UNIVERSITY AT ALBANY
State University of New York

SecureCSuite:
Secure Computation over Untrusted Cloud Servers

PRADEEP K ATREY

DEPARTMENT OF COMPUTER SCIENCE

UNIVERSITY AT ALBANY, STATE UNIVERSITY OF NEW YORK

Motivation

Data Per Minute

facebook: 510,000 comments, 293,000 status updates, and 136,000 photos

YouTube: 300 hours of video

204 million emails

twitter: 350,000 tweets

Google: 2.4 million search queries, 12000 GB free Google Drive space

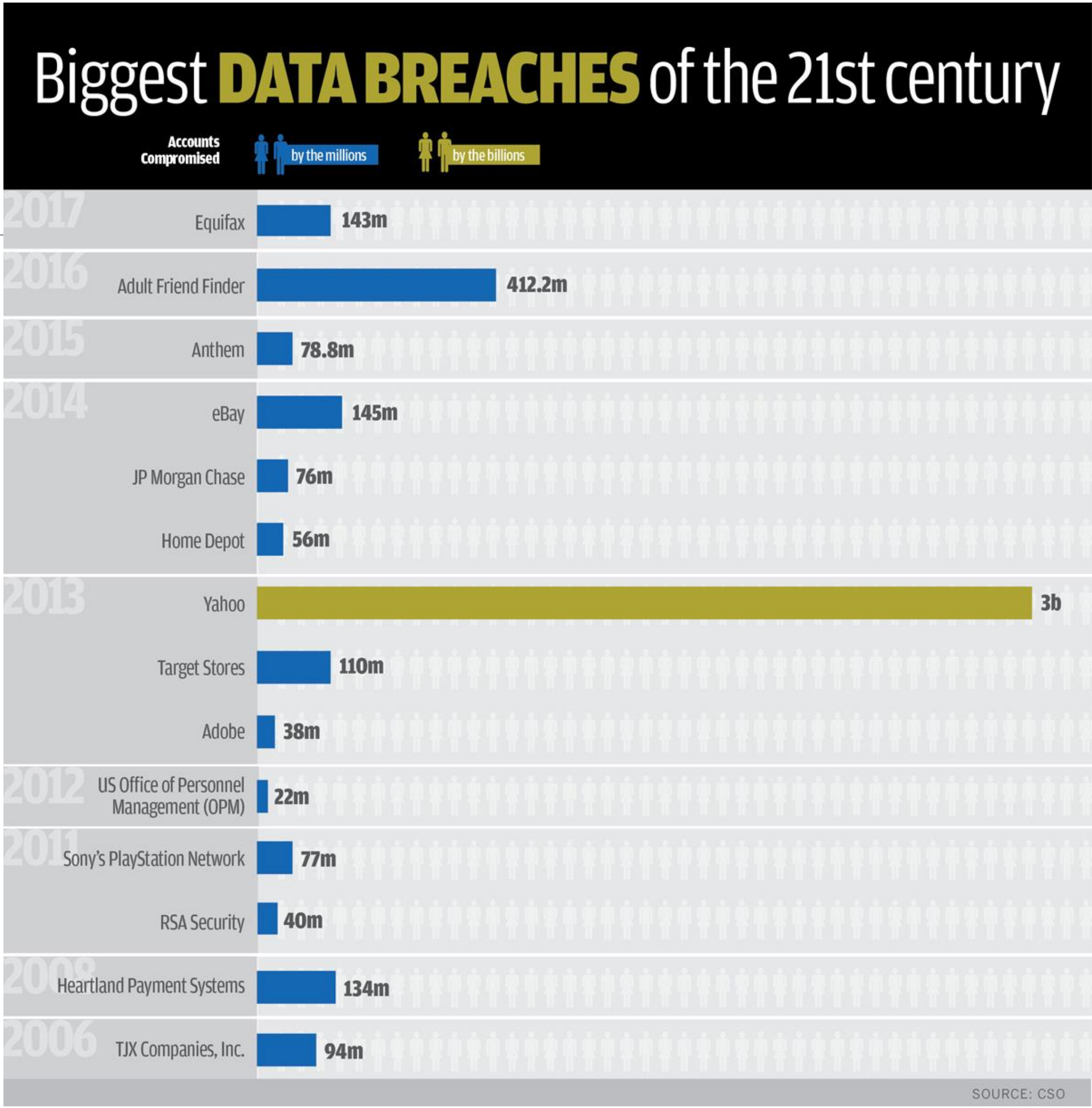
Terabytes of video

Gigabytes of audio data

> 2000 TB

STORAGE
&
PROCESSING

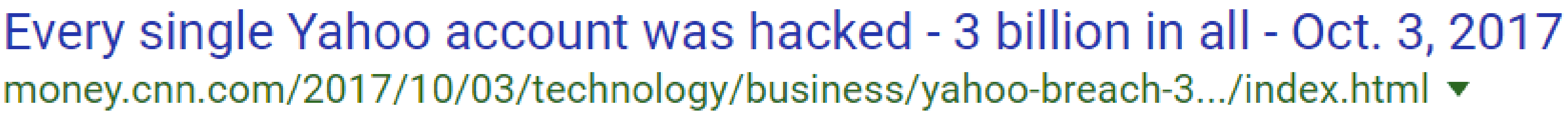
Motivation (cont.)



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

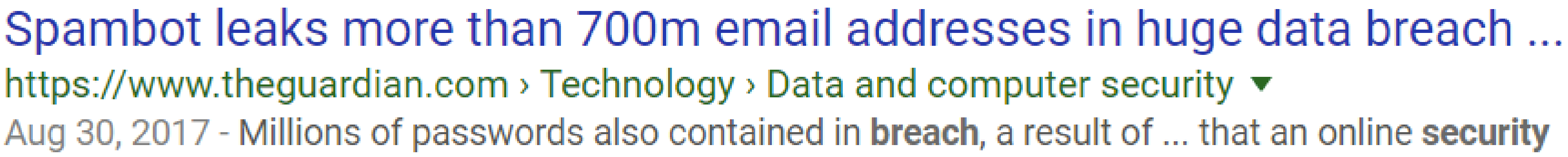
Motivation (cont.)

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

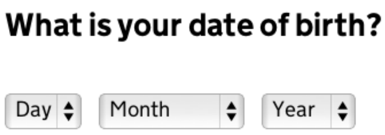
Passport

Enrollee Name
FIRST M LASTNAME JR
Enrollee ID
DZW920000000
Issuer (80840)
9101003777
RxBIN 004336
RxGrp RX4655

Health Policy Card

5424 1801 2345 6789
Valid from 01/14
Expiration date 12/31/16
L WALKER
08

Credit Card



What is your date of birth?

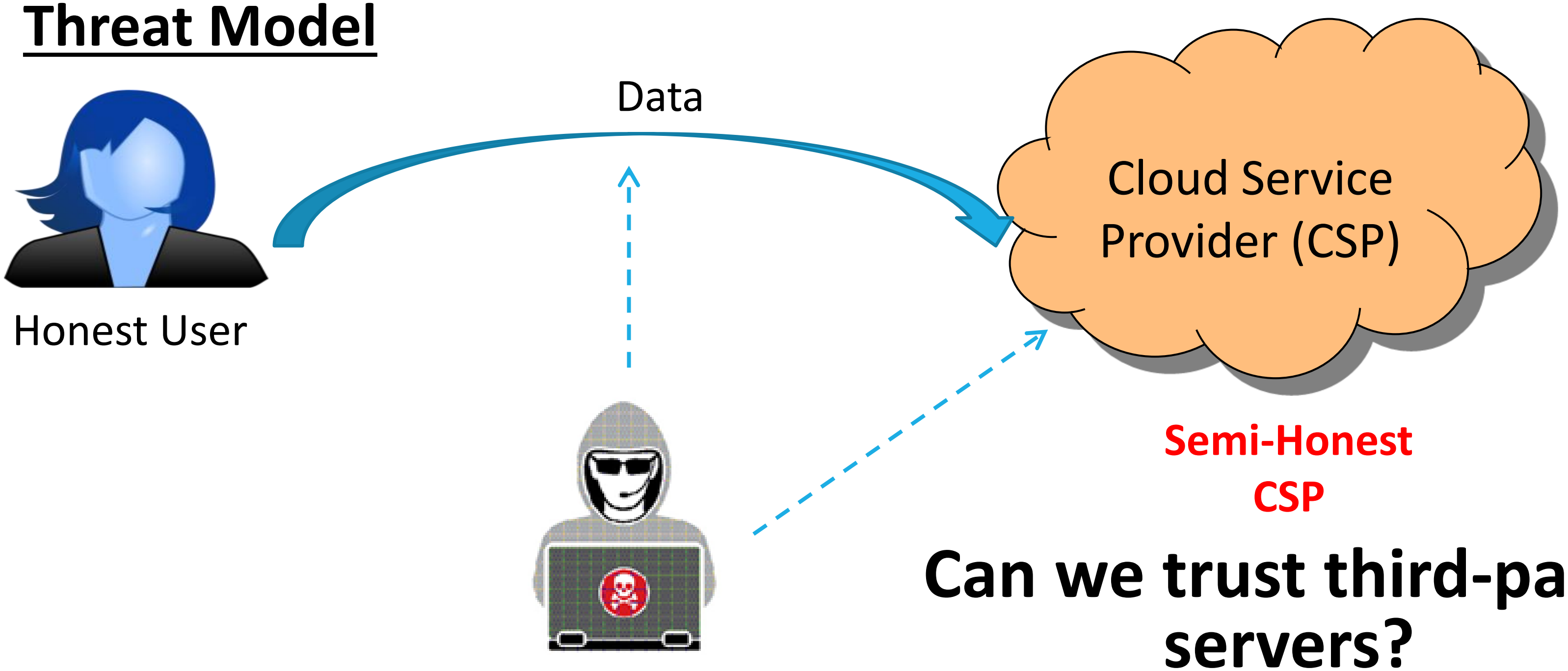
Day ▲▼ Month ▲▼ Year ▲▼

Date of Birth

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

Motivation (cont.)

Threat Model



Data

Cloud Service Provider (CSP)

Honest User

Malicious External Attacker

Semi-Honest CSP

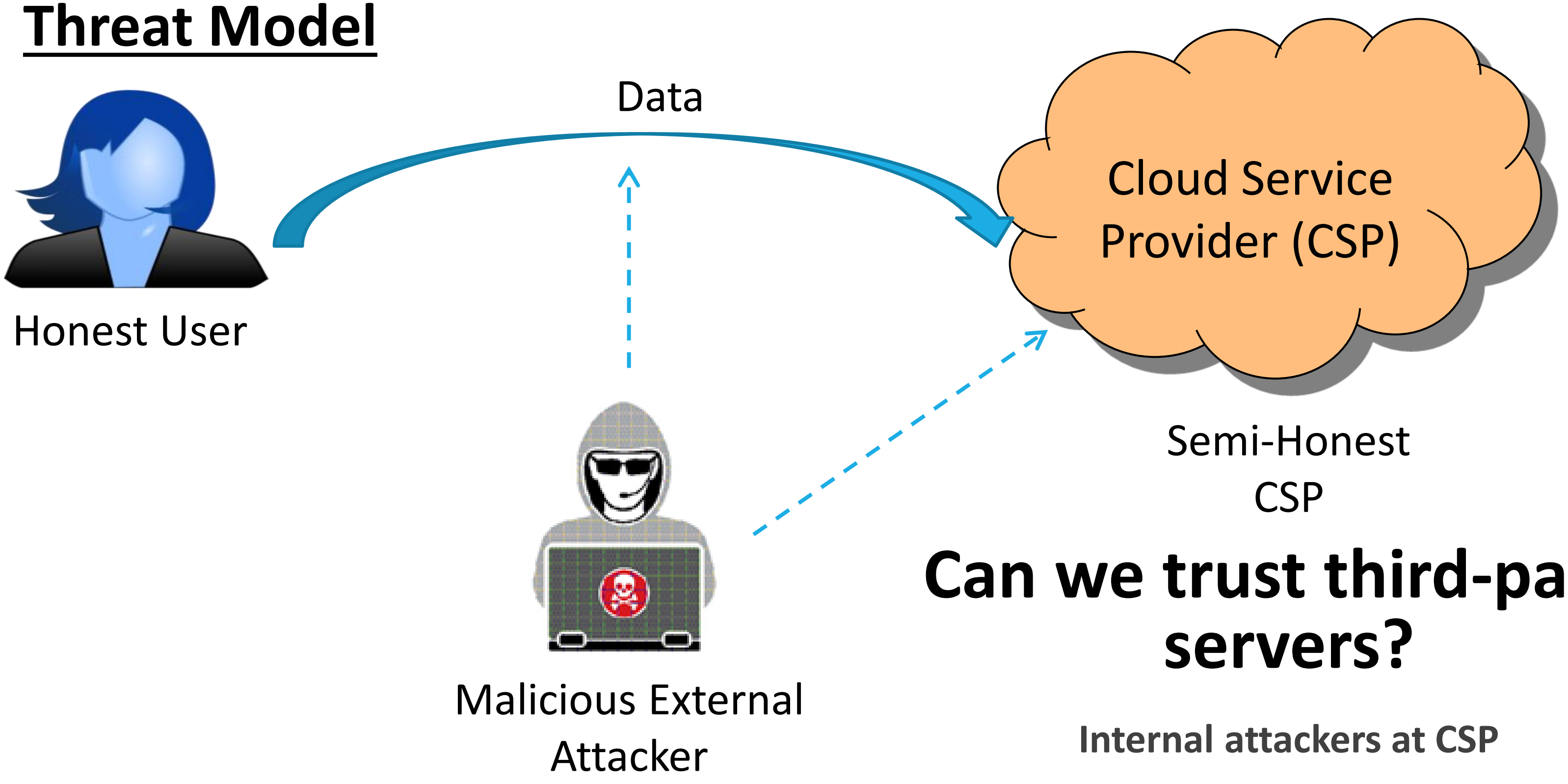
Can we trust third-party servers?

Internal attackers at CSP

Can We Securely Perform Tasks at Cloud?

Motivation (cont.)

Threat Model



Data

Honest User

Cloud Service Provider (CSP)

Semi-Honest CSP

Malicious External Attacker

Can we trust third-party servers?

Internal attackers at CSP

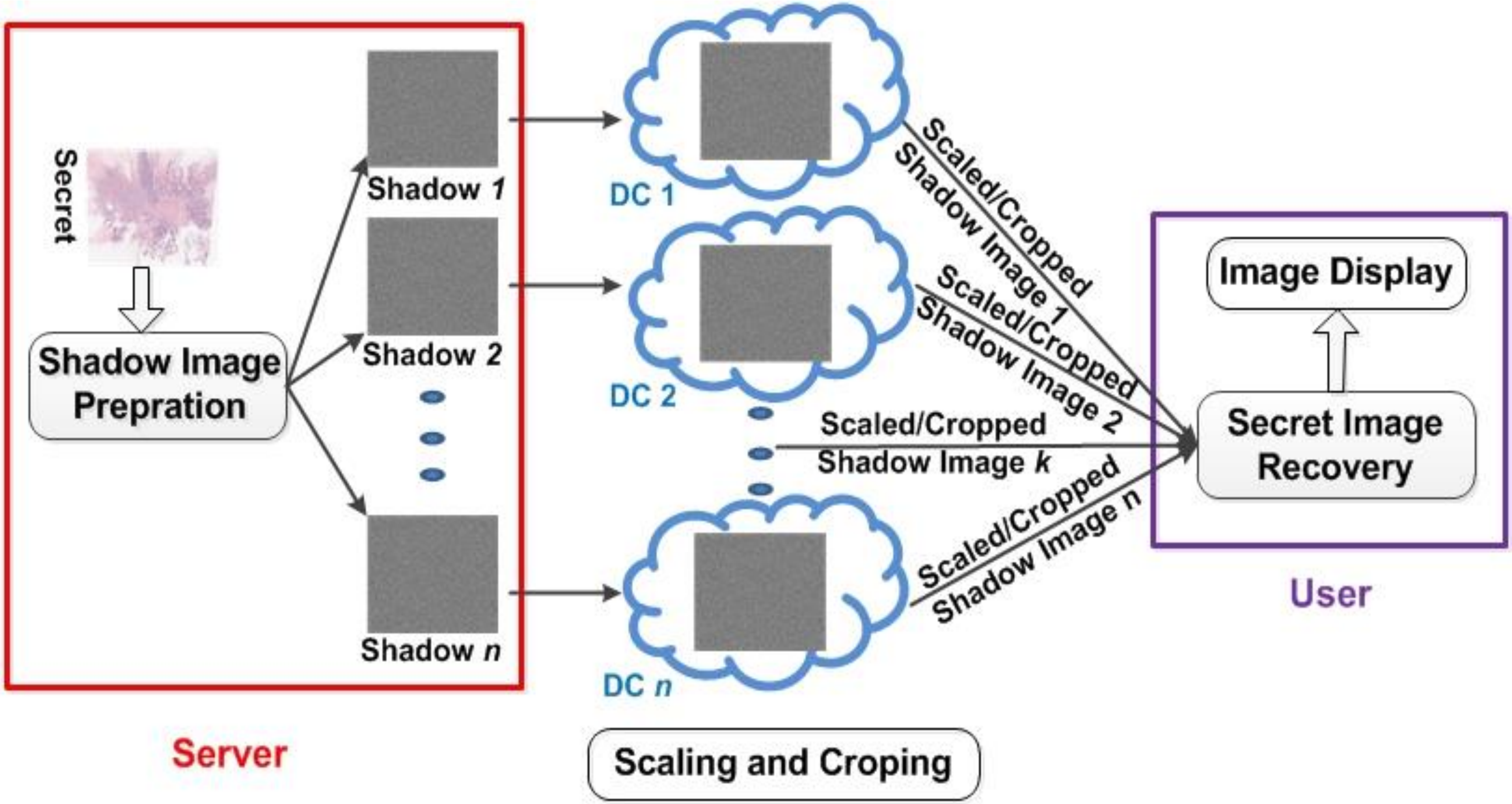
Can We Securely Perform Tasks at Cloud? → SecureCTask

SecureCSuite

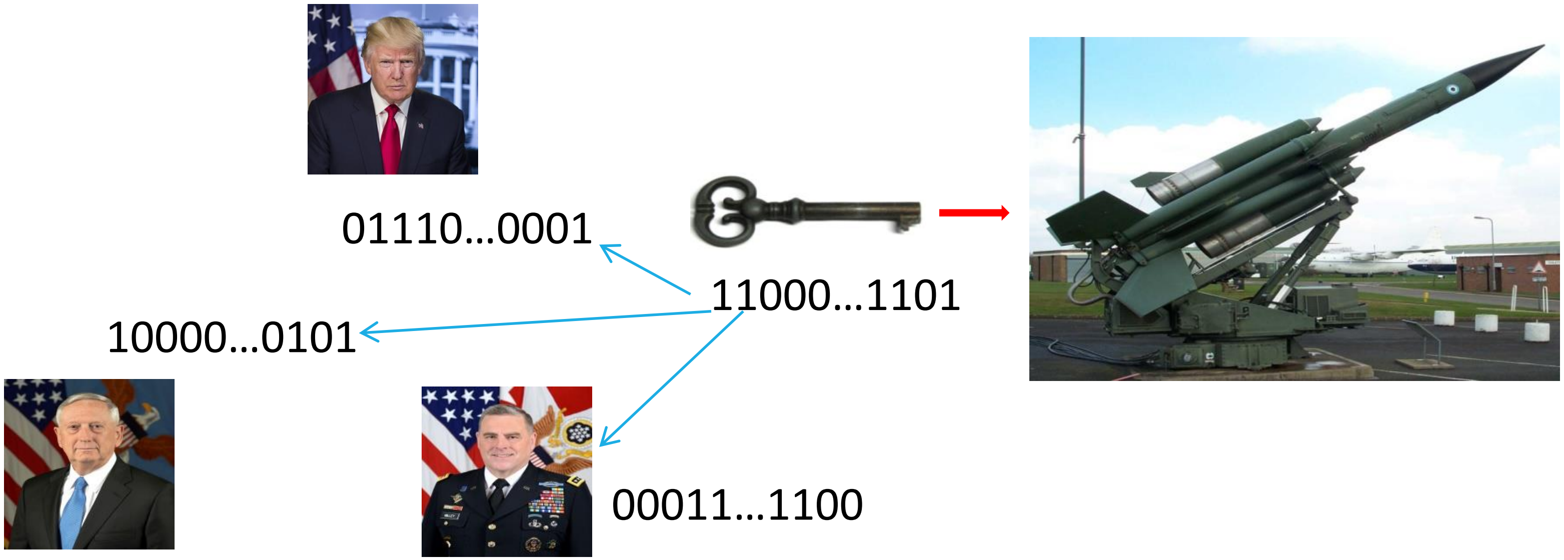
- **SecureCScaling**
  - **Secure Cloud-based Image/Video Scaling**
- SecureCEnhance
  - Secure Cloud-based Image/Audio Enhancement
- SecureCMail
  - Secure Cloud-based Emailing
- SecureCMerge
  - Secure Cloud-based PDF merging
- SecureCSearch
  - Searching of Keywords in Encrypted PDF

SecureCScaling:
Secure Cloud-based Image/Video Scaling

- Architecture and Workflow



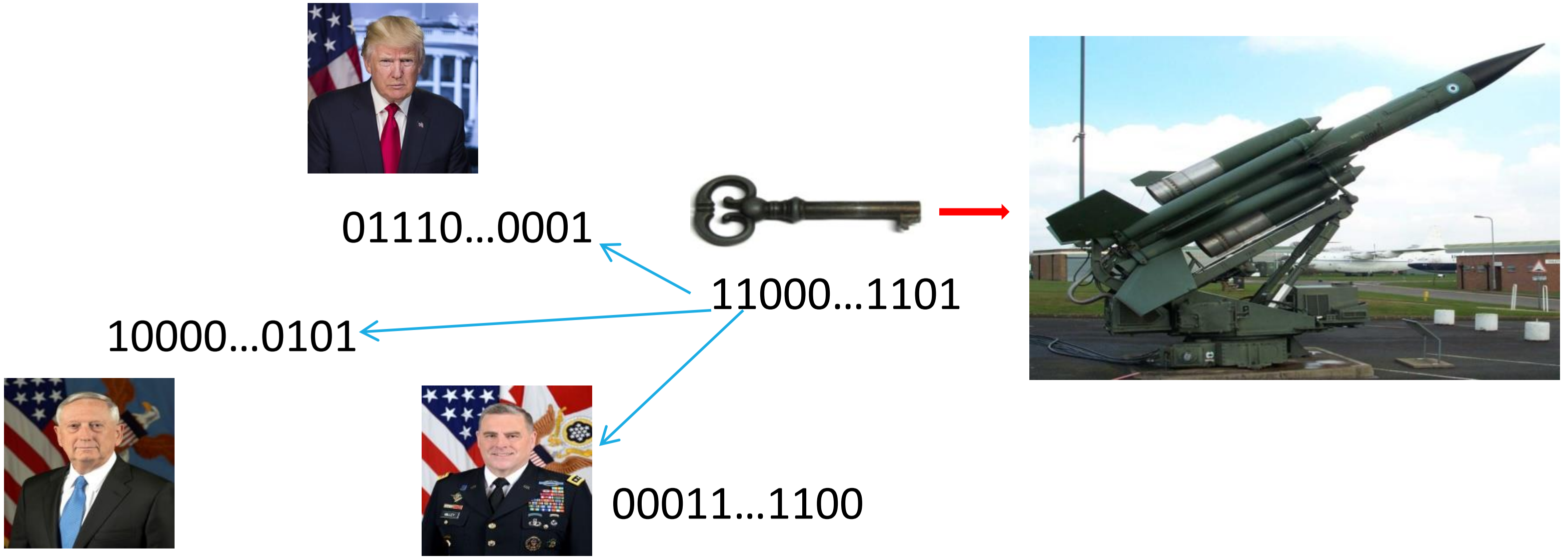
Cryptosystem - Shamir's Secret Sharing



Sharing a Secret

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

Cryptosystem - Shamir’s Secret Sharing



<u>Sharing a Secret</u>

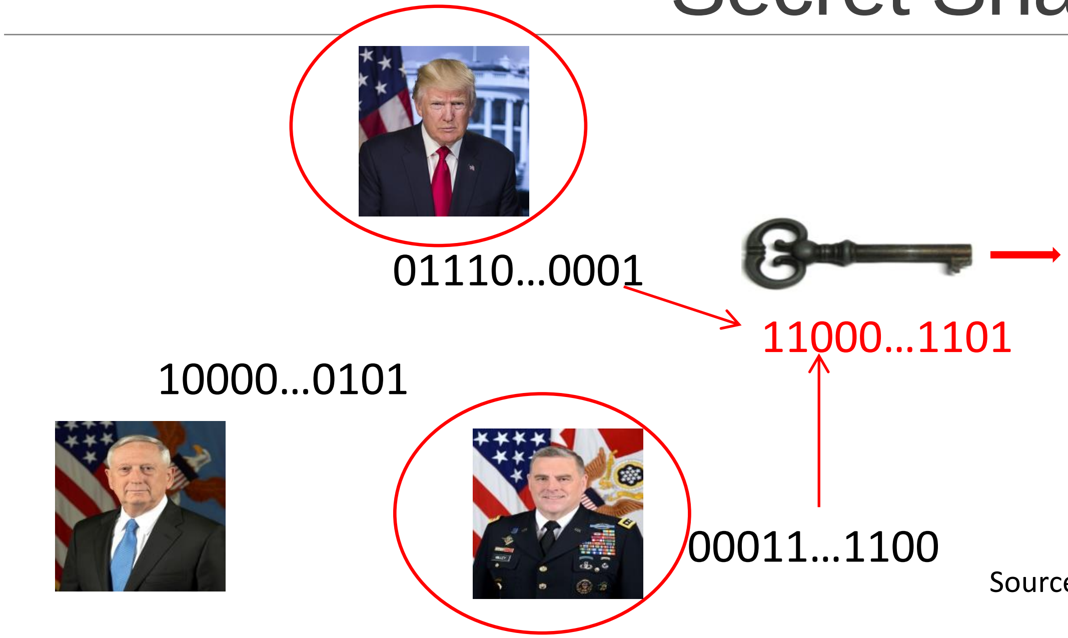
$$F(x) = \left(S + \sum_{i=1}^{k-1} a_i x^i\right) \bmod q$$

Secret

Random Number

Trash

Cryptosystem - Shamir's Secret Sharing



Source: http://www.ocss-va.org/jrotc/chain.html

Reconstructing a Secret

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

i^{th} *Share*

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

Cryptosystem - Shamir’s Secret Sharing

01110…0001

10000…0101

00011…1100

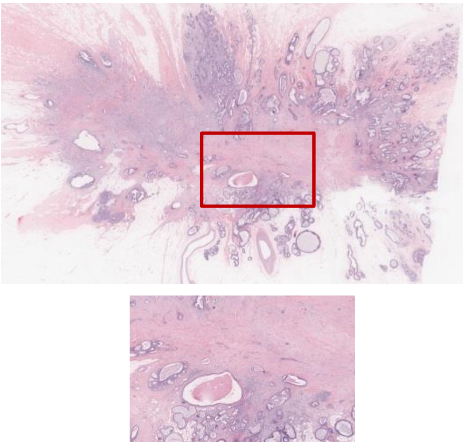
Source: http://www.ocss-va.org/jrotc/chain.html

Homomorphic property: E(A) o E(B) = E(AoB)

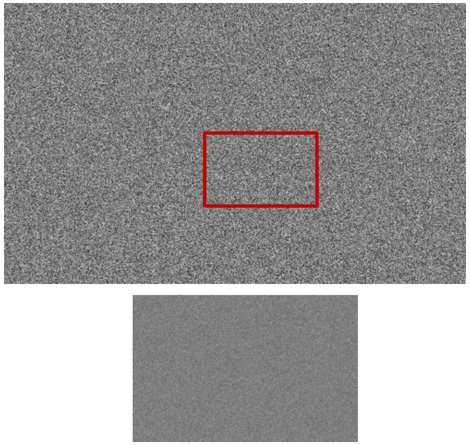
o: +, - *, /, |

SecureCScaling:
Secure Cloud-based Image Scaling

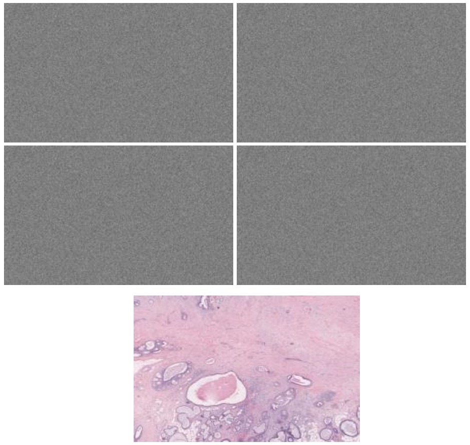
- Results: Scaling



Required



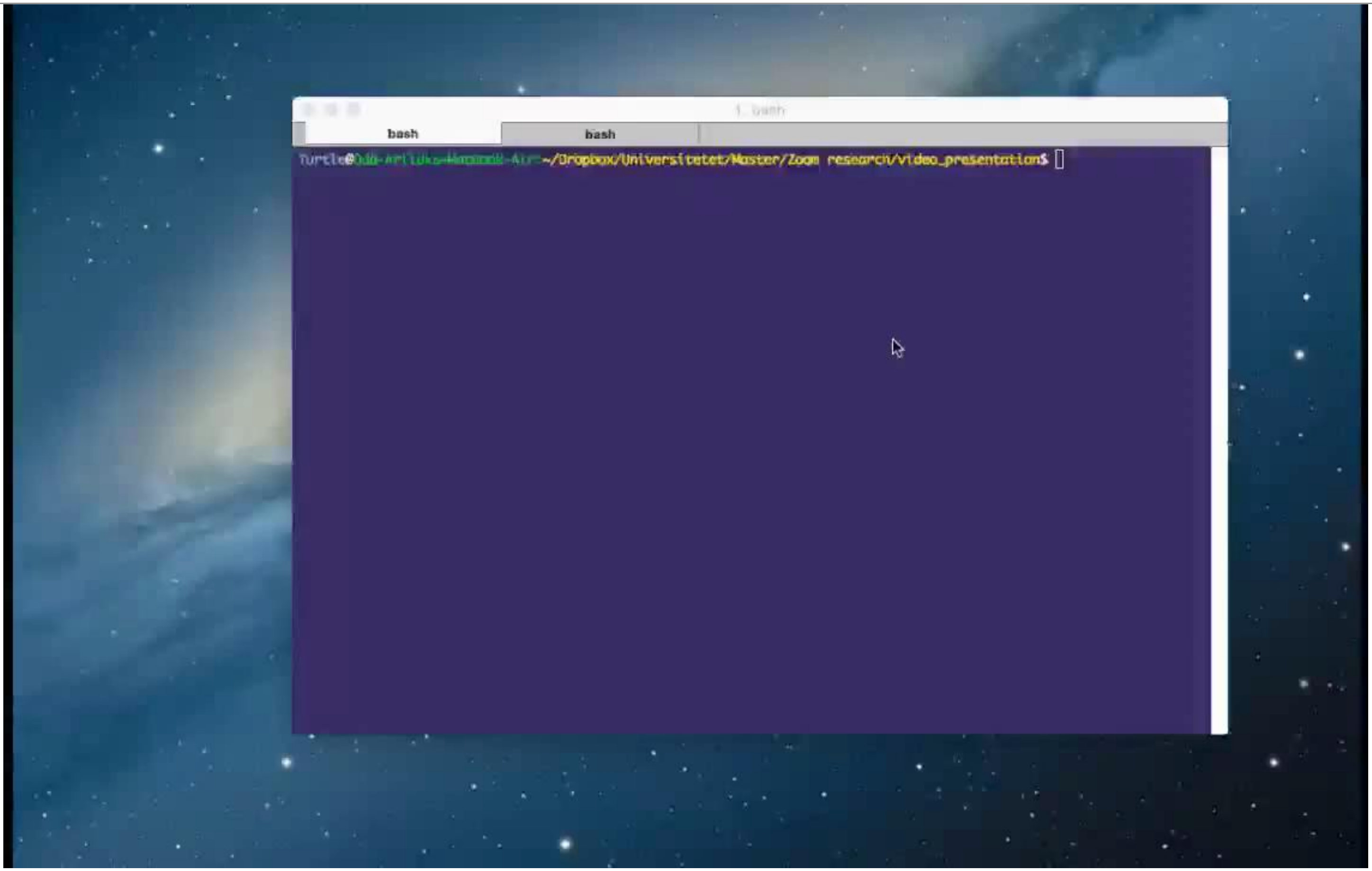
Zoomed Shadow Image



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



```
Turtle@Odd-Arilds-Macbook-Air:~/Dropbox/Universitetet/Master/Zoom research/video_presentation$ 
```

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.

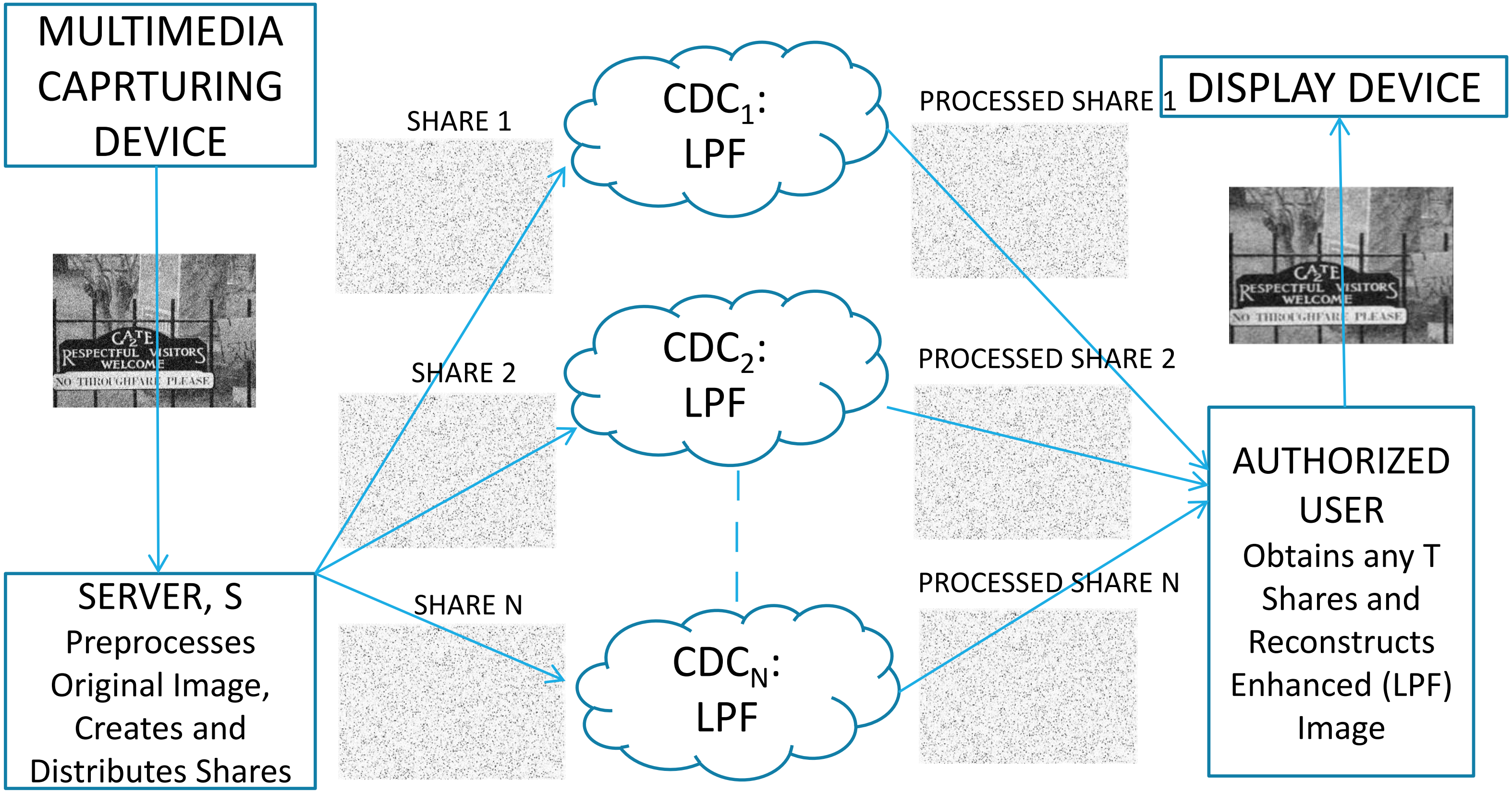
SecureCSuite

- 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
- SecureCSearch
  - Searching of Keywords in Encrypted PDF

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

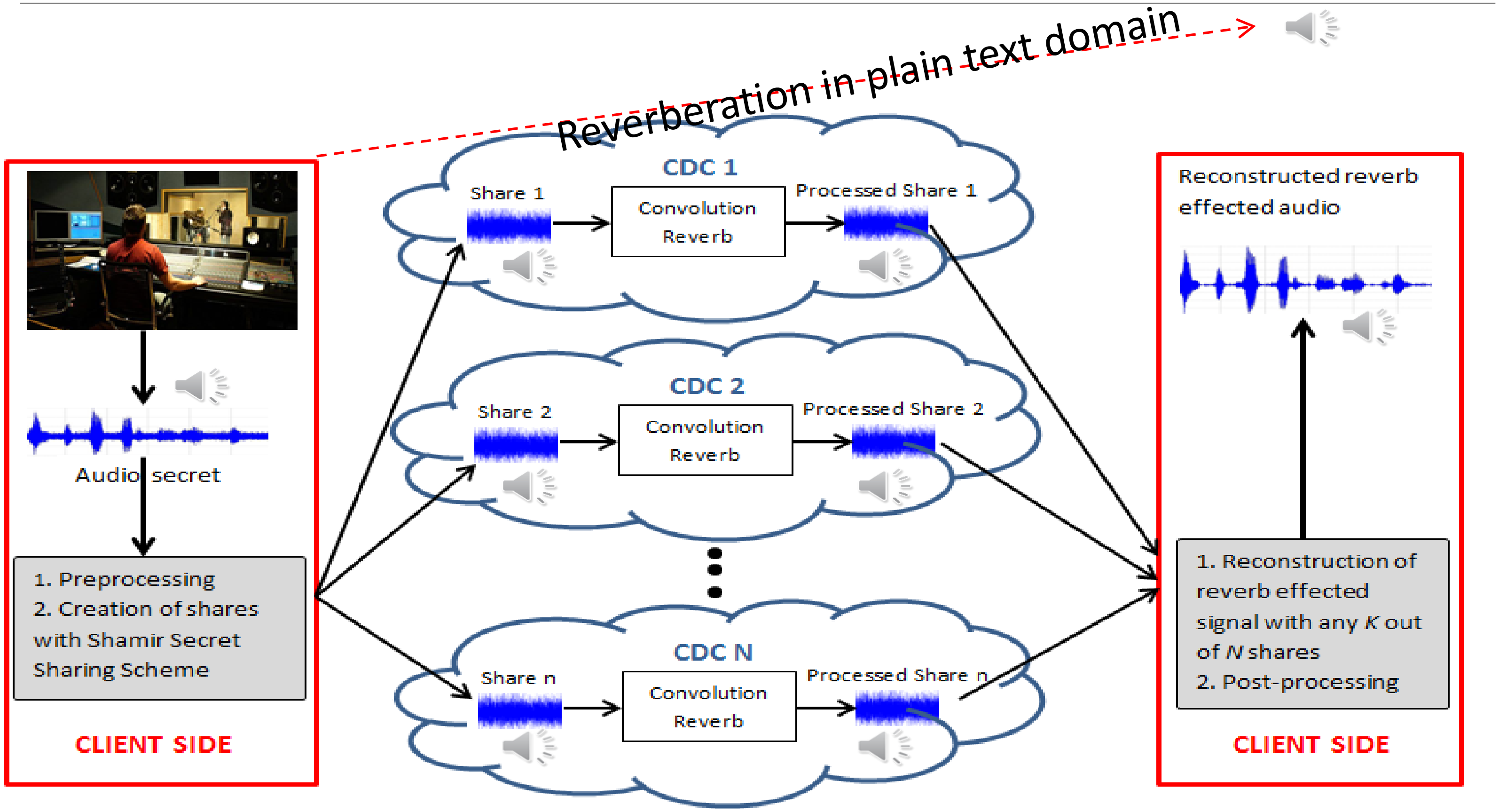
- Noise removal and anti-aliasing
  - Results – Scheme 1 (Demo)
  - Results – Scheme 2 (Demo)
- Edge and contrast enhancement (Demo)
- Dehazing (Demo)

More demos available on:

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

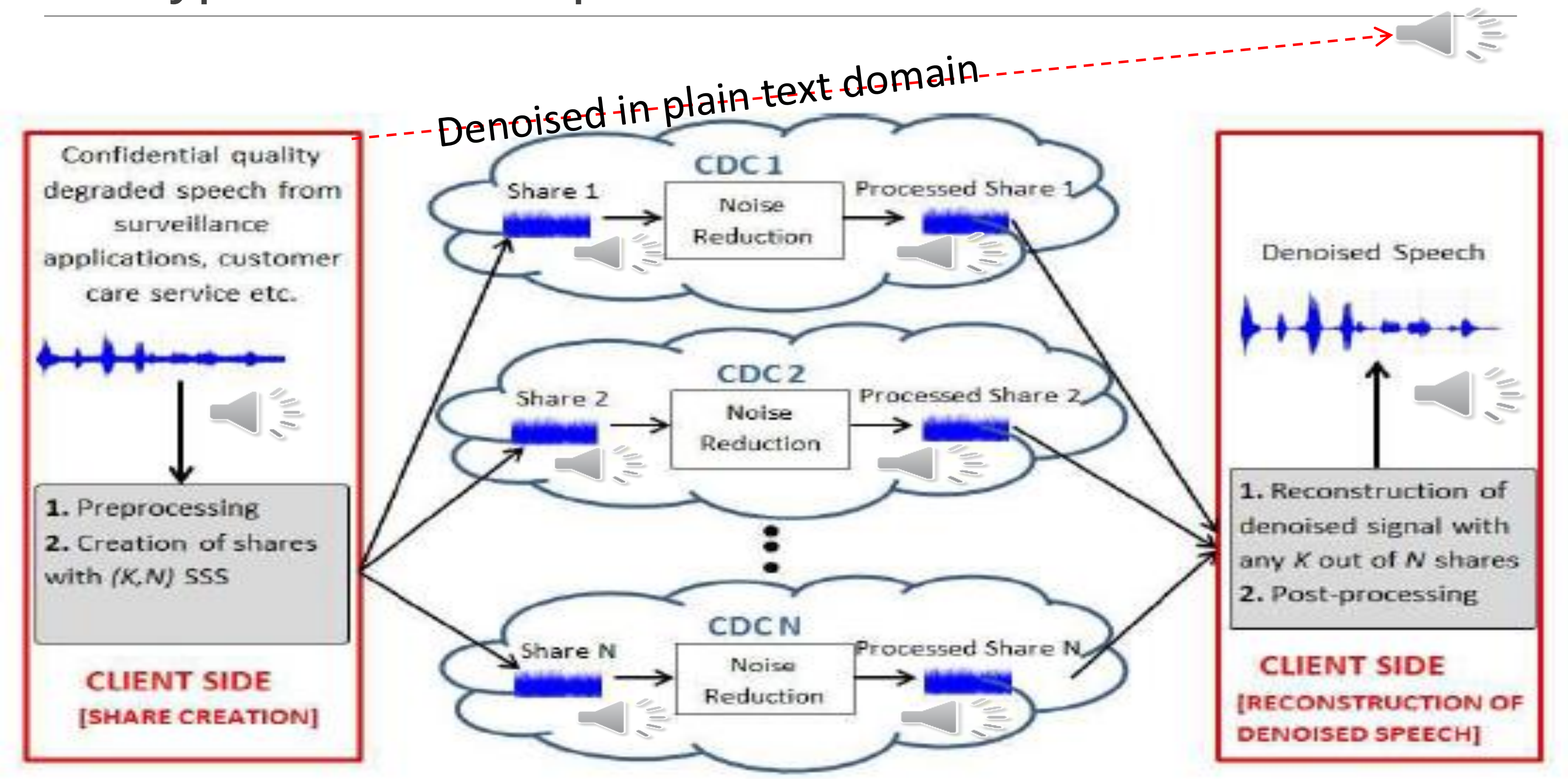
A. Lathey and P. K. Atrey. **Image enhancement in encrypted domain over cloud**. *ACM Transactions on Multimedia, Computing, Communications and Applications*, January 2015.

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


Denoised in plain text domain
Confidential quality degraded speech from surveillance applications, customer care service etc.
1. Preprocessing
2. Creation of shares with (K,N) SSS
CLIENT SIDE
[SHARE CREATION]
CDC 1
Share 1
Noise Reduction
Processed Share 1
CDC 2
Share 2
Noise Reduction
Processed Share 2
CDC N
Share N
Noise Reduction
Processed Share N
Denoised Speech
1. Reconstruction of denoised signal with any K out of N shares
2. Post-processing
CLIENT SIDE
[RECONSTRUCTION OF DENOISED SPEECH]

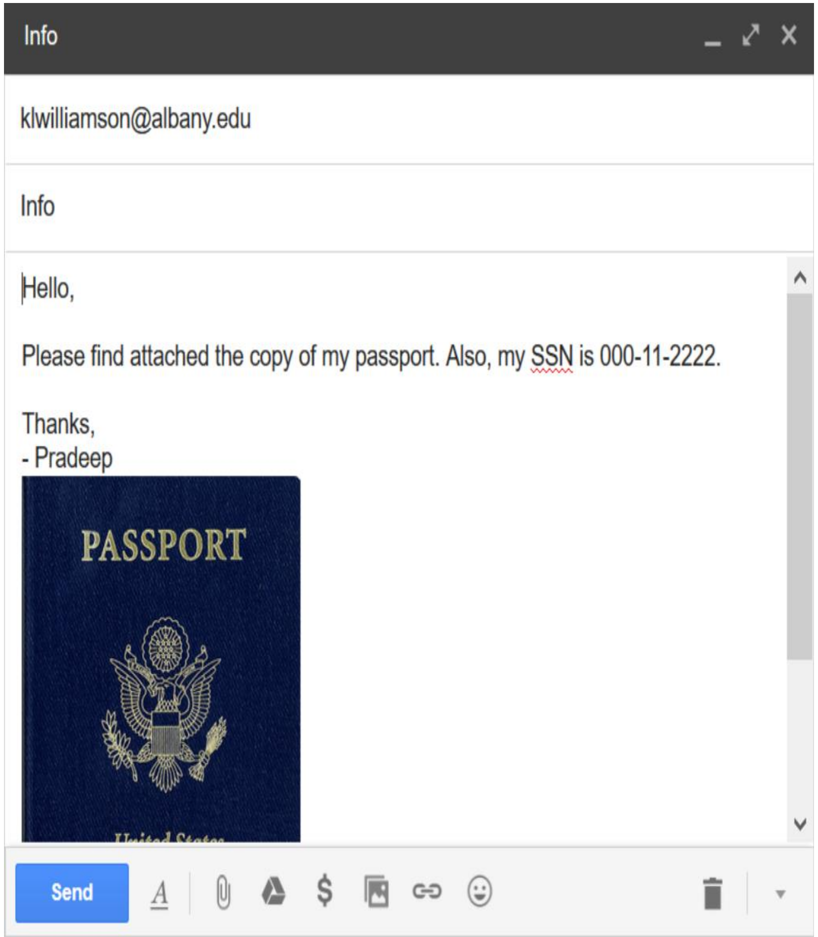
- Yakubu, N. Maddage and P. K. Atrey. **Encrypted domain cloud-based speech noise reduction**. *The 1st International Workshop on Privacy in Multimedia (PIM'16) with ICME'16*, July 2016, Seattle, WA, USA.
- A. Yakubu, N. Maddage and P. K. Atrey. **Securing speech noise reduction in outsourced environment**. ACM Transactions on Multimedia Computing, Communication and Applications. Vol. 13, No. 4, Article 51, August (2017).

SecureCSuite

- 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
- SecureCSearch
  - Searching of Keywords in Encrypted PDF

SecureCMail:
Securing Emails from Service Providers using Secret Sharing

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



klwilliamson@albany.edu

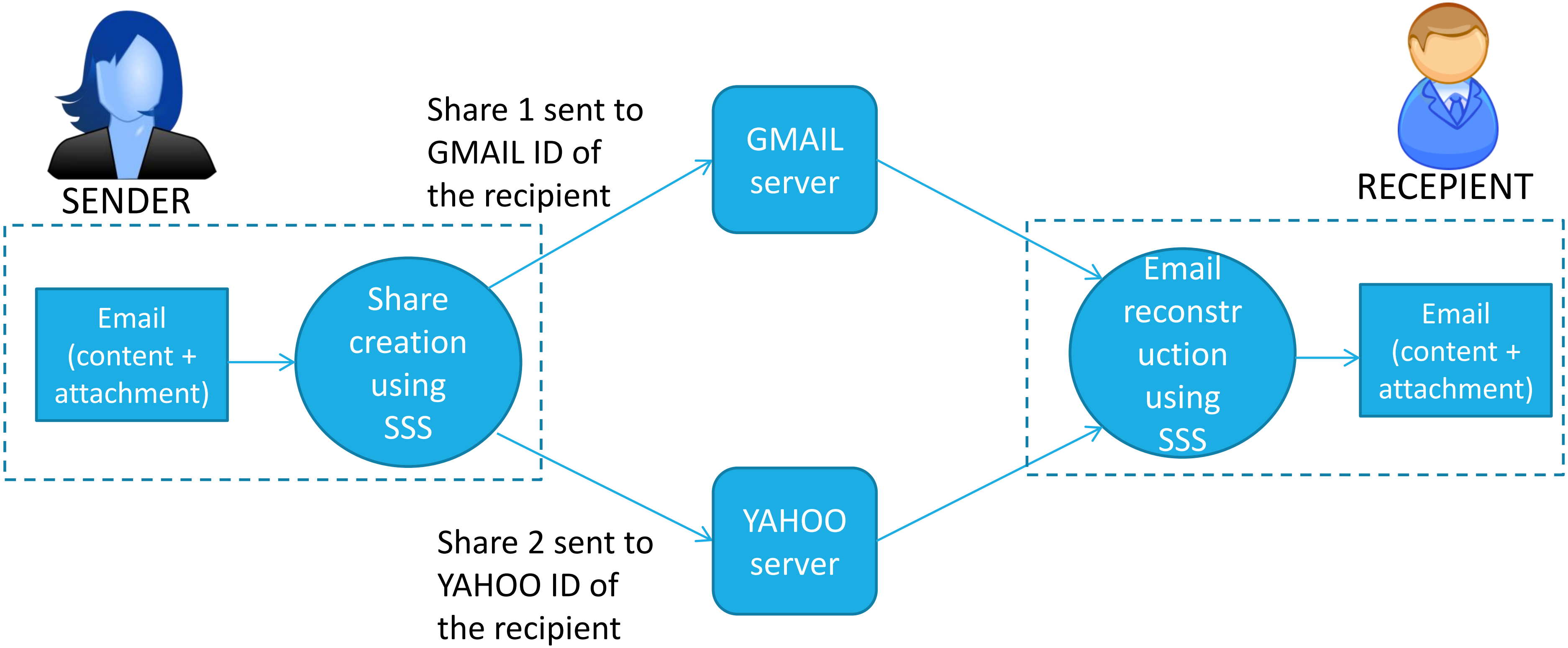
Info

Hello,

Please find attached the copy of my passport. Also, my SSN is 000-11-2222.

Thanks,
- Pradeep

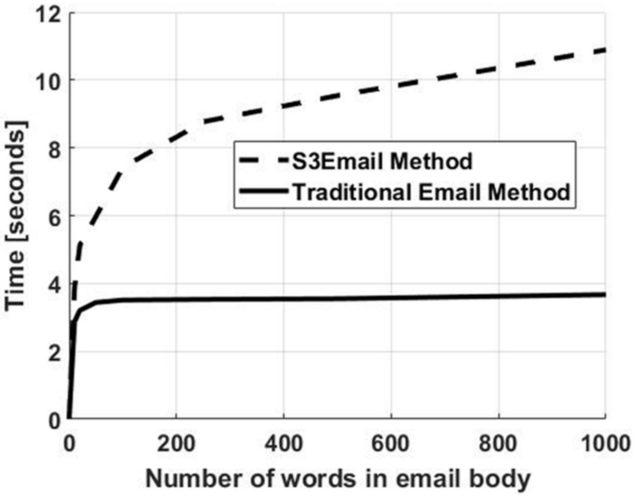
SecureCMail:
Securing Emails from Service Providers using Secret Sharing

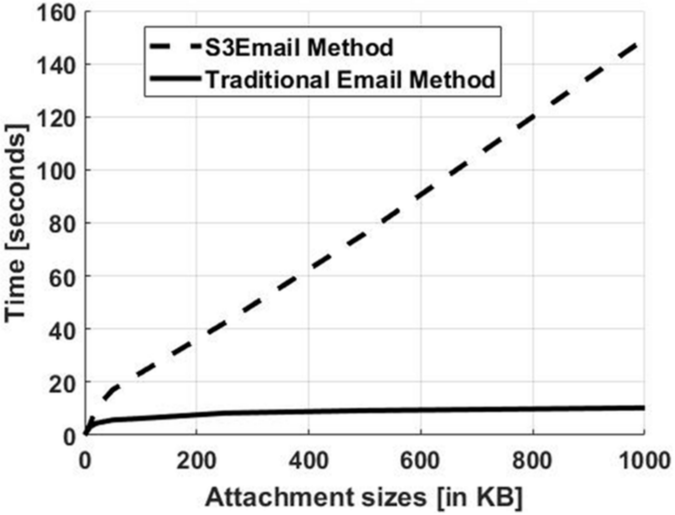

SENDER
Email (content + attachment)
Share creation using SSS
Share 1 sent to GMAIL ID of the recipient
GMAIL server
Share 2 sent to YAHOO ID of the recipient
YAHOO server
RECEPIENT
Email reconstr uction using SSS
Email (content + attachment)

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





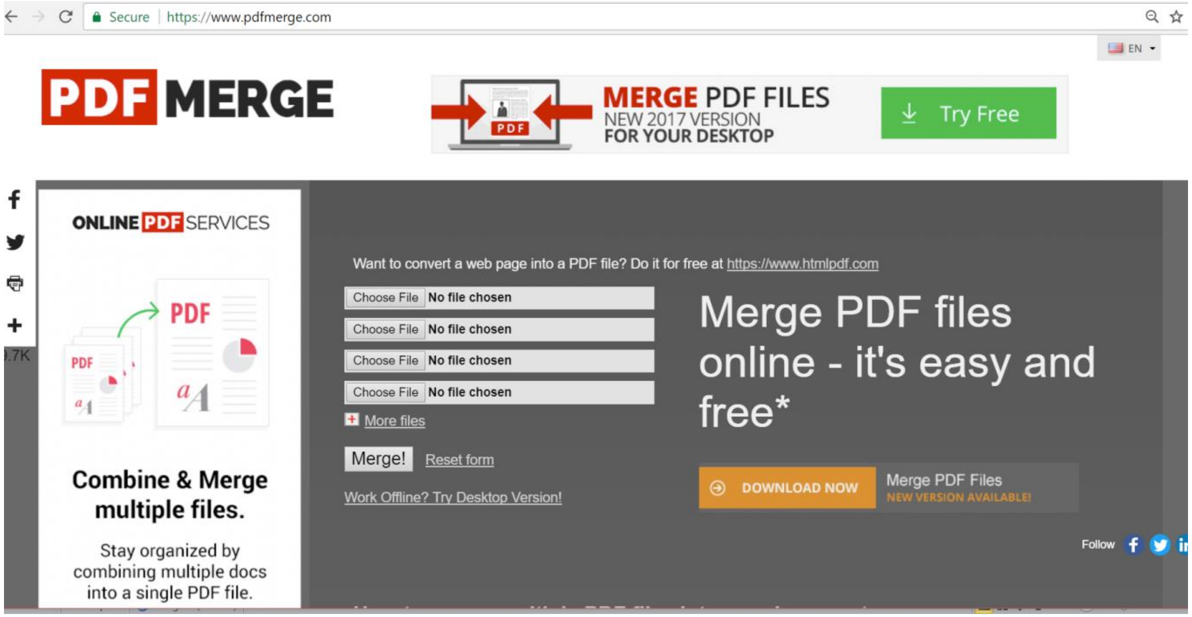
P. Singh, S. Arora, K. Williamson and P. K. Atrey. **S3Email: A method for securing emails from service providers**. The 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC'2017), Banff, Canada, October 2017.

SecureCSuite

- 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**
- SecureCSearch
  - Searching of Keywords in Encrypted PDF

SecureCMerge:
Secure Online PDF Merging

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



Combine & Merge multiple files.

Stay organized by combining multiple docs into a single PDF file.

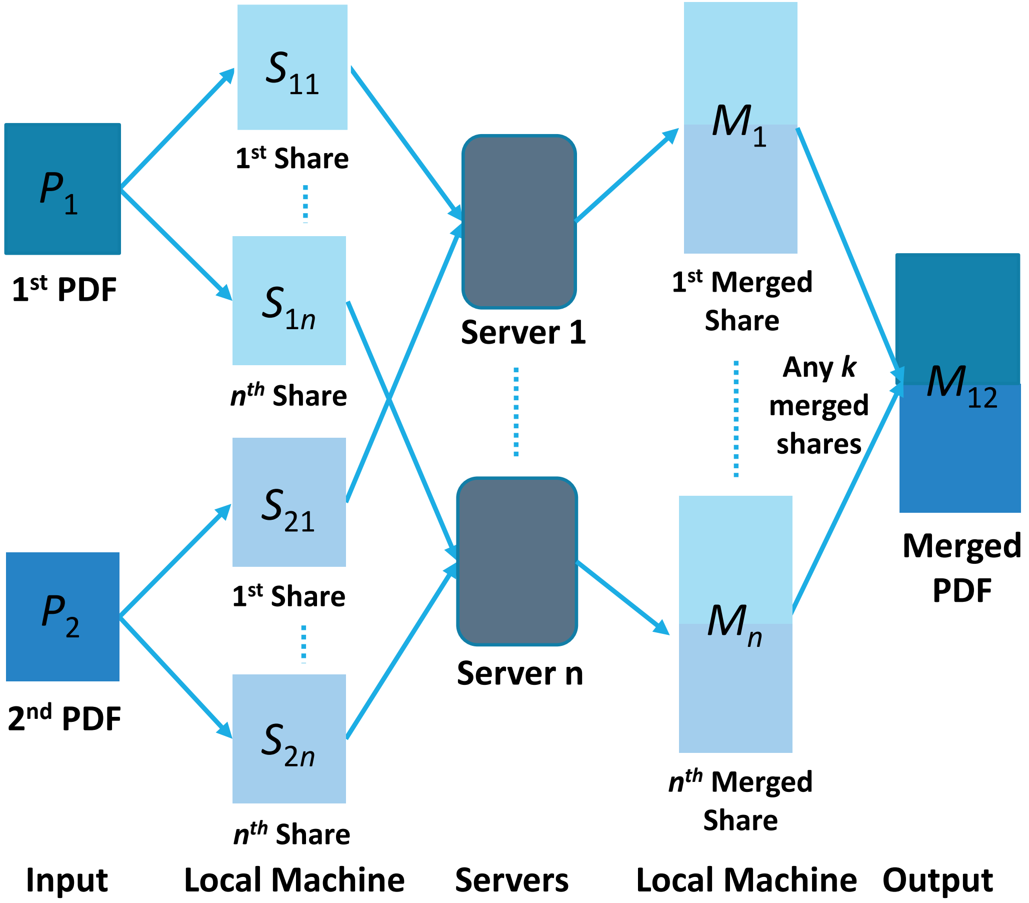
Want to convert a web page into a PDF file? Do it for free at https://www.htmlpdf.com

Merge PDF files online - it's easy and free*

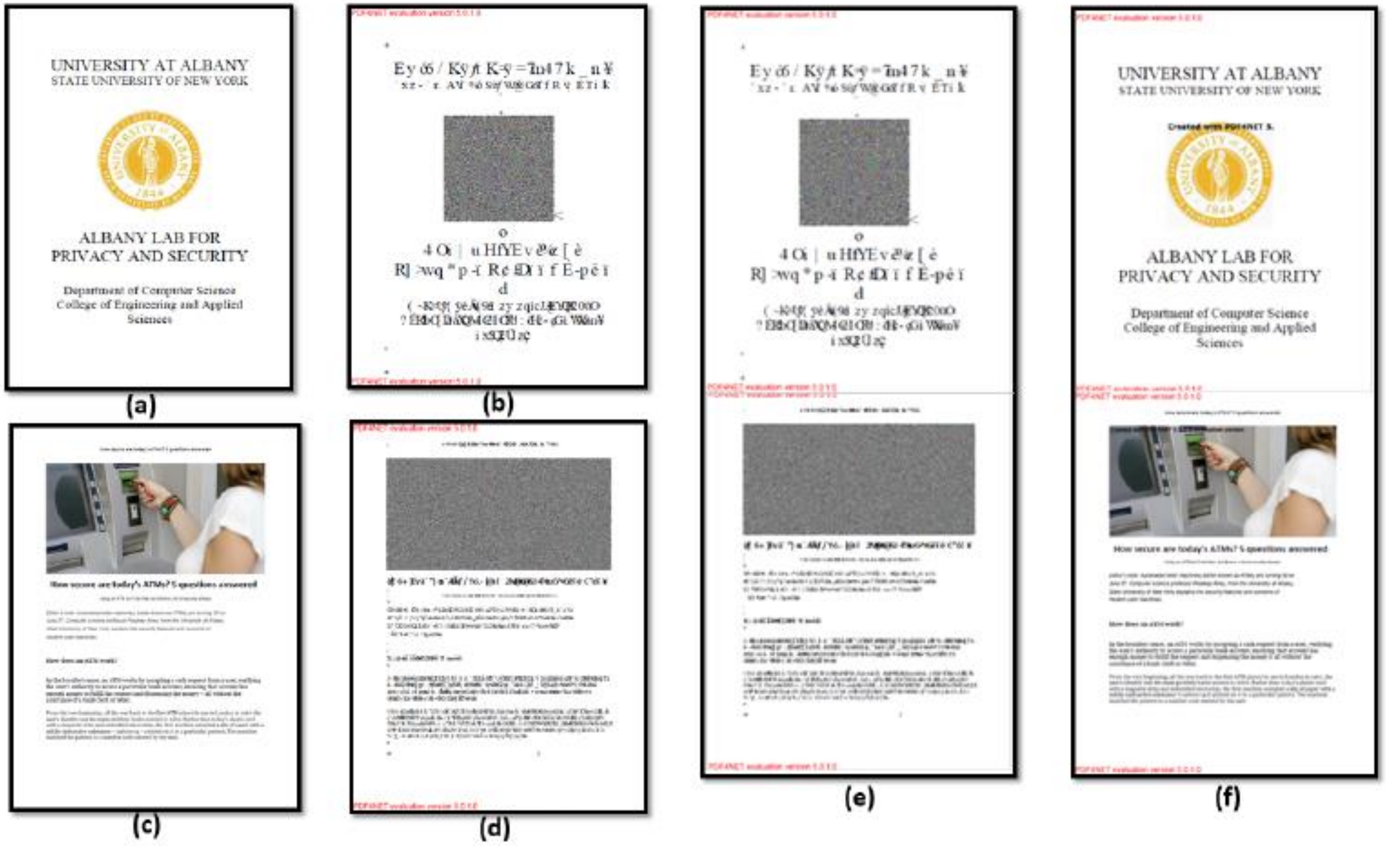
Work Offline? Try Desktop Version!

Can they see your documents? YES

SecureCMerge:
Secure Online PDF Merging

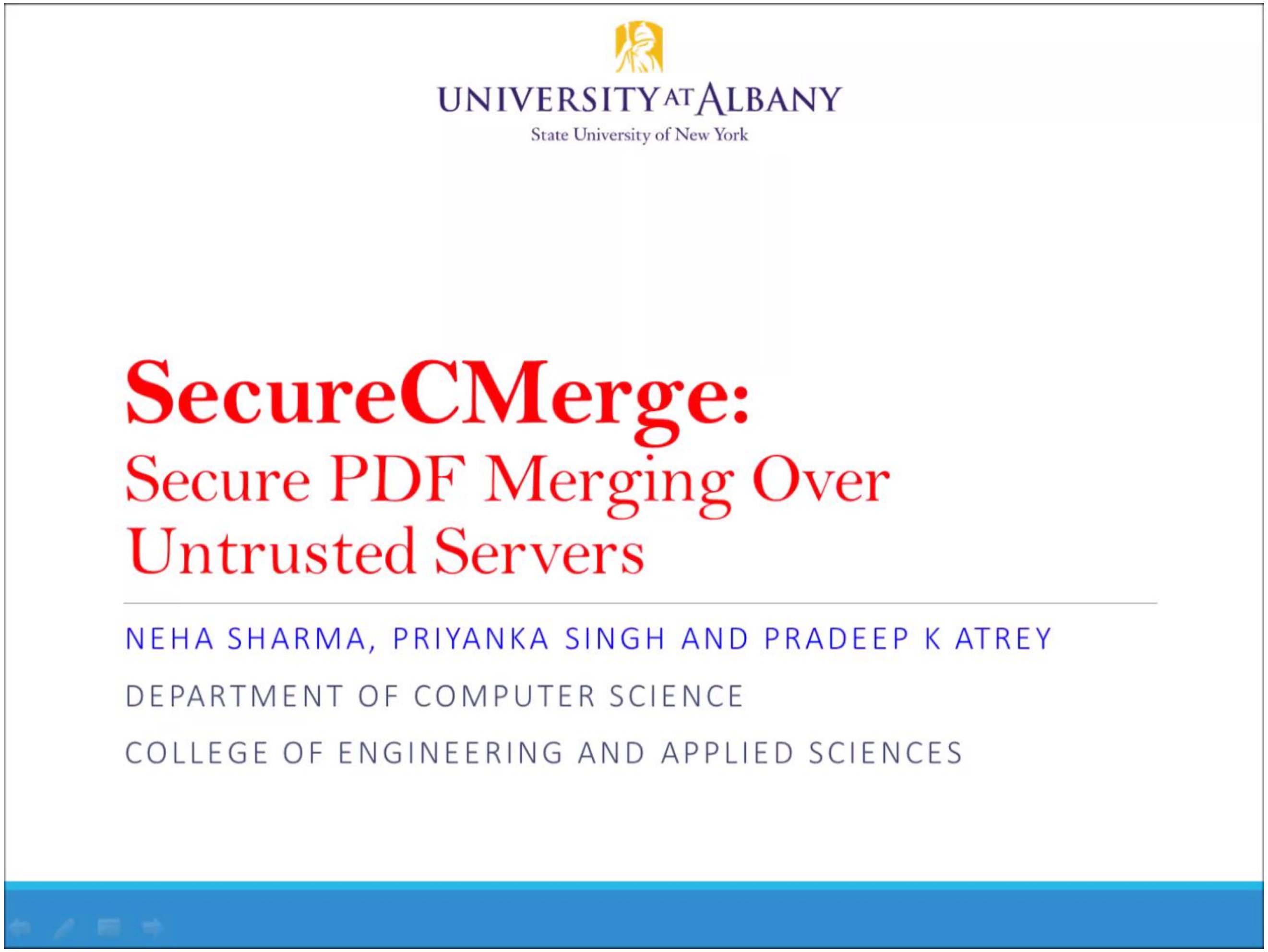


SecureCMerge:
Secure Online PDF Merging


UNIVERSITY AT ALBANY
STATE UNIVERSITY OF NEW YORK
ALBANY LAB FOR
PRIVACY AND SECURITY
Department of Computer Science
College of Engineering and Applied
Sciences
(a)
(b)
How secure are today's ATMs? 5 questions answered
(c)
(d)
(e)
Created with PDF4NET 5.
(f)

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 (Under review)

SecureCMerge:
Secure Online PDF Merging



UNIVERSITY AT ALBANY
State University of New York

SecureCMerge:
Secure PDF Merging Over Untrusted Servers

NEHA SHARMA, PRIYANKA SINGH AND PRADEEP K ATREY

DEPARTMENT OF COMPUTER SCIENCE

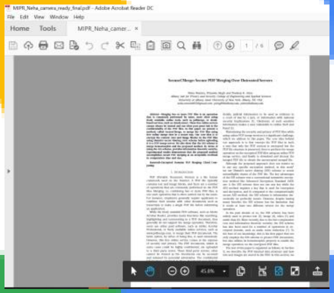
COLLEGE OF ENGINEERING AND APPLIED SCIENCES

SecureCSuite

- 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
- **SecureCSearch**
  - **Searching of Keywords in Encrypted PDF**

Motivation

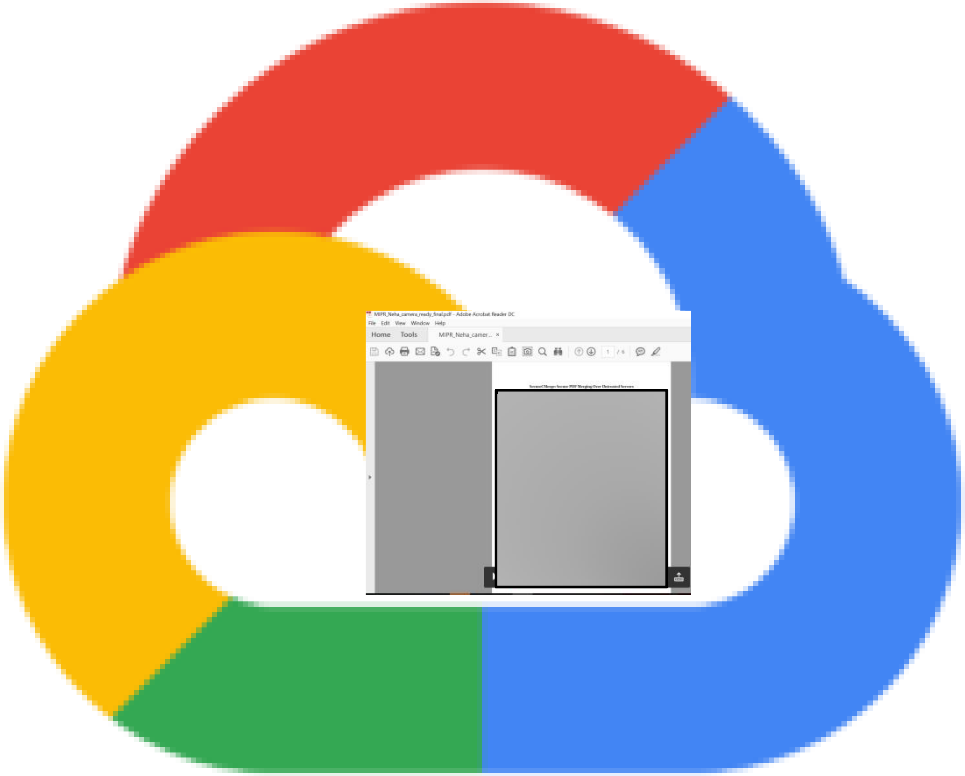
Q1: Do you keep your confidential pdf files over cloud?



SecureCMerge: Secure PDF Merging Over Untrusted Servers

Motivation (Cont.)

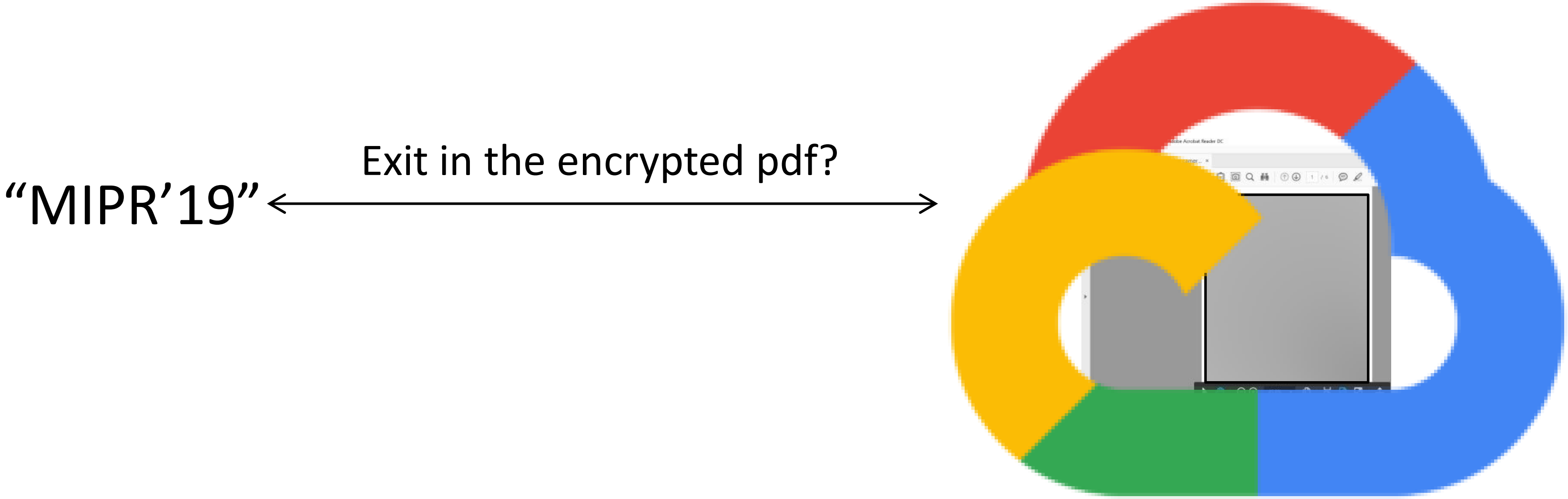
Q2: Would you like to encrypt your confidential pdf files before sending over cloud?



SecureCMerge: Secure PDF Merging Over Untrusted Servers

Motivation (Cont.)

Q3: Would you like to search for some keywords in your encrypted pdf files over cloud?



“MIPR’19”

Exit in the encrypted pdf?

Motivation (cont.)

What to do? How do we search given keywords in an encrypted pdf?

Which encryption scheme to use?

Key Contribution and Core Idea

Contribution: SecureCSearch, a method to search given keyword in encrypted PDF files.

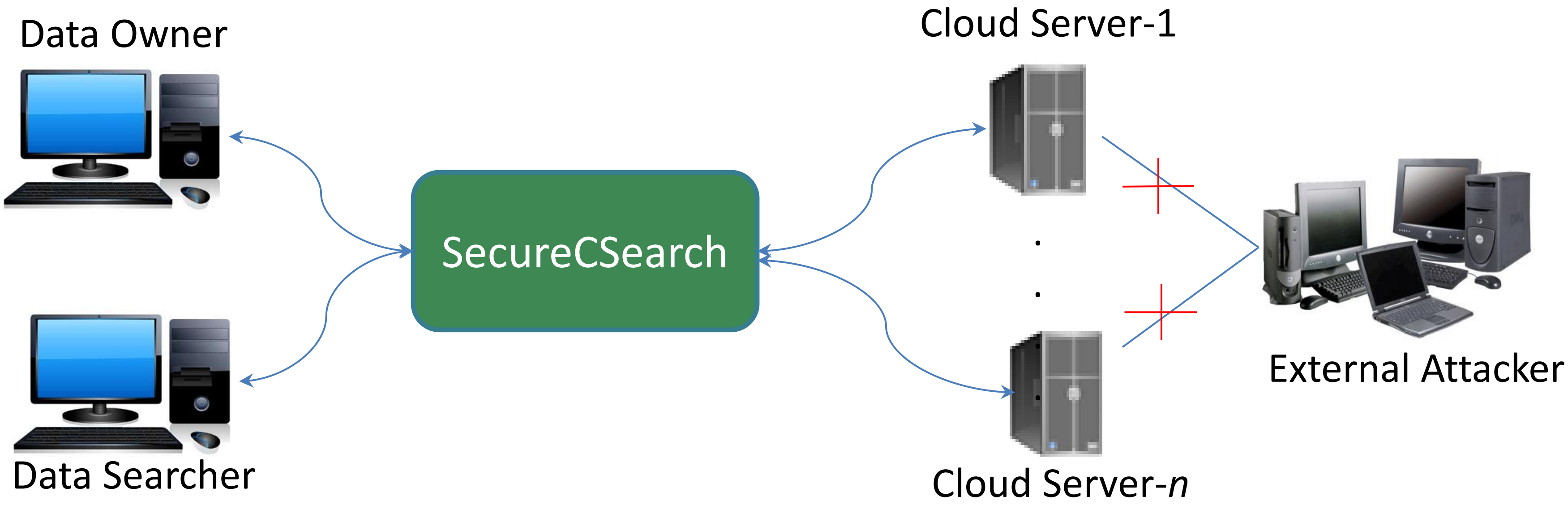
Idea: Using Shamir's secret sharing (SSS) scheme in a novel way.

Problem with the use of AES for searchable encryption: Block-based encryption

SSS scheme – used for text [3], images [4], videos [5], and audio [7].
SSS-based PDF merge [8]

[3] M. Sudha and C. Thanujat, "Randomly tampered image detection and self-recovery for a text document using shamir secret sharing," in *IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology*, Bengaluru, India, 2017, pp. 688–691.
[4] P. Singh and B. Raman, "Reversible data hiding based on Shamir's secret sharing for color images over cloud," *Information Sciences*, vol. 422, pp. 77 – 97, 2018.
[5] Y. Liu, L. Chen, M. Hu, Z. Jia, S. Jia, and H. Zhao, "A reversible data hiding method for H.264 with Shamir's (t,n)-threshold secret sharing." *Neurocomputing*, vol. 188, pp. 63 – 70, 2016.
[6] N. M. Yoeseph, F. A. Purnomo, B. K. Riasti, M. A. Safiie, and T. N. Hidayat, "Steganography on multiple MP3 files using spread spectrum and Shamir's secret sharing," *Journal of Physics: Conference Series*, vol. 776, no. 1, pp. 012–089, 2016.
[7] A. M. Yakubu, N. C. Maddage, and P. K. Atrey, "Securing speech noise reduction in outsourced environment," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 13, no. 4, p. 51, 2017.
[8] N. Sharma, P. Singh, and P. K. Atrey. SecureCMerge: Secure PDF merging over untrusted servers. In Proceedings of the IEEE International Conference on Multimedia Information Processing and Retrieval (MIPR), Miami, FL, USA.

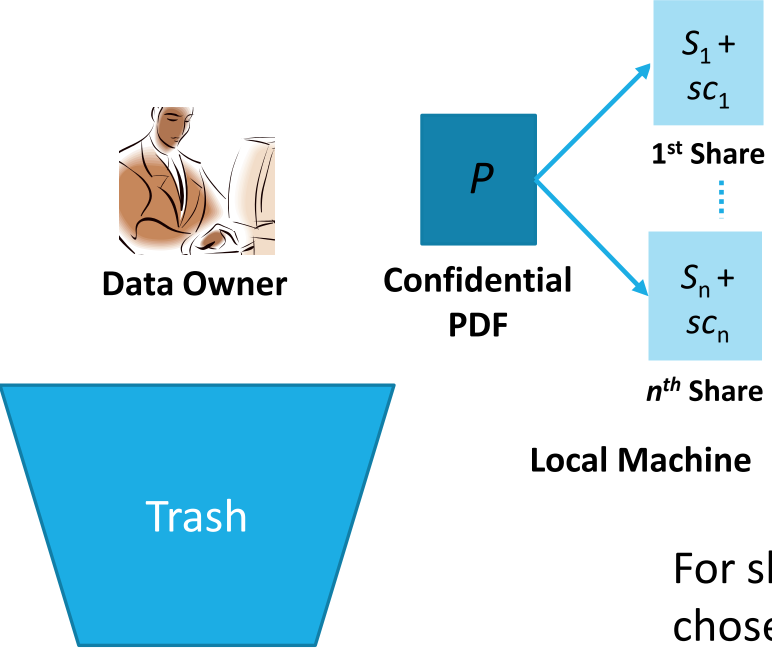
Proposed Work
System Model



- ***Data Owner (*****Trusted):** An individual or an organization or a computer application that uploads PDF files to Cloud Servers.
- ***Cloud Server*** **(Honest-but-Curious):** Stores the encrypted PDF files and provides the keyword searching option to data searchers.
- ***Data Searcher*** **(Trusted or an honest-but-curious)*:*** An individual or a computer application that searches a keyword on the encrypted PDF files on the Cloud Servers.
- ***External Attacker*** **(Non-trusted)*:*** An individual or a computer application that attempts to access the stored PDF files without authorization.

Proposed Work

SecureCSearch Method: **Share Creation**



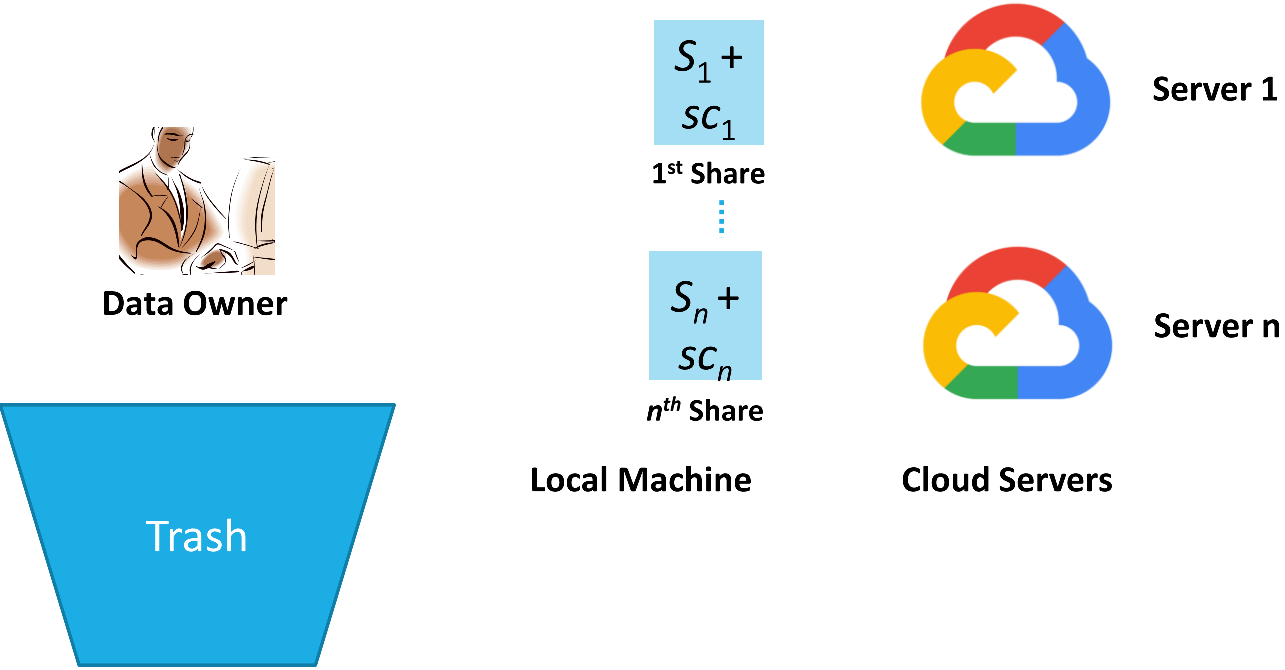
S_1 = 1st share of P
sc_1 = 1st share of the l coefficients used for creating S_1 to S_n

S_n = n^{th} share of P
sc_n = n^{th} share of the l coefficients used for creating S_1 to S_n

For sharing a word, k - 1 coefficients are randomly chosen from the l = = r × (k - 1) coefficients.

Proposed Work

SecureCSearch Method: **Share Outsourcing to Cloud**



Data Owner

Trash

$S_1 +$
sc_1

1st Share

$S_n +$
sc_n

n^{th} Share

Local Machine

Server 1

Server n

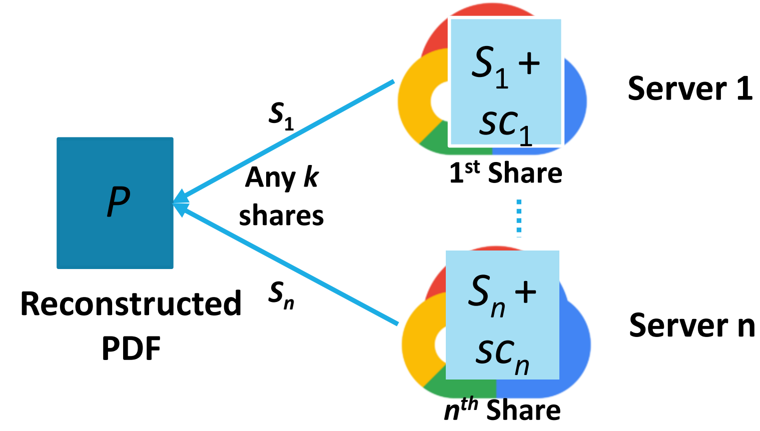
Cloud Servers

Proposed Work

SecureCSearch Method: **Secret Reconstruction w/o Keyword Searching**

Data Owner

Trash

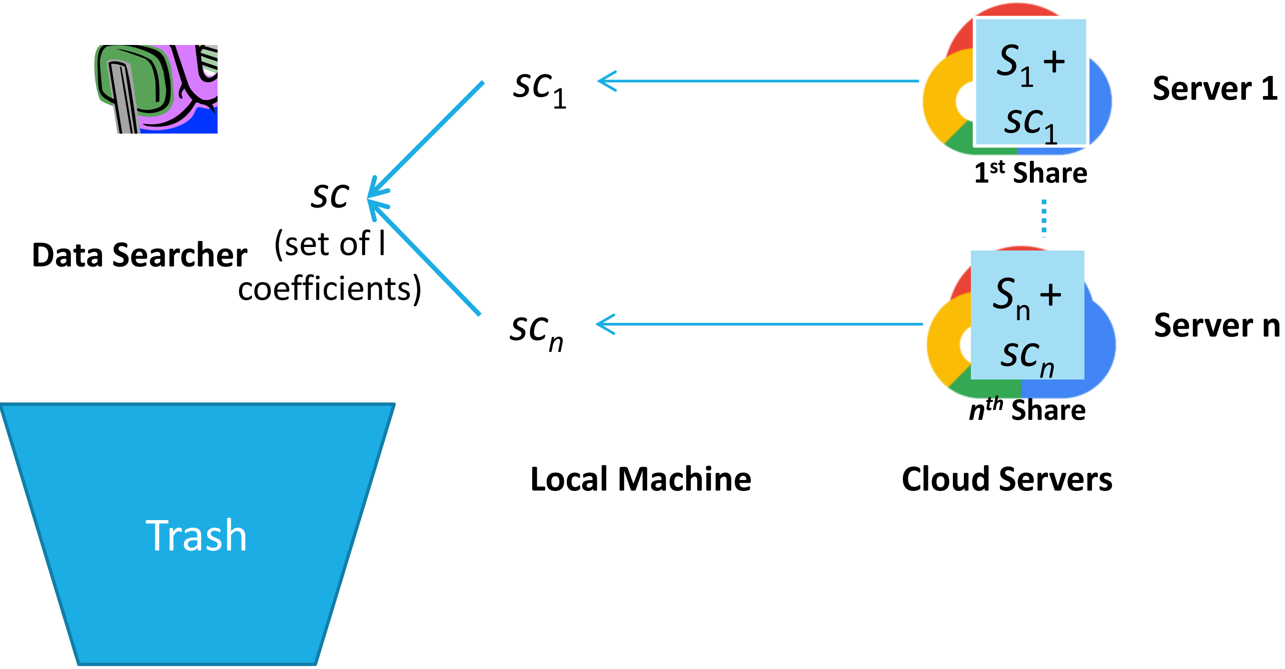


Local Machine

Cloud Servers

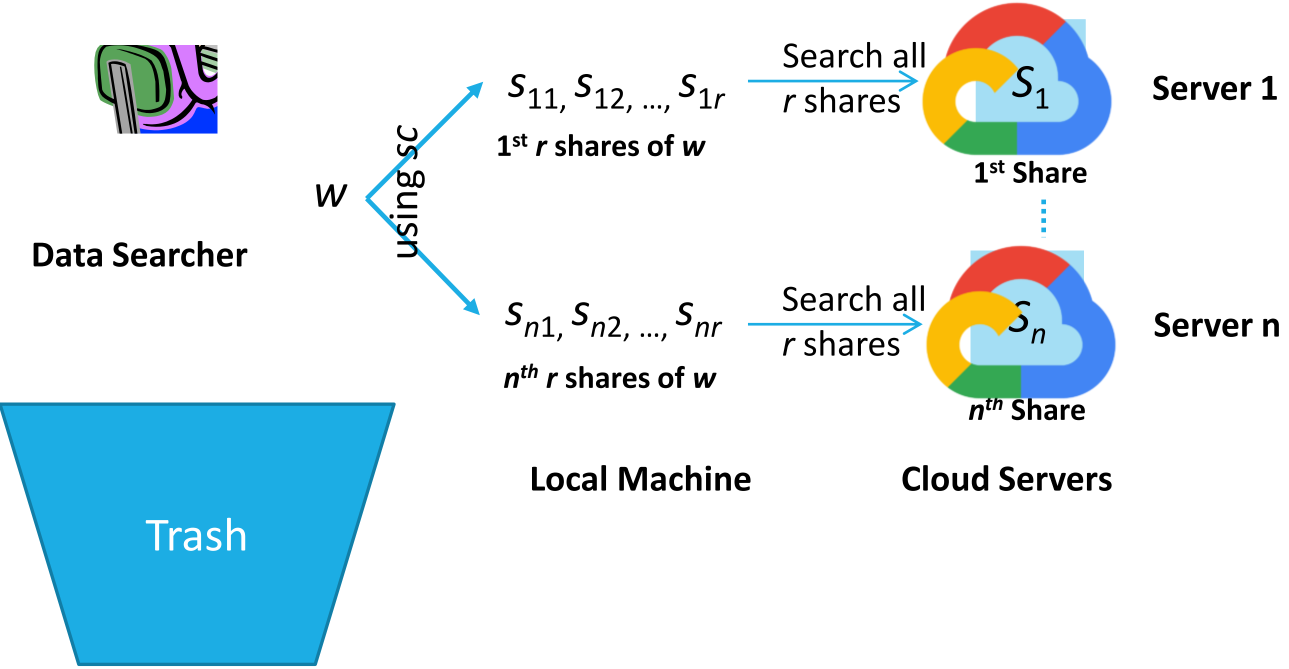
Proposed Work

SecureCSearch Method: Searching Keyword into Shares over Cloud by Data Searcher



Proposed Work

SecureCSearch Method: **Searching Keyword into Shares over Cloud by Data Searcher**



Data Searcher

w using SC

$S_{11}, S_{12}, \ldots, S_{1r}$

1st *r* shares of *w*

$S_{n1}, S_{n2}, \ldots, S_{nr}$

n*th *r* shares of *w

Search all *r* shares

Search all *r* shares

S_1

1st Share

S_n

***n*th Share**

Server 1

Server n

Local Machine

Cloud Servers

Trash

The keyword is found, if exists

Data Searcher will know there is a PDF on cloud that contains the given keyword

It can't reconstruct unless authorized to download *k* shares i.e. $S_1, S_2, \ldots.$

Data Owner

Will also follow the same steps as Data Searcher, but will be able to download the secret PDF containing the keyword by downloading and combining all the *k* shares.