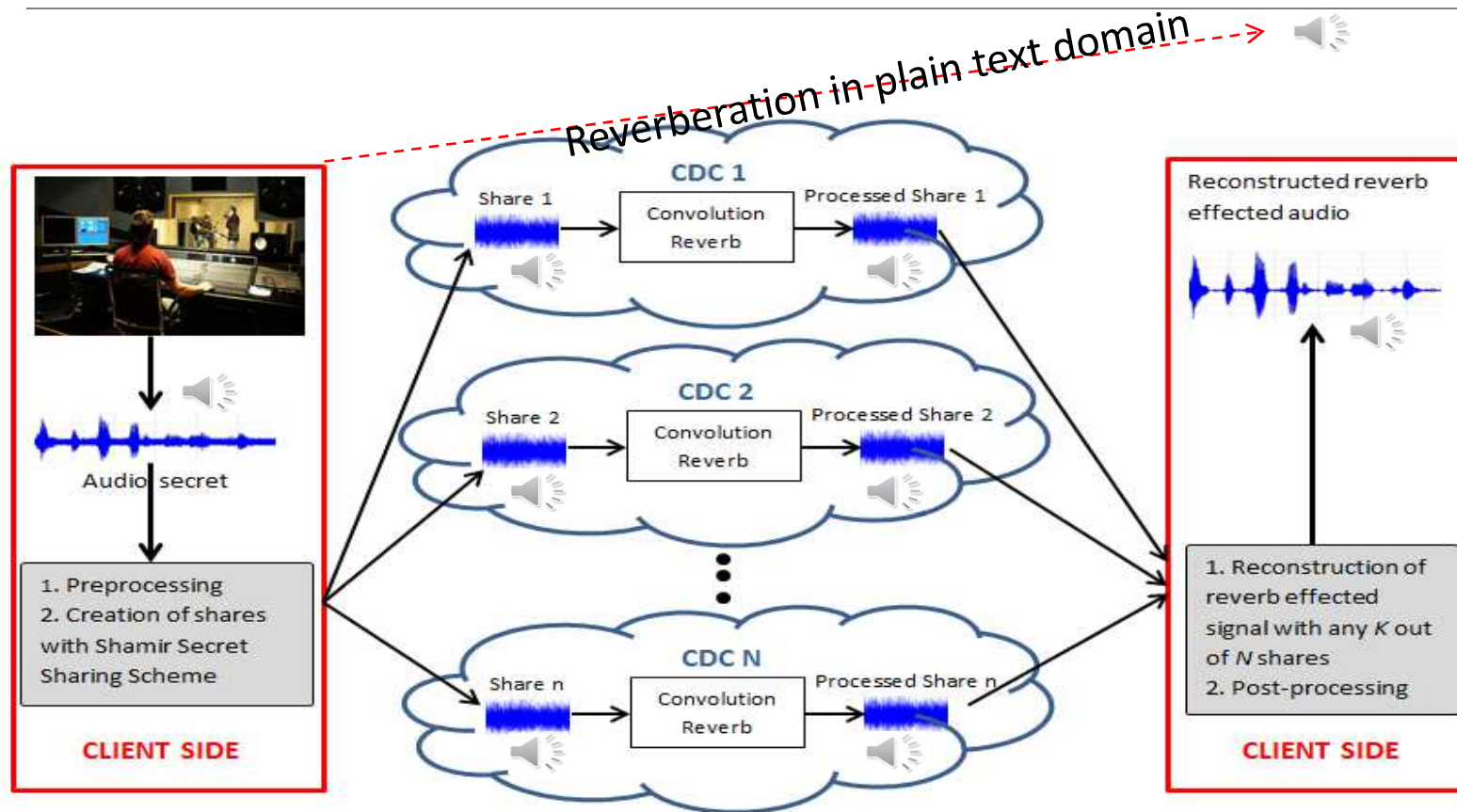
More demos available on:

- <https://sites.google.com/site/ankitaresearchdemos/home>

A. Lathey and P. K. Atrey. [Image enhancement in encrypted domain over cloud](#). *ACM Transactions on Multimedia, Computing, Communications and Applications*, January 2015.

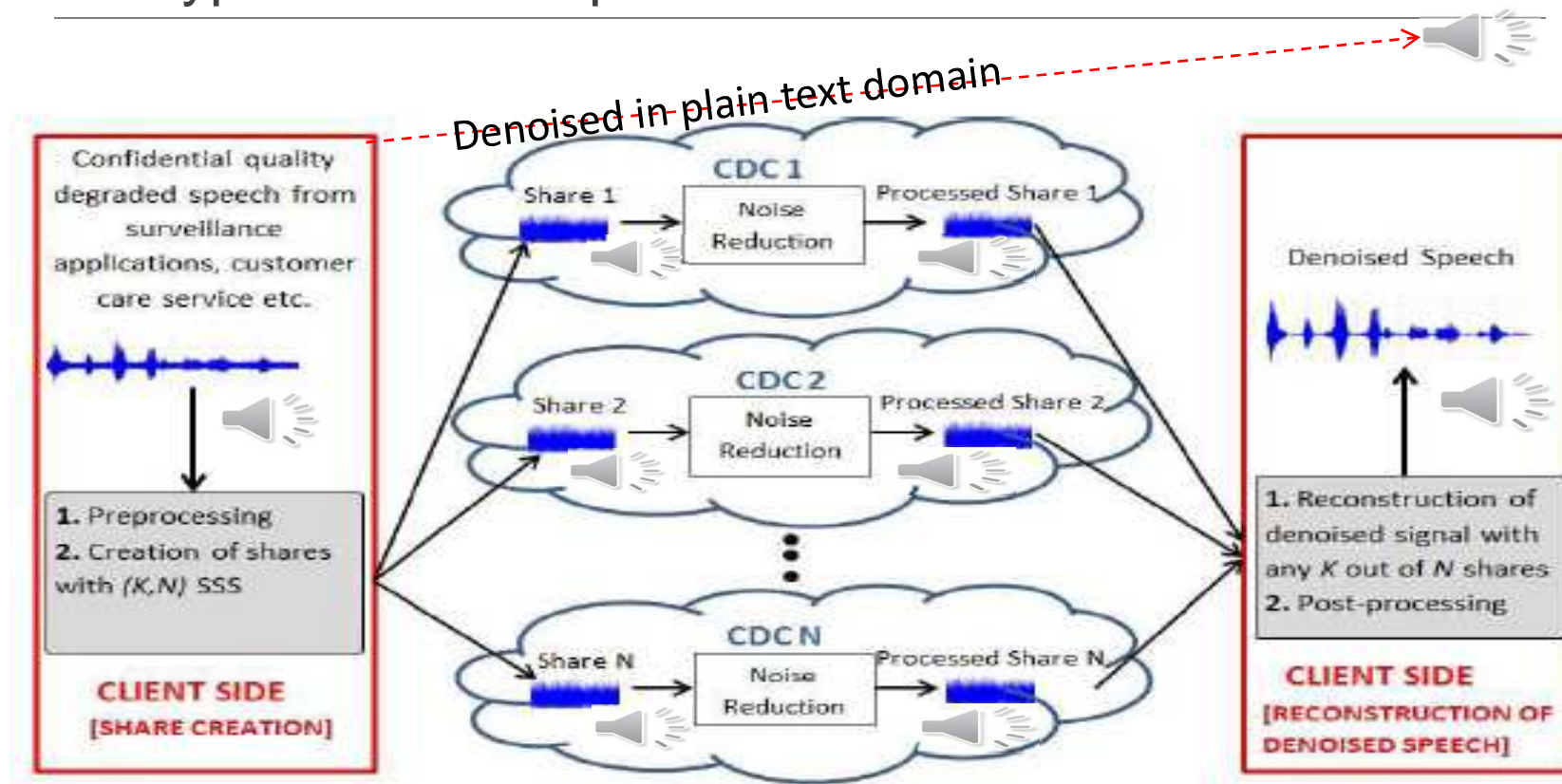


SecureCEnhance: Encrypted-domain Audio Reverberation over Cloud



A. Yakubu, N. Maddage and P. K. Atrey. [Secure audio reverberation over cloud](#). *The 10th International Symposium on Information Assurance (ASIA'15) with NYS Cyber Security Conference*, pp 39-43, June 2015, Albany, NY, USA.

SecureCEnhance: Encrypted-domain Speech Noise Reduction over Cloud



- A. Yakubu, N. Maddage and P. K. Atrey. [Encrypted domain cloud-based speech noise reduction](#). *The 1st International Workshop on Privacy in Multimedia (PIM'16) with ICME'16*, July 2016, Seattle, WA, USA.

- A. Yakubu, N. Maddage and P. K. Atrey. [Securing speech noise reduction in outsourced environment](#). *ACM Transactions on Multimedia Computing, Communication and Applications*. Vol. 13, No. 4, Article 51, August (2017).

SecureCTask

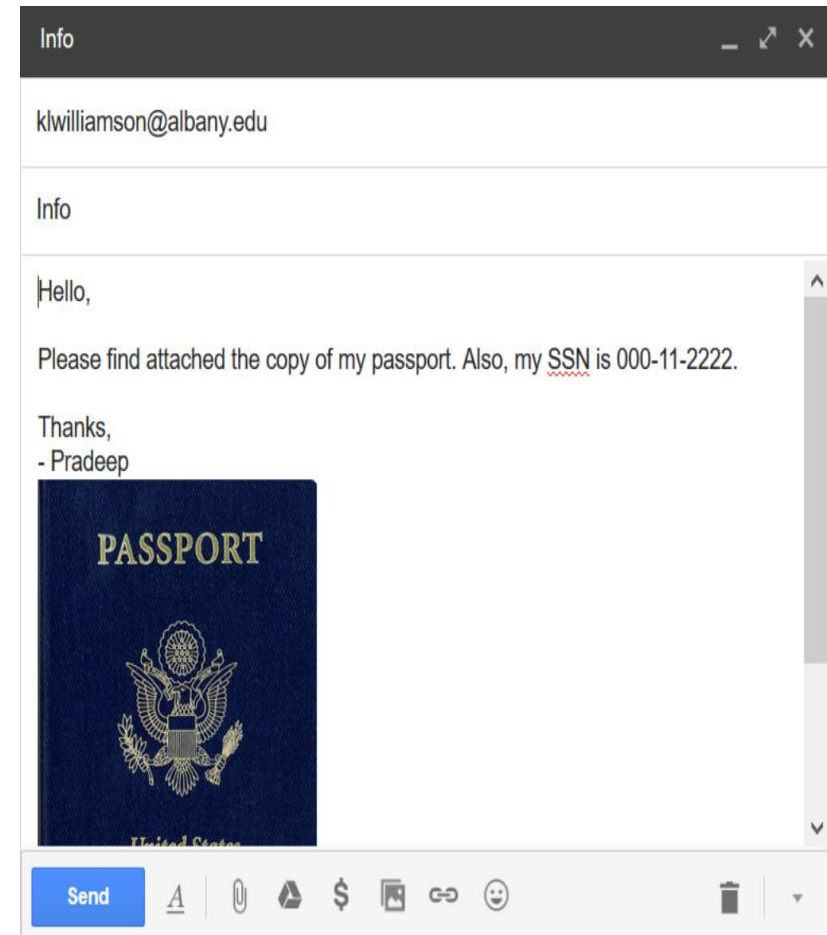
- SecureCScaling
 - Secure Cloud-based Image/Video Scaling
- SecureCEnhance
 - Secure Cloud-based Image/Audio Enhancement
- **SecureCMail**
 - **Secure Cloud-based Emailing**
- SecureCMerge
 - Secure Cloud-based PDF merging
- SecureCEdit
 - Secure Cloud-based Document Editing
- SecureCDedup
 - Secure Cloud-based Data Deduplication

SecureCMail:

Securing Emails from Service Providers using Secret Sharing

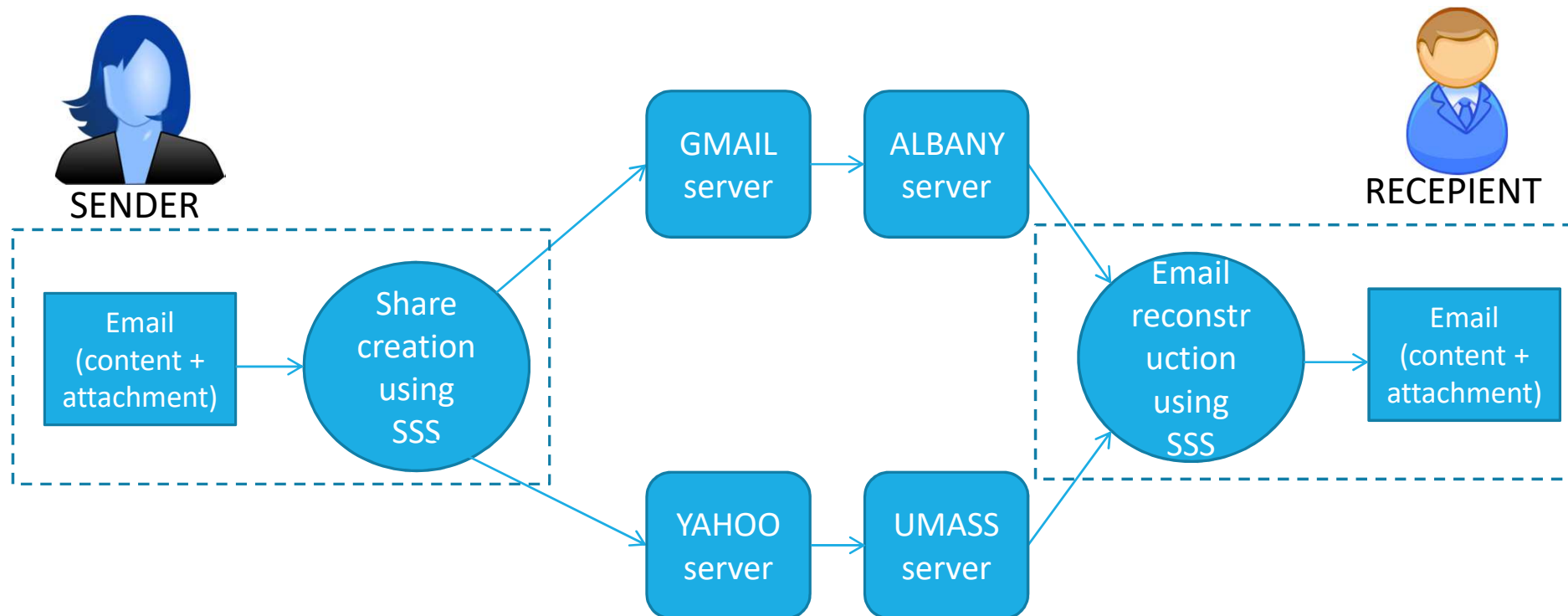
Have you ever sent
any confidential
information such as
passport and SSN
over email?

Gmail now has more than 1 billion
monthly active users – **Alarming?**



SecureCMail:

Securing Emails from Service Providers using Secret Sharing

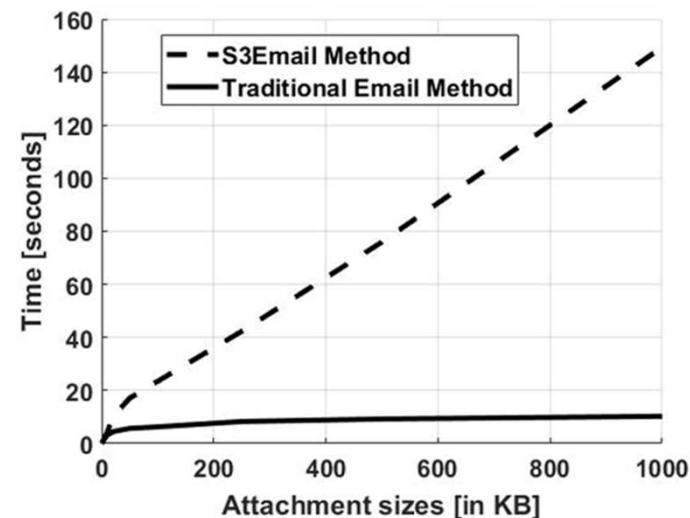
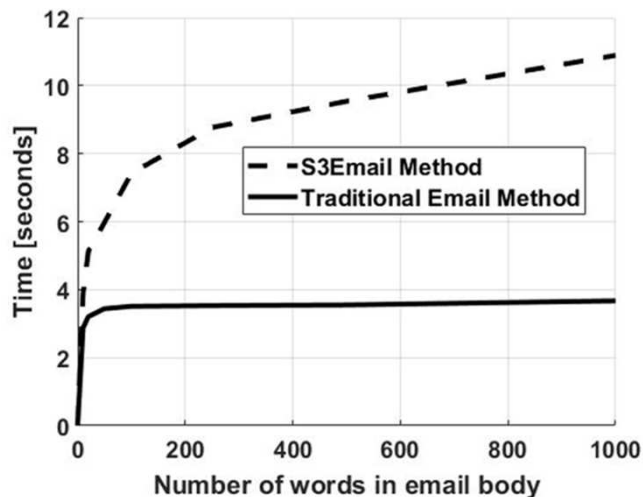


P. Singh, S. Arora, K. Williamson and P. K. Atrey. **S3Email: A method for securing emails from service providers**. *The 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC'2017)*, Banff, Canada, October 2017.

SecureCMail:

Securing Emails from Service Providers using Secret Sharing

Demo: <http://www.screencast.com/t/NiURJXpZdL1>



P. Singh, S. Arora, K. Williamson and P. K. Atrey. **S3Email: A method for securing emails from service providers**. The 2017 IEEE International Conference on Systems, Man, and Cybernetics ([SMC'2017](#)), Banff, Canada, October 2017.



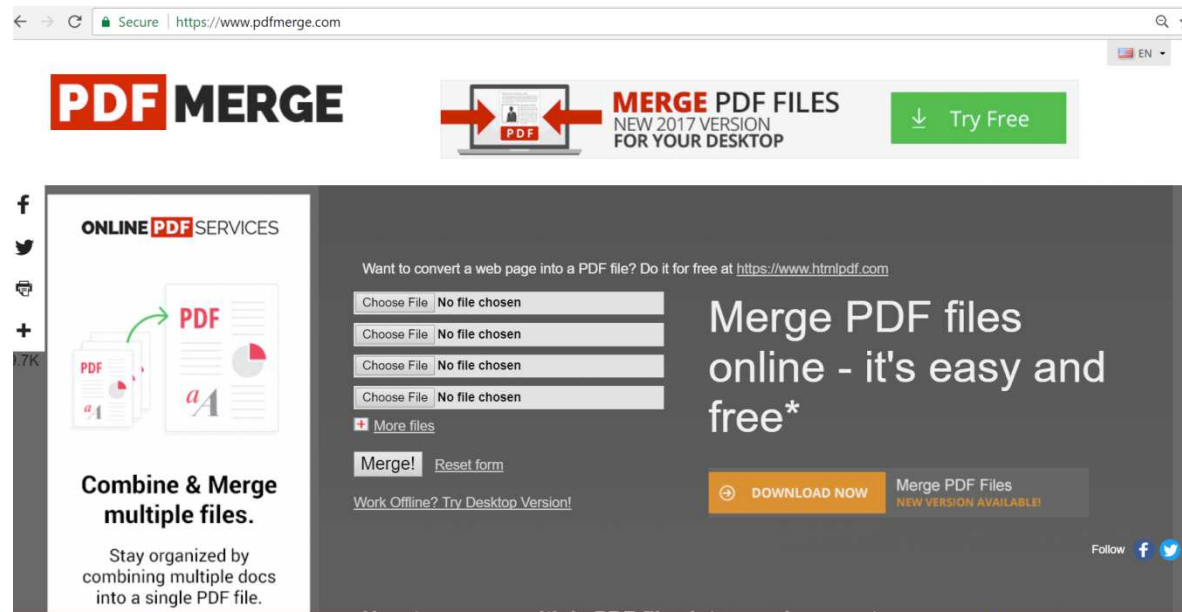
SecureCTask

- SecureCScaling
 - Secure Cloud-based Image/Video Scaling
- SecureCEnhance
 - Secure Cloud-based Image/Audio Enhancement
- SecureCMail
 - Secure Cloud-based Emailing
- **SecureCMerge**
 - **Secure Cloud-based PDF merging**
- SecureCEdit
 - Secure Cloud-based Document Editing
- SecureCDedup
 - Secure Cloud-based Data Deduplication



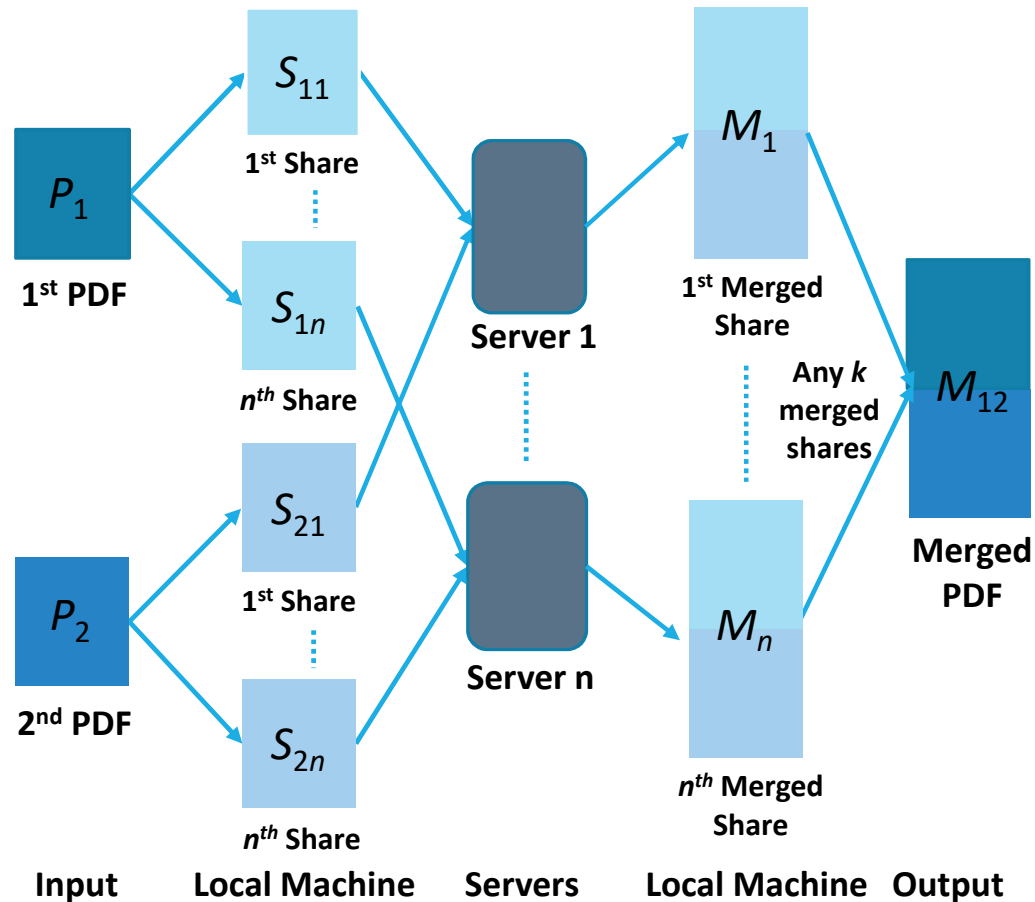
SecureCMerge: Secure Online PDF Merging

Have you ever merged two pdf files using online merge tools?

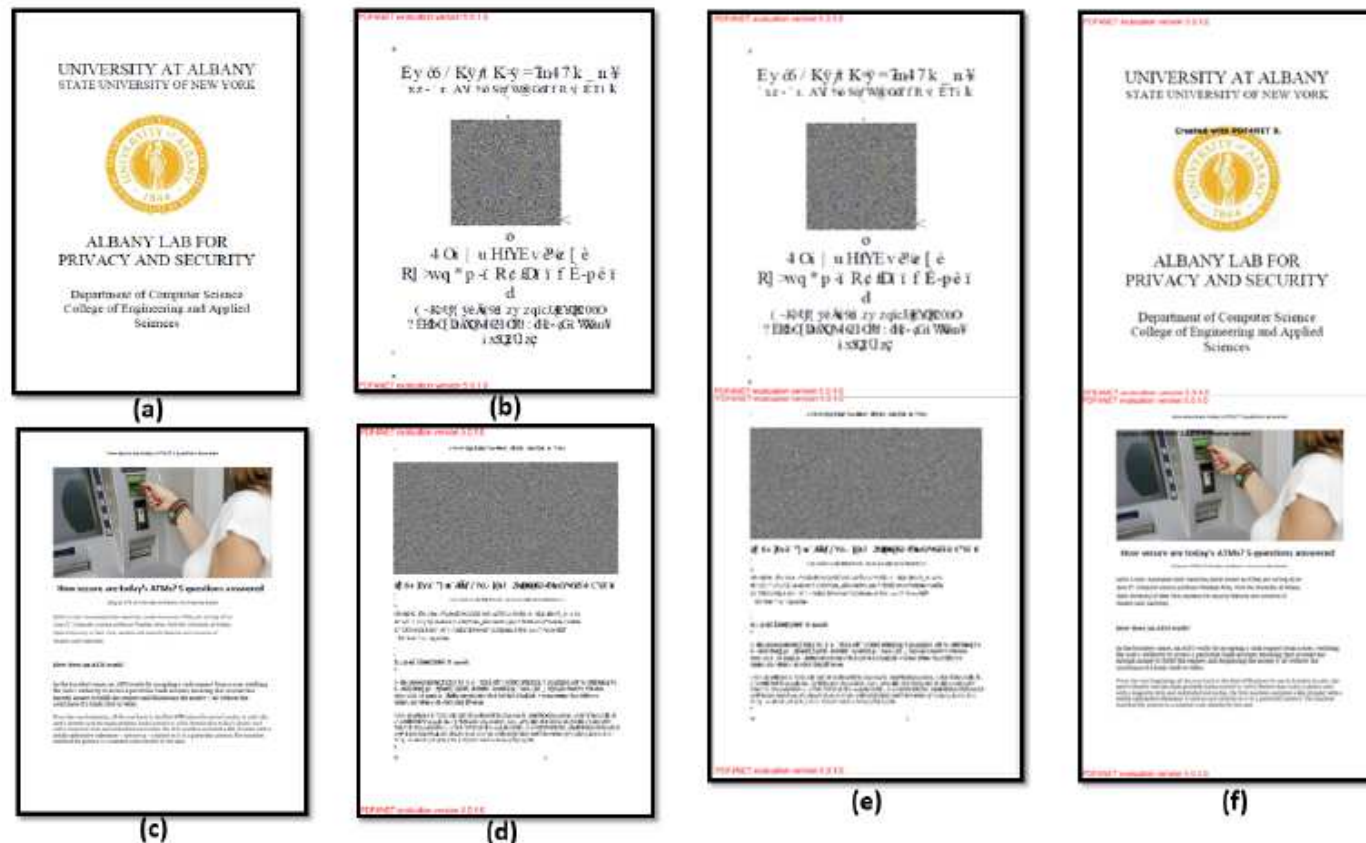


Can they see your documents? YES

SecureCMerge: Secure Online PDF Merging



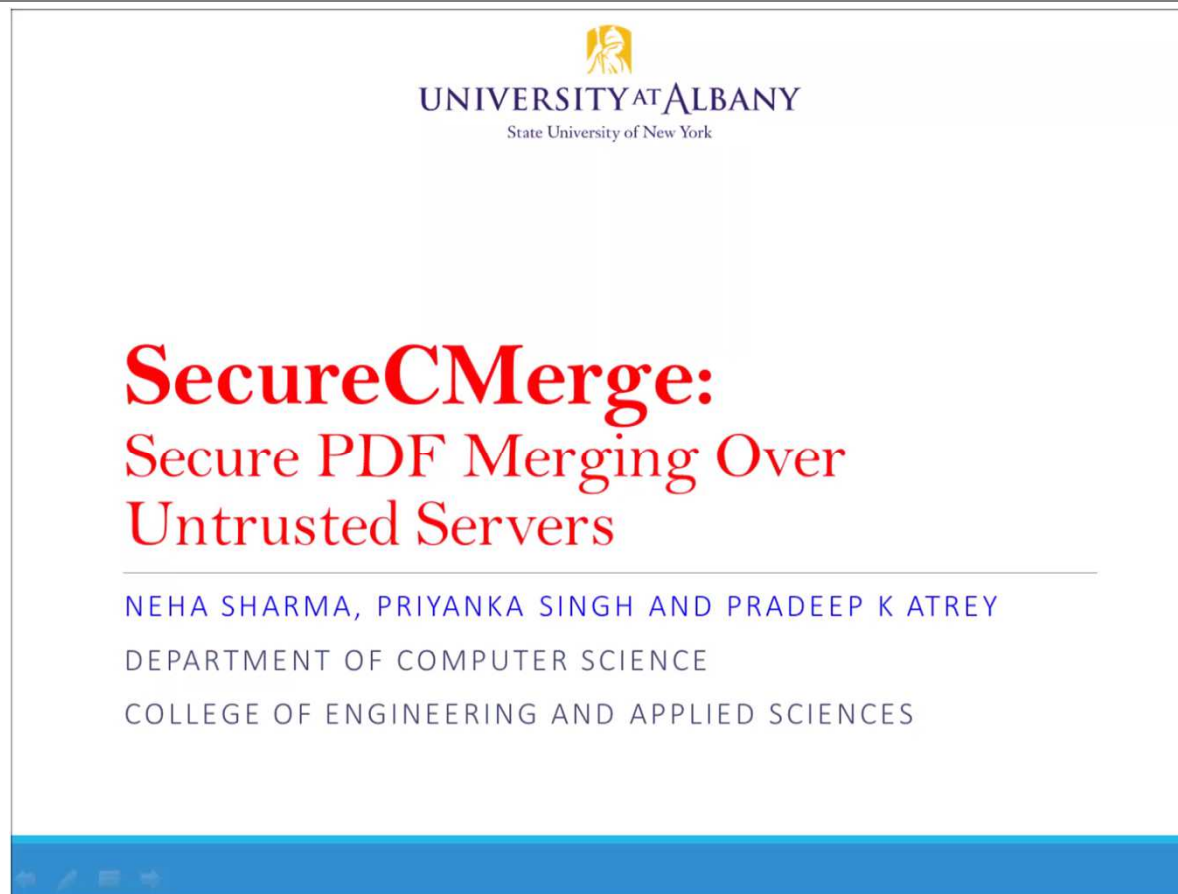
SecureCMerge: Secure Online PDF Merging



N. Sharma, P. Singh and P. K. Atrey. [SecureCMerge: Secure PDF Merging over Untrusted Servers](#). *IEEE Int. Conf. on Multimedia Information Processing and Retrieval (MIPR) 2018, Miami, USA (Accepted)*



SecureCMerge: Secure Online PDF Merging



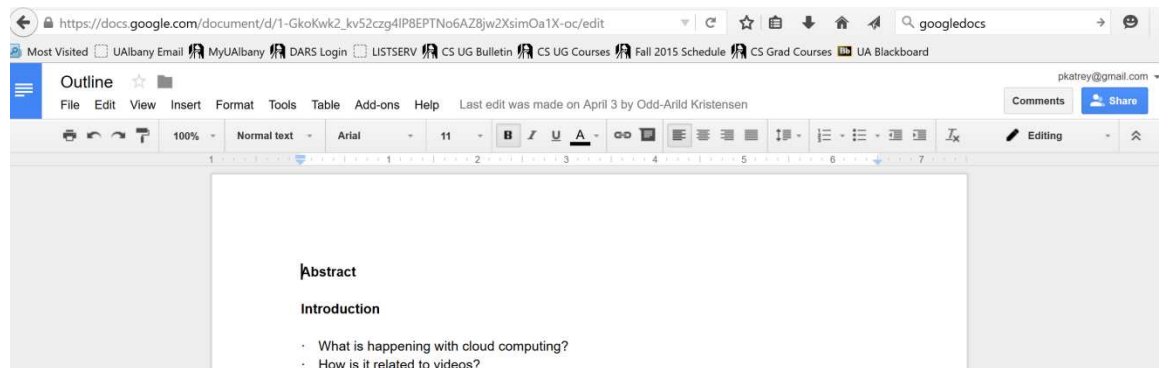
N. Sharma, P. Singh and P. K. Atrey. [SecureCMerge: Secure PDF Merging over Untrusted Servers](#). *IEEE Int. Conf. on Multimedia Information Processing and Retrieval (MIPR) 2018, Miami, USA (Accepted)*

SecureCTask

- SecureCScaling
 - Secure Cloud-based Image/Video Scaling
- SecureCEnhance
 - Secure Cloud-based Image/Audio Enhancement
- SecureCMail
 - Secure Cloud-based Emailing
- SecureCMerge
 - Secure Cloud-based PDF merging
- **SecureCEdit**
 - **Secure Cloud-based Document Editing**
- SecureCDedup
 - Secure Cloud-based Data Deduplication

SecureCEdit: Secure Online Document Editing

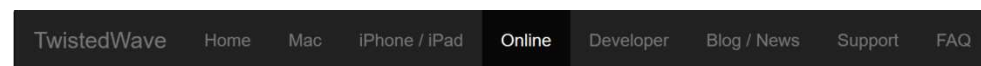
- Google Docs: Are they secure?



- Online image editing



- Online Audio Editor



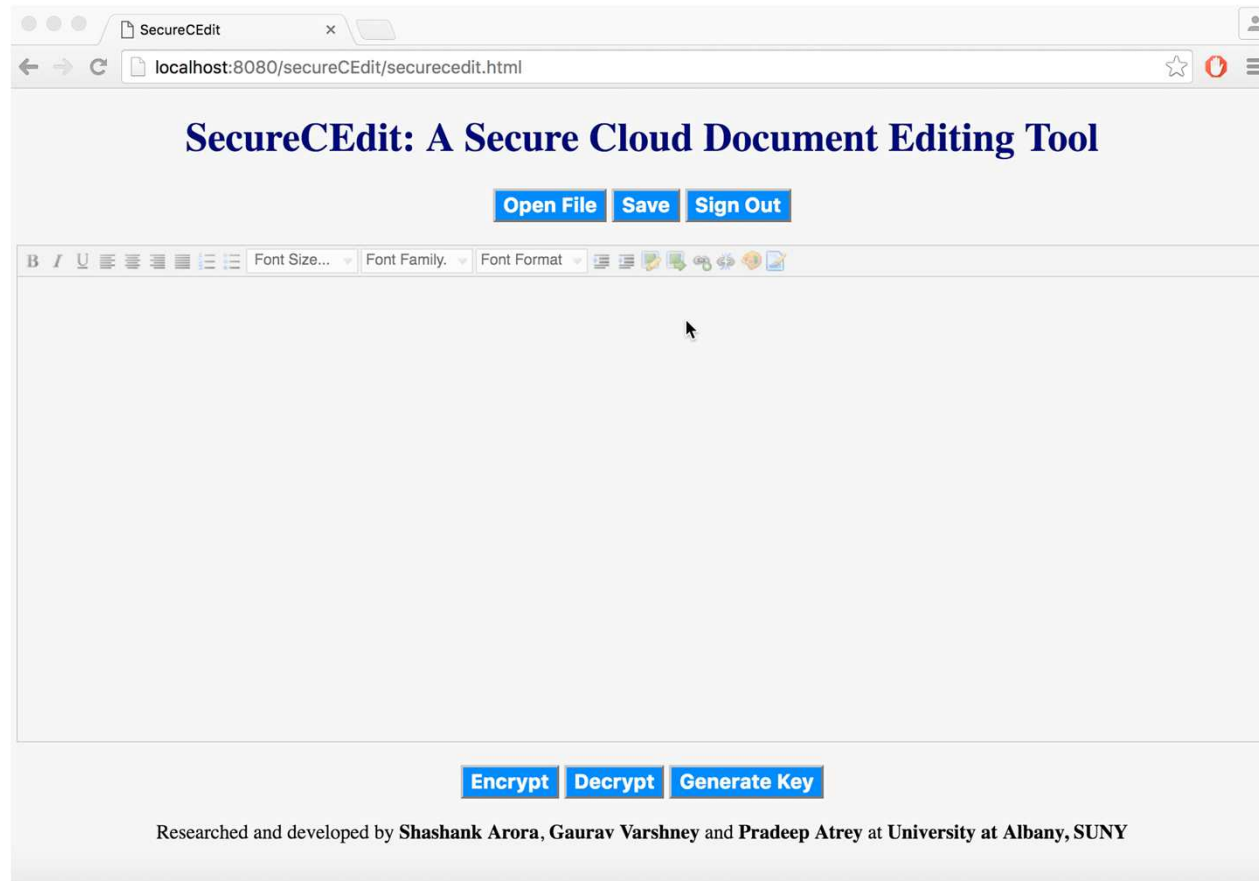
TWISTEDWAVE

TwistedWave Online

A browser-based audio editor



SecureCEdit: Secure Online Document Editing



Key Generation:

$$k_i = (s_{1i} + s_{2i} + s_{3i}) \bmod 256$$

s_1 : The application key,

s_2 : Cloud storage key

s_3 : User specified key

Further Issues:

- Secure Collaborative Editing
- Secure Concurrent Access

S. Arora, G. Varshney, P. K. Atrey and M. Mishra. [SecureCEdit: An approach for secure cloud-based document editing](#).

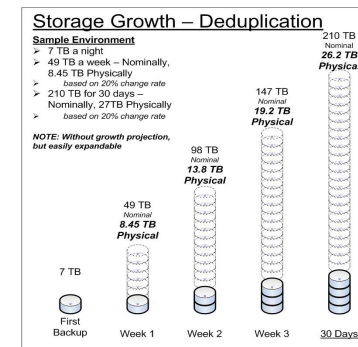
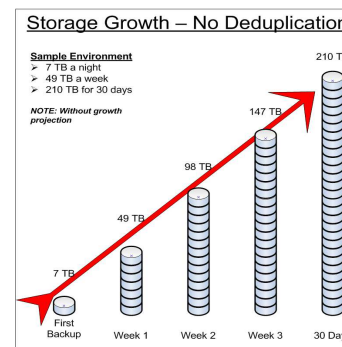
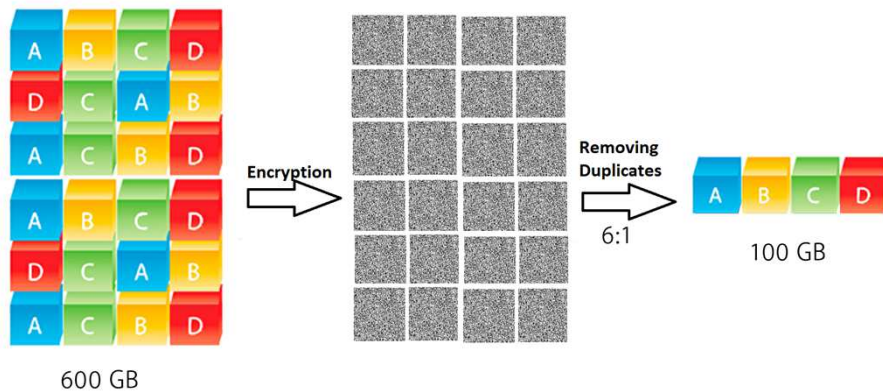
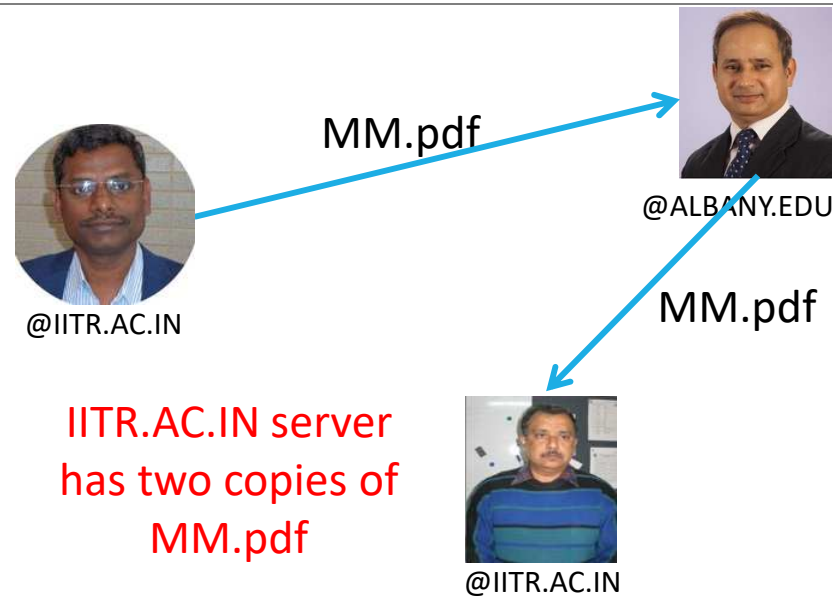
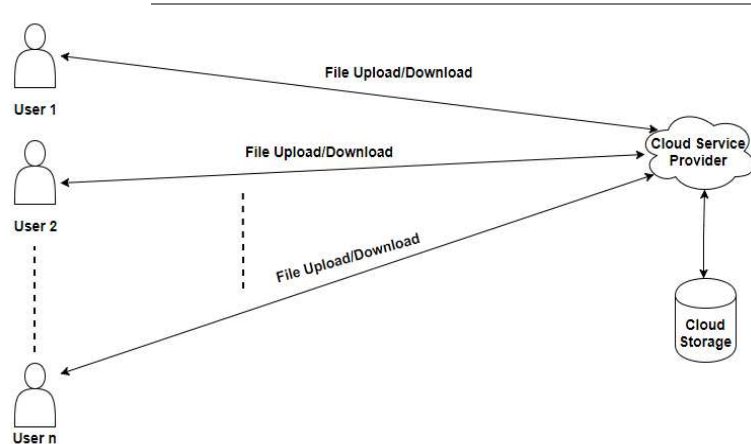
The 2nd International Workshop on Security and Privacy in the Cloud (SPC'16) with IEEE CNS'16, Philadelphia, USA

SecureCTask

- SecureCScaling
 - Secure Cloud-based Image/Video Scaling
- SecureCEnhance
 - Secure Cloud-based Image/Audio Enhancement
- SecureCMail
 - Secure Cloud-based Emailing
- SecureCMerge
 - Secure Cloud-based PDF merging
- SecureCEdit
 - Secure Cloud-based Document Editing
- **SecureCDedup**
 - **Secure Cloud-based Data Deduplication**

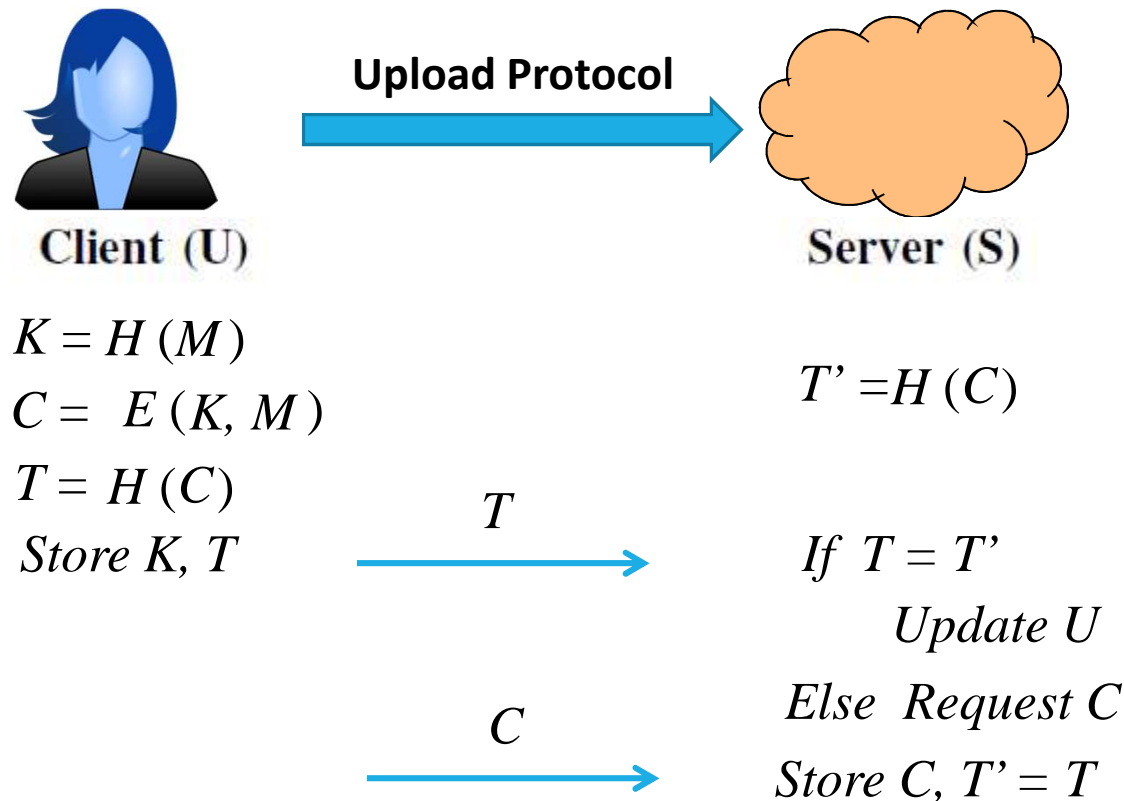


SecureCDedup: Secure Cloud-based Data Deduplication



SecureCDedup: Secure Cloud-based Data Deduplication

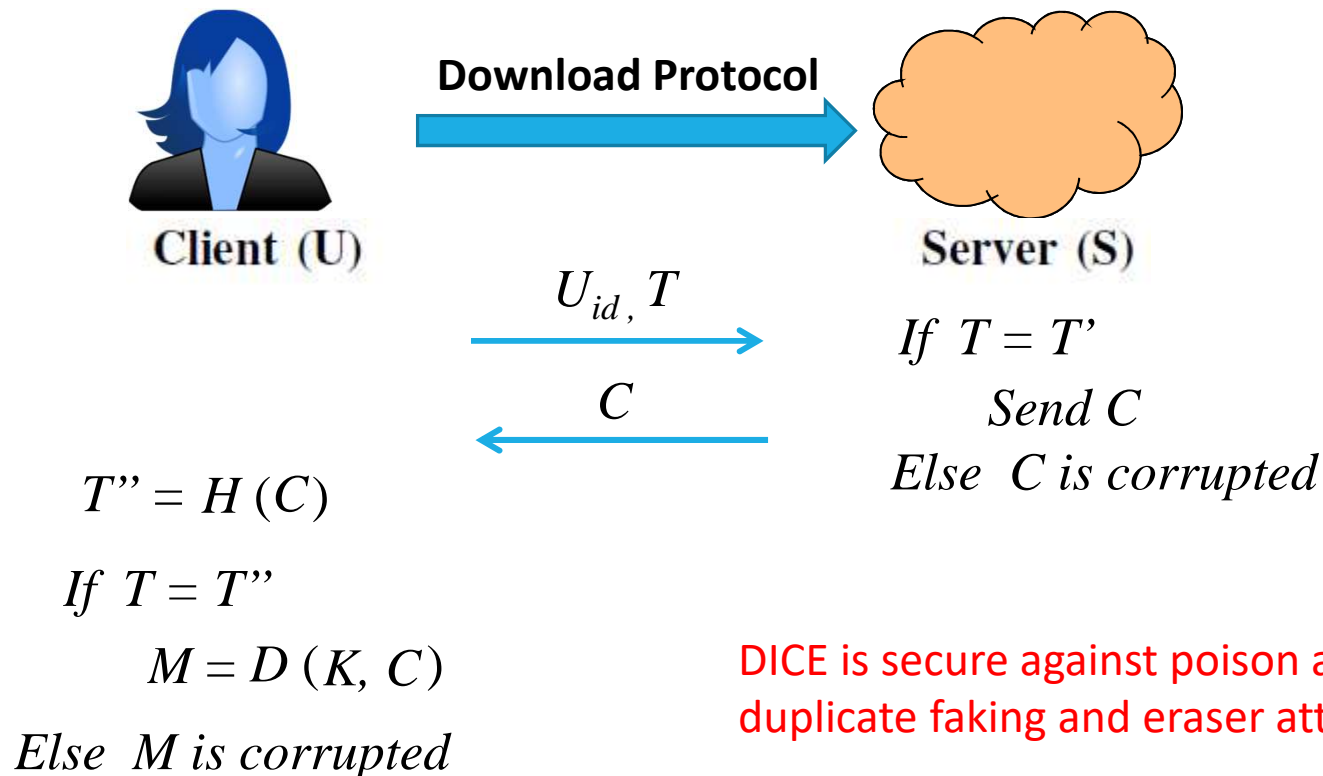
Dual Integrity Convergent Encryption (DICE) Protocol



A. Agarwala, P Singh and P. K. Atrey. [DICE: A dual integrity convergent encryption protocol for client side secure data deduplication](#). The 2017 IEEE International Conference on Systems, Man, and Cybernetics ([SMC'2017](#)), Banff, Canada, October 2017.

SecureCDedup: Secure Cloud-based Data Deduplication

Dual Integrity Convergent Encryption (DICE) Protocol

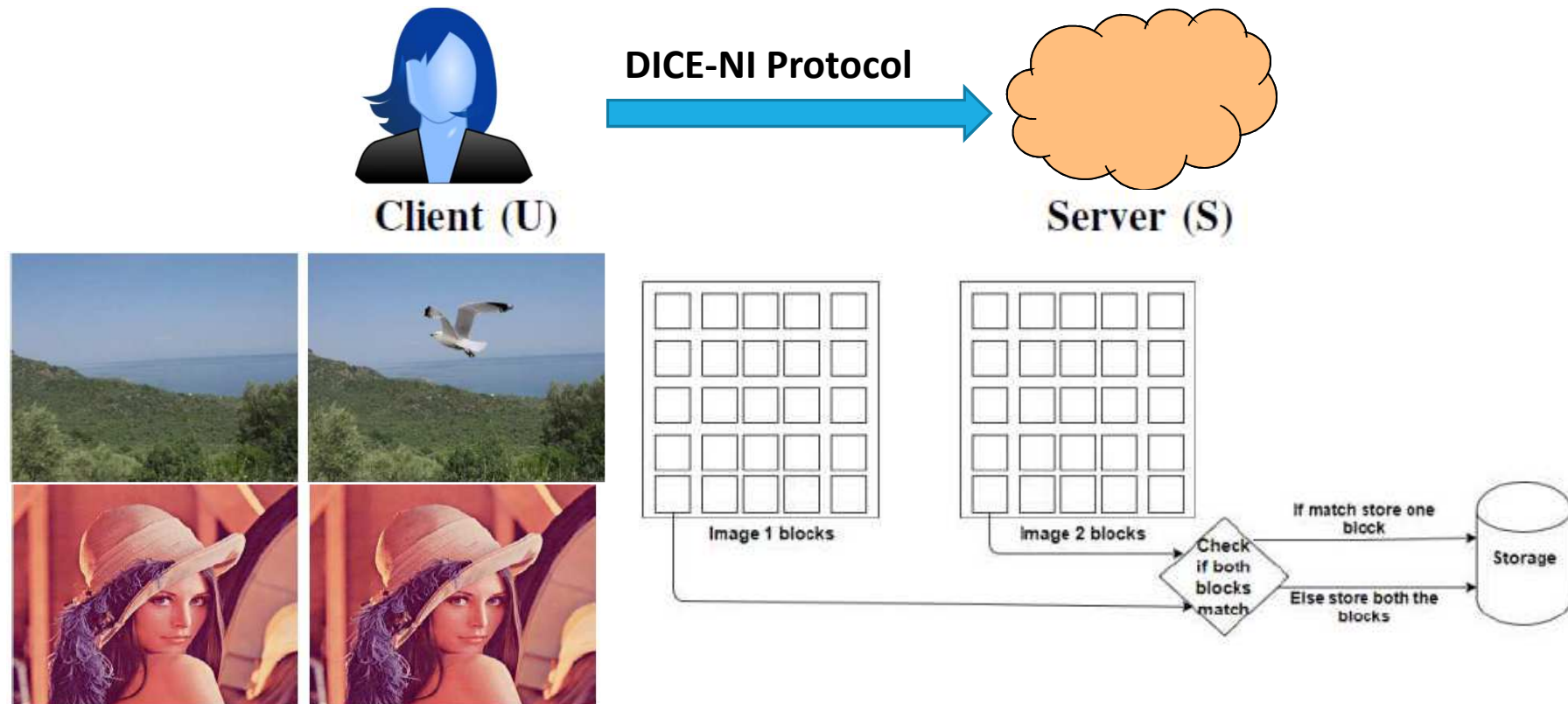


DICE is secure against poison attack (i.e. duplicate faking and eraser attacks)

A. Agarwala, P Singh and P. K. Atrey. [DICE: A dual integrity convergent encryption protocol for client side secure data deduplication](#). The 2017 IEEE International Conference on Systems, Man, and Cybernetics ([SMC'2017](#)), Banff, Canada, October 2017.

SecureCDedup: Secure Cloud-based Data Deduplication

DICE Protocol for Near-Identical (NI) Images



A. Agarwala, P Singh and P. K. Atrey. [Client Side Image Data Deduplication Using DICE Protocol](#). *IEEE Int. Conf. on Multimedia Information Processing and Retrieval (MIPR) 2018, Miami, USA (Accepted)*

What Next?

This is not the end of the world! Encouraging sign 😊

Application area	Analysis tasks	Type of media and features used
Social media and networks	Personality detection	Text, images, video, demographic and social features
	Cyber bullying detection	Text and social features
	Spending behavior analysis	Text, social features
	Disease spread detection	Text, social features
Multimedia surveillance	Hate posts detection	Text, audio, images, video and social features
	Face detection and recognition	Image, video
	Suspicious event detection	Image, video
	Data quality improvement	Image, video, audio
	Data search and retrieval	Text, image, video, audio
	Scaling and zooming	Image, video
E-health	3D medical data rendering and visualization	3D data, image
	Scaling and zooming	Image, video
Bio-informatics	DNA sequence analysis	Text and numbers



Thanks to Collaborators



Ankita Lathey



Nishant Joshi



Manoranjan
Mohanty



Wei-Tsang
Ooi



Manoj
Mishra



Gaurav
Varshney



Priyanka
Singh



Kaliel
Williamson



Abukari
Yakubu



Namunu
Maddage



Shashank Arora



Neha Sharma



Ashish Agarwala



THANK YOU

Eυχαριστώ

Asante

Vielen
Dank

Teşekkürler

Hvala

ขอบคุณ

DMnvwd

धन्यवाद

شكراً

Grazie

Bedankt

Gracias

Dankie

go raibh maith agaibh

Köszönettel

Obrigado!

ありがとう !

شكراً

Merci

Díky

谢谢 !

WAD MAHAD

SAN TAHAY

متشكراً
감사합니다

GADDA GUEY

Urakoze

