THE UNIVERSITY OF WINNIPEG

Secure Medical Data Visualization over Cloud

Pradeep K. Atrey
University of Winnipeg, Canada
p.atrey@uwinnipeg.ca
www.acs.uwinnipeg.ca/pkatrey/

Winnipeg


UWINNIPEG
THE HEART OF THE CITY,
the heart of the continent
THE UNIVERSITY OF WINNIPEG


Fort McMurray
Manitoba
Grande Prairie
Saskatchewan
Thompson
Edmonton
Flin Flon
Prince Albert
Saskatoon
Calgary
Swift Current
Regina
Brandon
Winnipeg
Ontario
Timmins
Amos
Quebec
Ottawa
Montreal
Fredericton
Halifax
Seattle
Spokane
Vancouver
Portland
Williston
Grand Forks
Minnesota
Duluth
Helena
Butte
Montana
Bismarck
Boise
Twin Falls
Minneapolis
St. Paul
Wisconsin
Milwaukee
Chicago
Toronto
Detroit
Buffalo
Rochester
Hartford
Boston
Providence
Concord
Augusta
Reno
Salt Lake City
Cheyenne
Scottsbluff
Nebraska
Omaha
Iowa
Cleveland
Pittsburgh
New York
Philadelphia
Baltimore
Oakland
Provo
Boulder
Indianapolis
Dayton
Washington D. C.
Las Vegas
Denver
Kansas City
Cincinnati
Richmond
Norfolk
Louisville
St. Louis
U. S. A.
Santa Fe
Oklahoma City
Nashville
Charlotte
Los Angeles
Albuquerque
Memphis
Columbia
San Diego
Phoenix
Little Rock
Birmingham
Atlanta
Mexicali
Tucson
Dallas
Jackson
Tallahassee
Jacksonville
Hermosillo
Austin
Baton Rouge
ATLANTIC
OCEAN

THE UNIVERSITY OF WINNIPEG

Security and Privacy Issues in Multimedia Systems

Social Networks

Source: Youtube

Video surveillance

Source: http://www.peripatetic.us/classes/SP08/time/surveil.htm

e-Health

Clerk fined for 'death watch'

A medical office clerk has been fined $10,000 for repeatedly accessing the private records of the cancer-stricken wife of a man with whom she was having an affair.

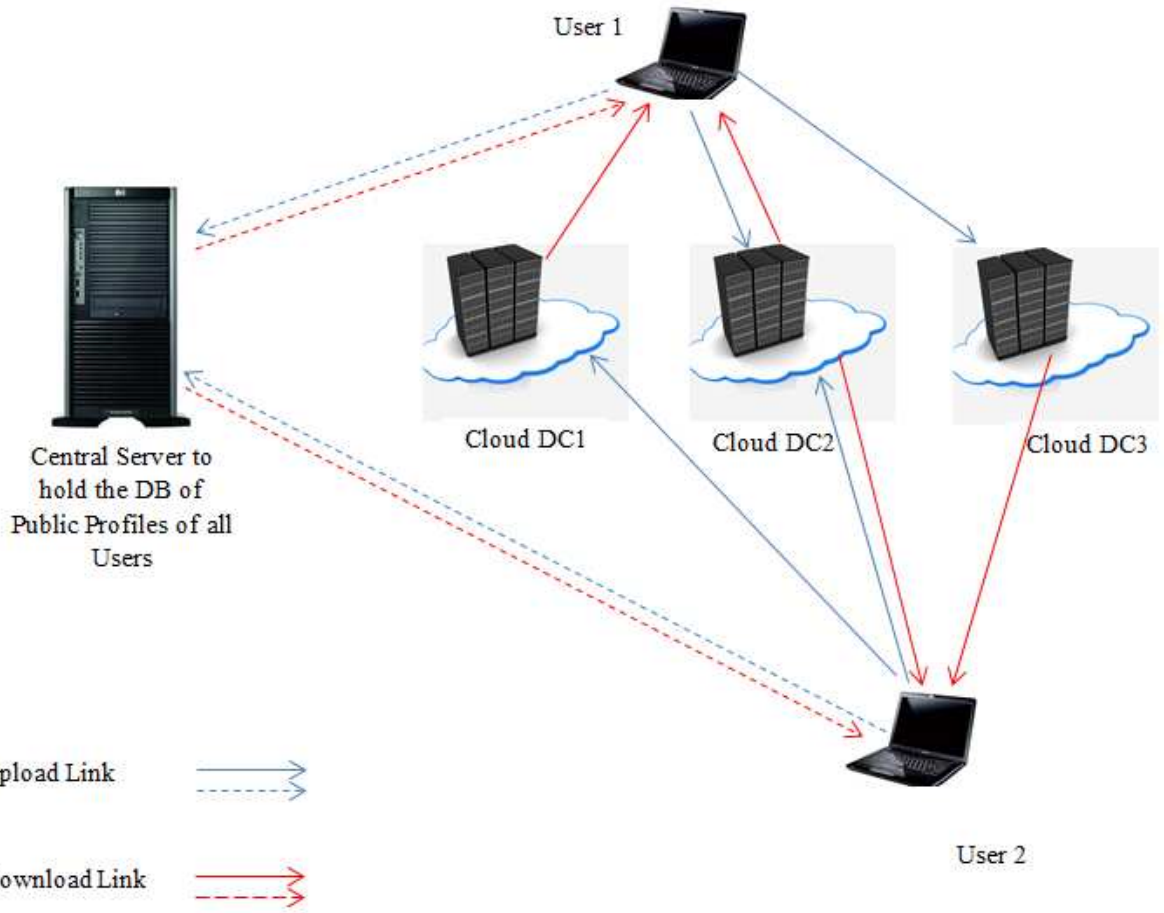
BY THE CALGARY HERALD APRIL 14, 2007

Source: http://www.canada.com/story.html?id=3dda9b24-25ba-4ce1-b717-64588079b2e4

A Secure and Privacy-aware Cloud-based Architecture for Social Networks

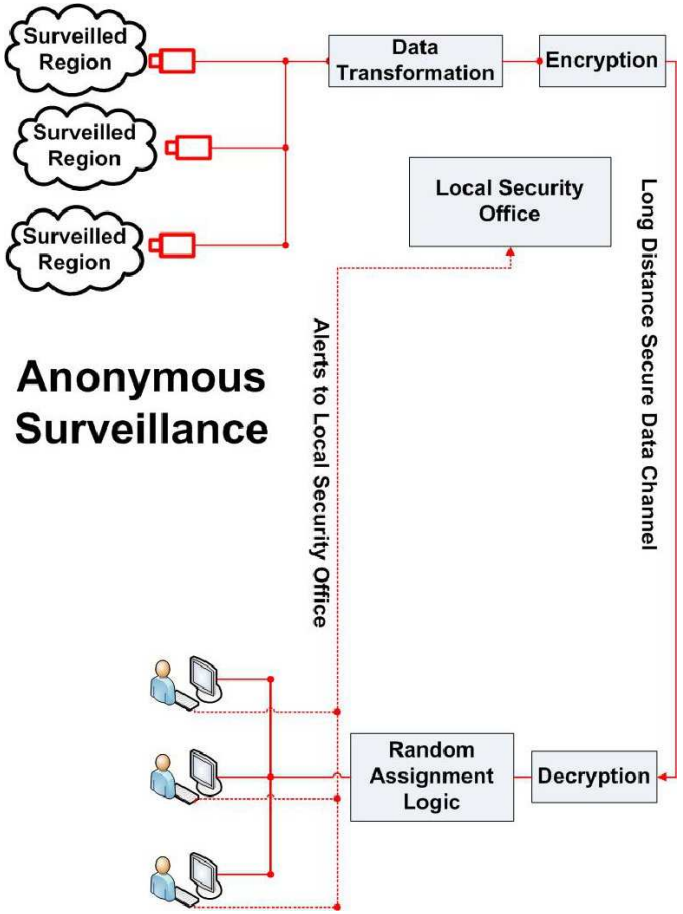
Targeted toward Untrusted Social Networking Operators

Developed a secret sharing based framework



Privacy in Video Surveillance

- Anonymous surveillance (Remote CCTV monitoring)



M. Saini, P. K. Atrey, S. Mehrota and M. S. Kankanhalli. Anonymous surveillance. IEEE ICME Workshop on Advances in Automated Multimedia Surveillance of Public Safety (AAMS-PS'2011), July 2011, Barcelona, Spain.

THE UNIVERSITY OF WINNIPEG

Secure Medical Data Visualization over Cloud

Pradeep K. Atrey
University of Winnipeg, Canada
p.atrey@uwinnipeg.ca
www.acs.uwinnipeg.ca/pkatrey/

THE UNIVERSITY OF WINNIPEG

Collaborators

Manoranjan Mohanty

&

Wei Tsang Ooi

NUS National University of Singapore

Outline

- Introduction and motivation
- Background and related work
- Proposed framework
- Experiments, results and analysis
- Conclusion and future work

Outline

- Introduction and motivation
- Background and related work
- Proposed framework
- Experiments, results and analysis
- Conclusion and future work

THE UNIVERSITY OF WINNIPEG

Shortage of Medical Experts

Region	Number of doctors (2006 census)
Southern Ontario	27,560
Southern Quebec	18,545
Southern British Columbia	9,625
Southern Alberta	7,250
Nova Scotia	2,480
Southern Manitoba	2,405
Southern Saskatchewan	1,965
New Brunswick	1,430
Northern Ontario	1,275
Southern Newfoundland and Labrador	1,270
Northern Quebec	730
Northern British Columbia	420
Northern Alberta	345
Prince Edward Island	215
Yukon	115
Northern Manitoba	105
Northwest Territories	65
Northern Newfoundland and Labrador	20
Nunavut	15
Northern Saskatchewan	10

Northern Canada Southern Canada

http://www.centreforthenorth.ca/blogs/herethenorth/somebodycalladoctor

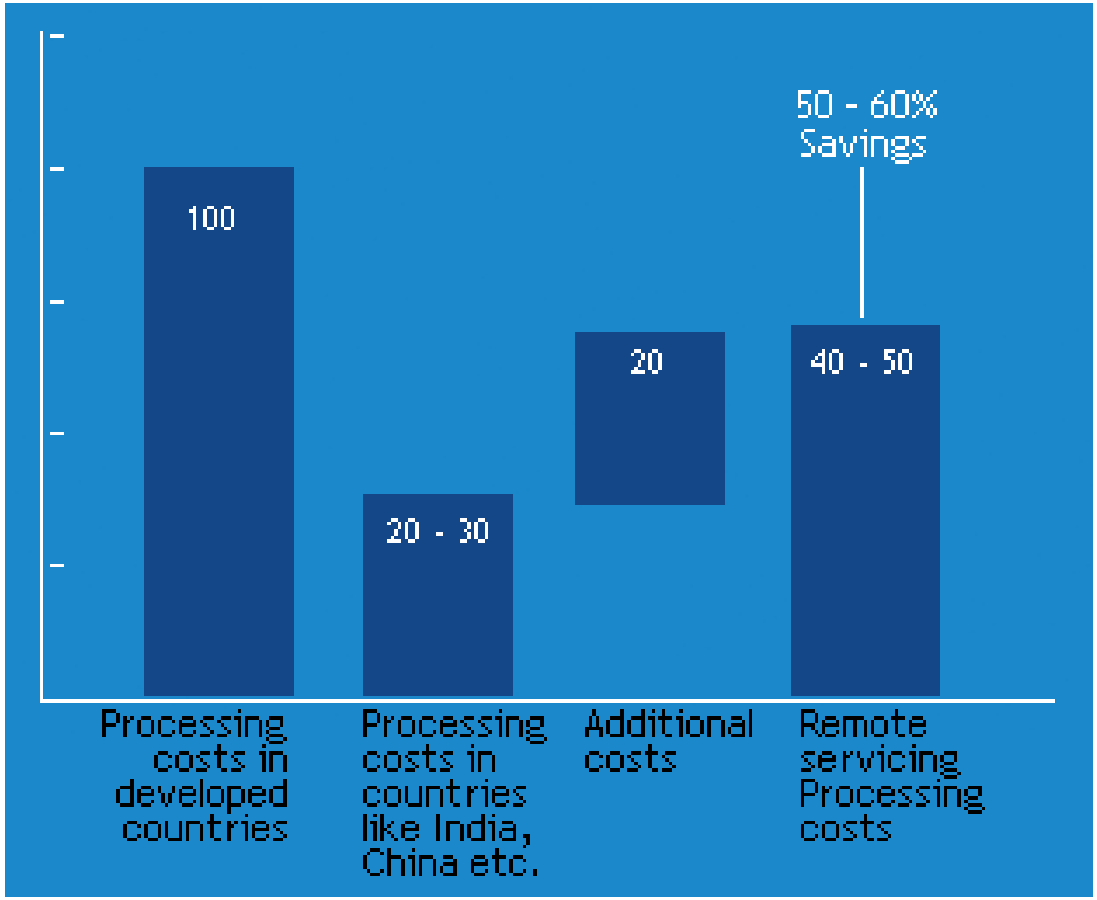
THE UNIVERSITY OF WINNIPEG

Remote Medical Services

http://www.centreforthenorth.ca/blogs/herethenorth/somebodycalladoctor
http://www.amiconnecticut.com/images/ProstateMRI.JPG

Medical Outsourcing

Medical Outsourcing



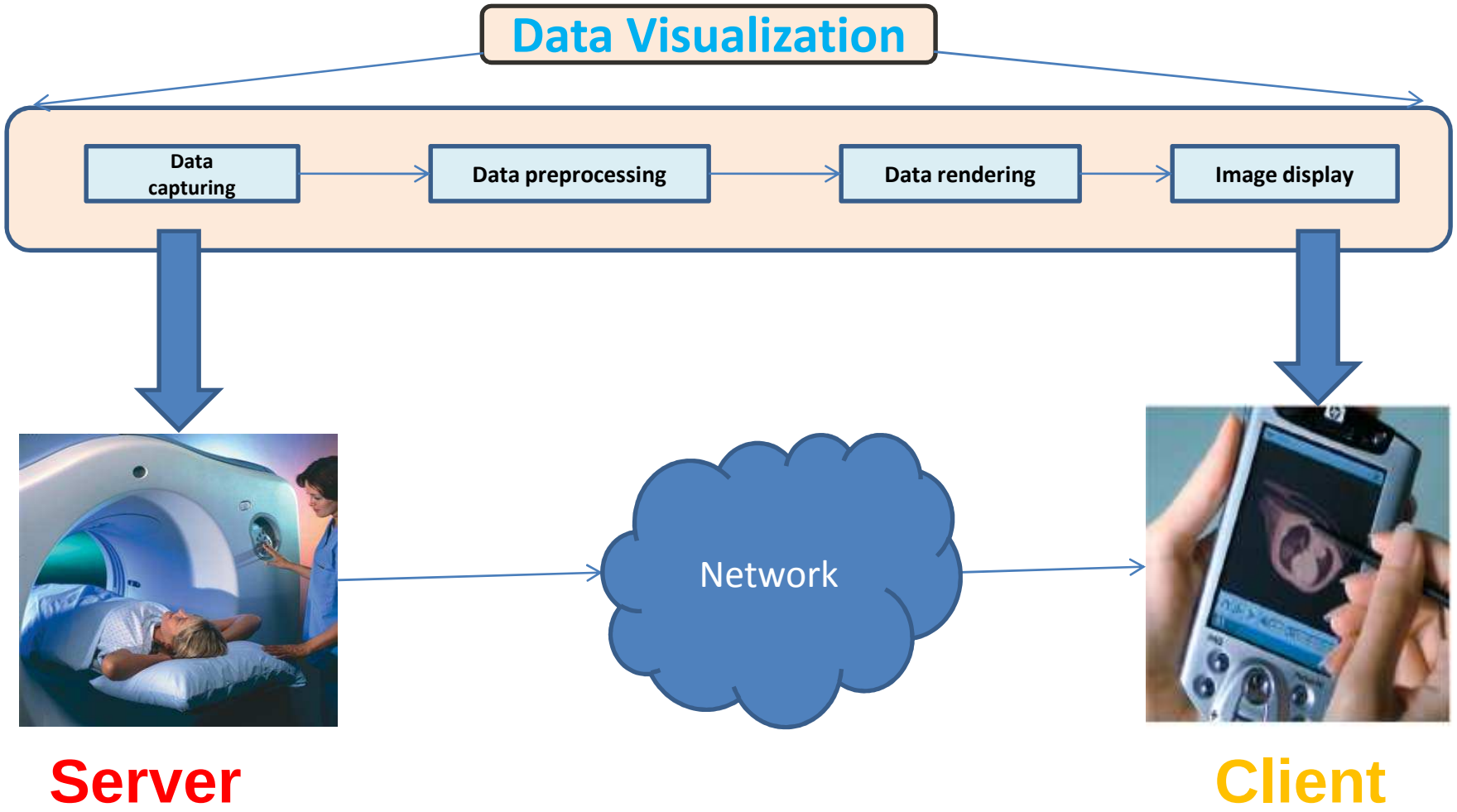
http://www.offshoremedicalbilling.com/images/trends1.gif

Remote Medical Data Visualization is need of the hour

Outline

- Introduction and motivation
- Background and related work
- Proposed framework
- Experiments, results and analysis
- Conclusion and future work

Remote visualization: Client-server approach



THE UNIVERSITY OF WINNIPEG

Two Choices for Rendering: Client-side Rendering

- Low visualization latency

- Low quality image

THE UNIVERSITY OF WINNIPEG

Two Choices for Rendering: Server-side Rendering

Data capturing

Data preprocessing

Data rendering

Server

Rendered

User intera

Rende

age

Image display

Client

Server Side Rendering preferred in 3D remote medical data visualization due to:

✓Low-end client hardware
✓ Quality of image more important than latency

- High visua
- High quality

THE UNIVERSITY OF WINNIPEG

Server-side Rendering: Observations

City A

Motivation For:

Cloud-based rendering

Server

Clients

- Ob… …erver by hospita…
- Ob… …e main contributor to visualization …icy for geographically distant server and client.

Cloud-based Rendering Framework

Data capturing

Data preprocessing

Server

Cloud

Image display

Client

Preprocessed data

Data rendering

Rendered image

THE UNIVERSITY OF WINNIPEG

Cloud-based Rendering: Past Work

- **3Di-Cloud** - Shina System's cloud-based image management and advanced (3D/4D) visualization software s
  (http://www.3di-imaging.co
- **3Dnet Medica** imaging service and community
  via .html)
- A Cloud-D ynamically
  inz; Ukis,
  Vlad g approach
  using Clo
  (http:// bs_a ?arnumber=6068330

Security is an issue:

Third-party cloud data centers.

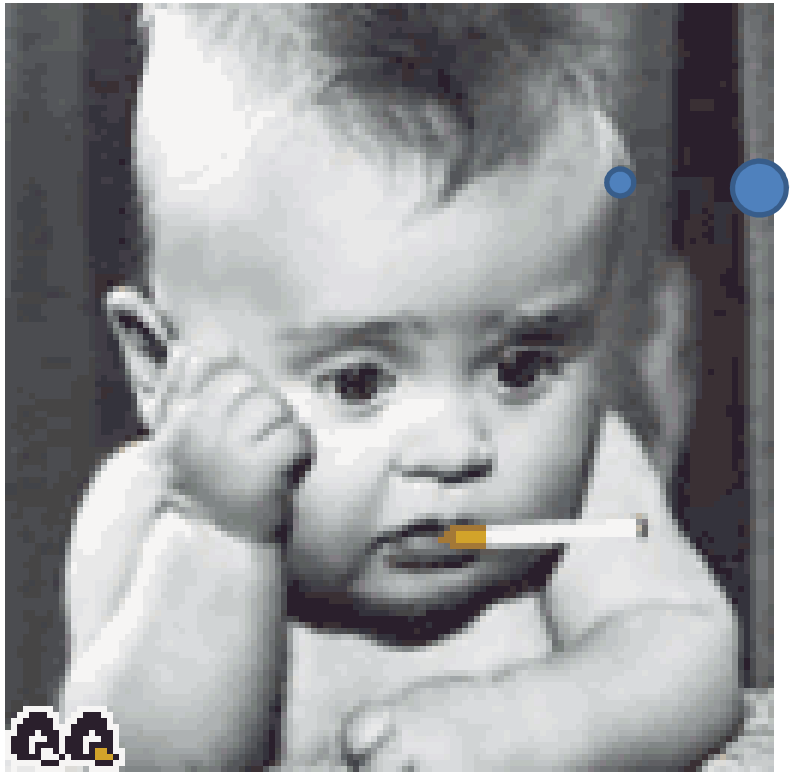
Security and Privacy Concerns

- How many of you would mind if your medical image data is available to an adversary?

- Who can be an adversary?

http://greenberg-art.com/.Toons/ Toons,%20social/ qqxsgMedical%20privacy.gif

What to do?



How to perform secure medical data visualization over cloud?

Outline

- Introduction and motivation
- Background and related work
- Proposed framework
- Experiments, results and analysis
- Conclusion and future work

Research Goal and Contribution

- Goal:
  - To address the security issue in cloud-based 3D medical data visualization
- Contribution:
  - A secure cloud-based medical data visualization framework that integrates cryptographic secret sharing scheme into 3D data rendering pipeline

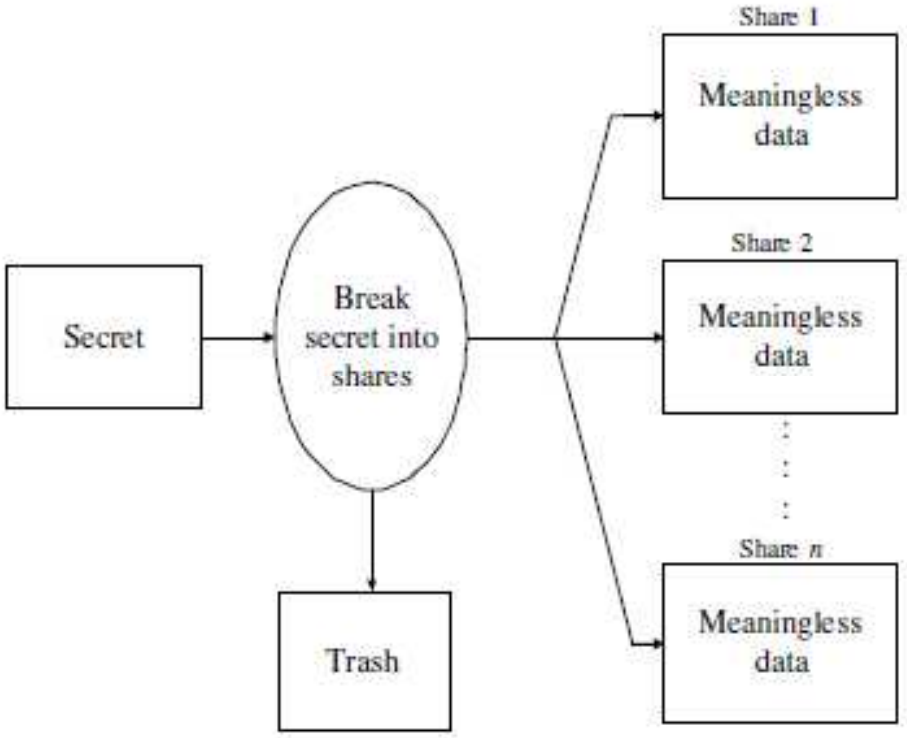
THE UNIVERSITY OF WINNIPEG

Shamir's Secret Sharing

- Suppose we want to use (k,n) threshold scheme to share our secret **S** where $k < n$
- Choose at random (k-1) coefficients $a_1, a_2,\ldots, a_{k-1}$ and let **S** be the a_0

  $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1} \bmod p$

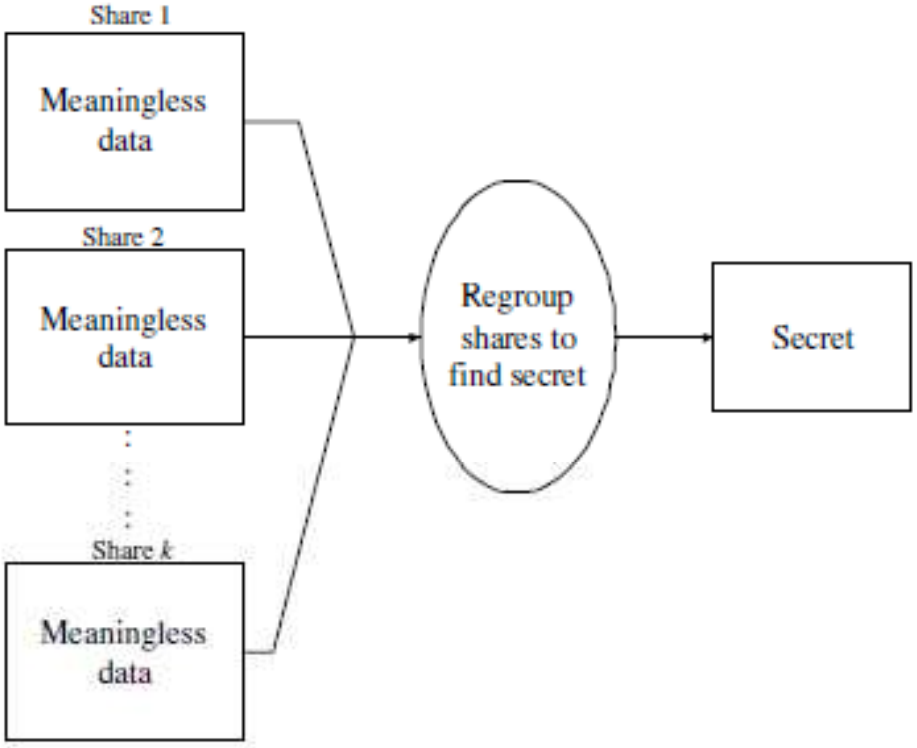
- Construct n shares (i, $f(i)$) where $i = 1, 2,\ldots, n$.



Breaking the secret into n shares

Shamir's Secret Sharing (Cont…)

- Given any subset of *k* of these pairs, we can find the coefficients of the polynomial by Lagrange interpolation, and then evaluate a_0 = **S**, which is the secret.

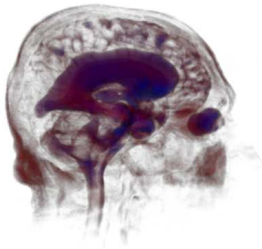


Reconstructing the secret using $k \leq n$ shares

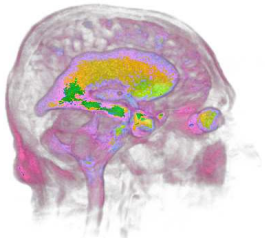
Secret Sharing holds homomorphism property on binary addition and scalar multiplication which allows multiple secrets to be combined by direct computation on the shares.

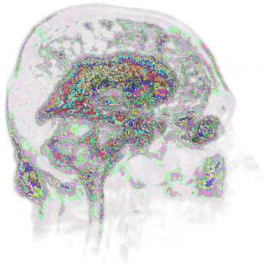
Cloud-based Secure Rendering: Goal

- To hide critical color coded information of medical image from cloud data centers.



Original image

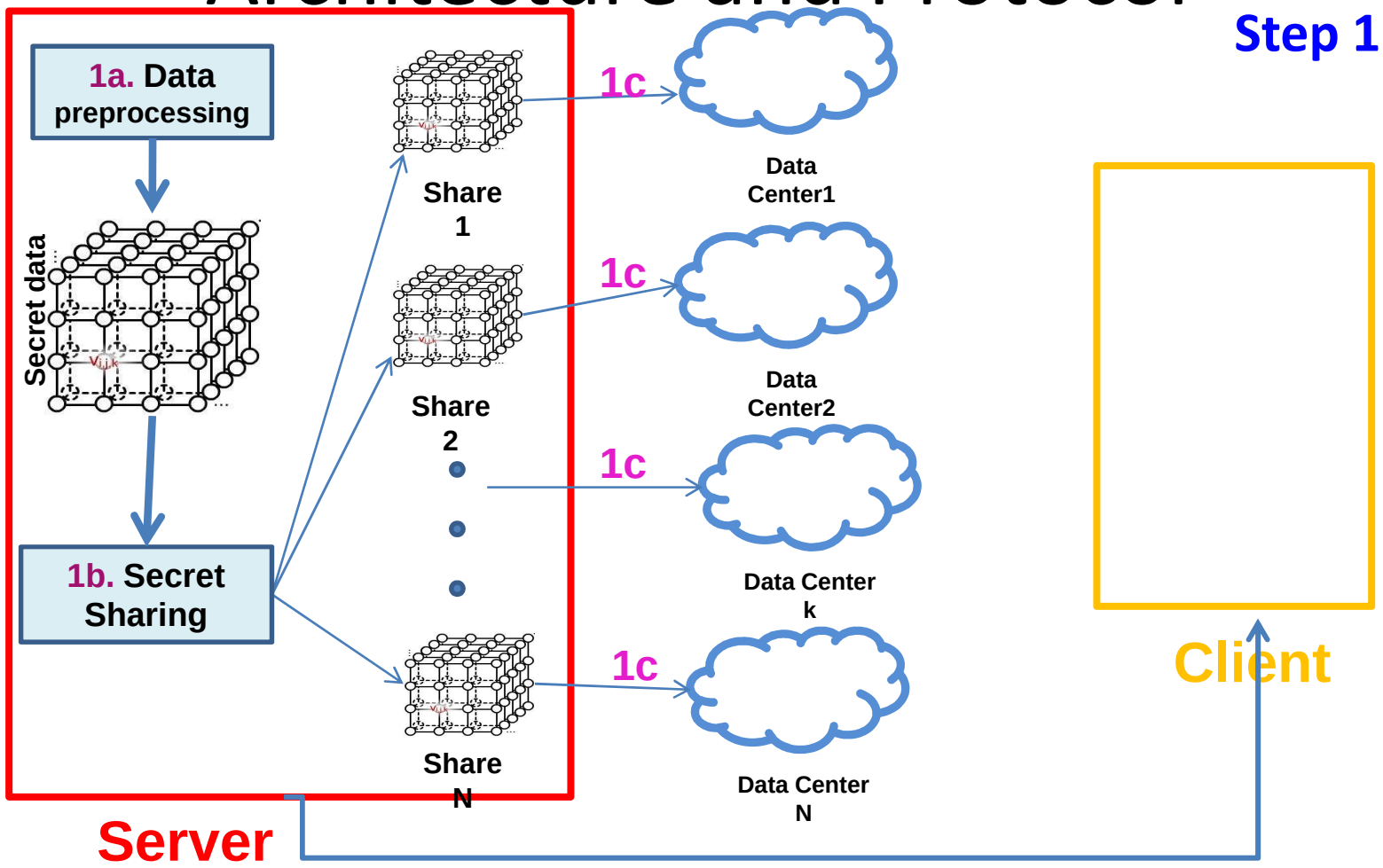




Color transformed images

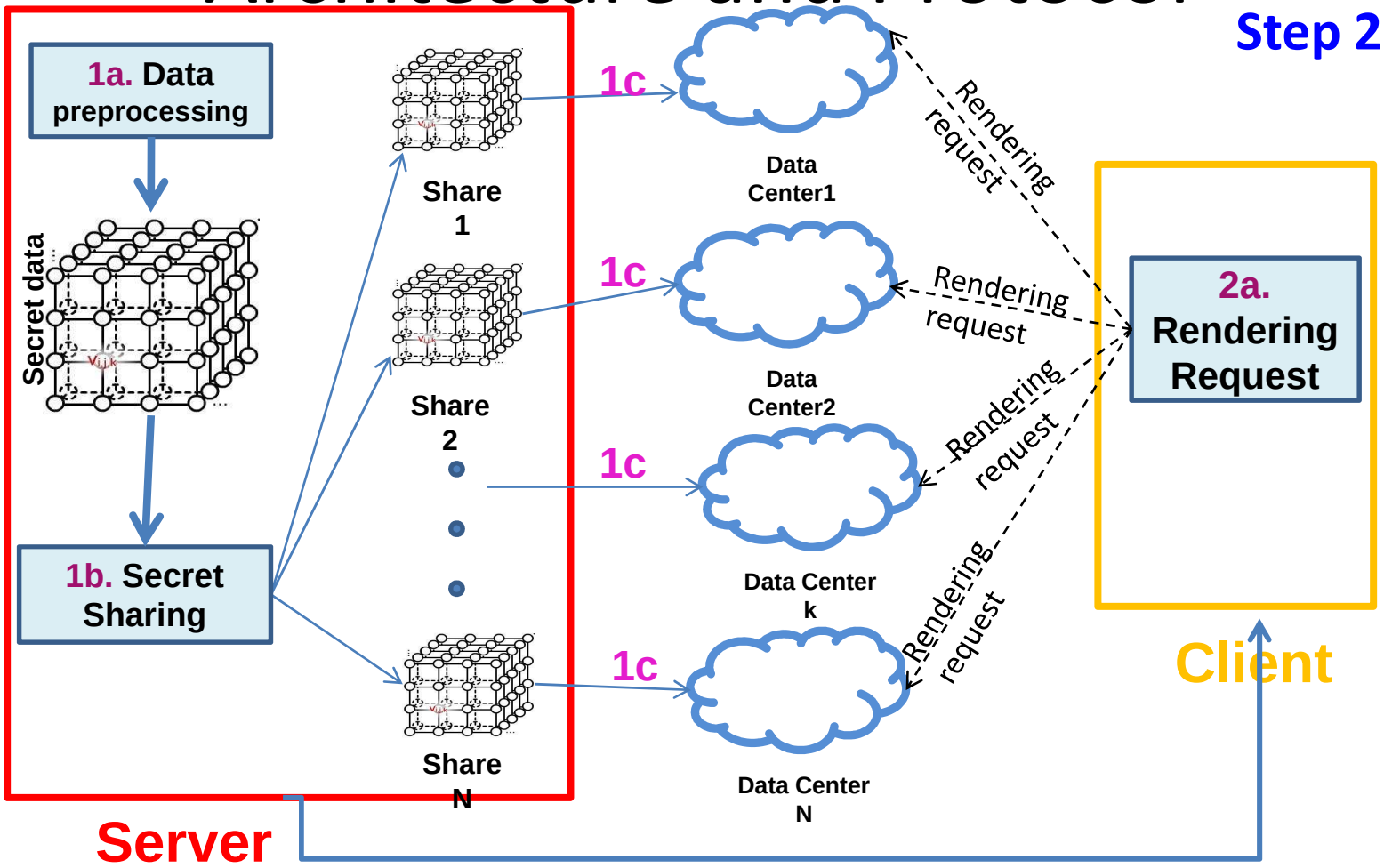
THE UNIVERSITY OF WINNIPEG

Cloud-based Secure Rendering (*CSR*): Architecture and Protocol



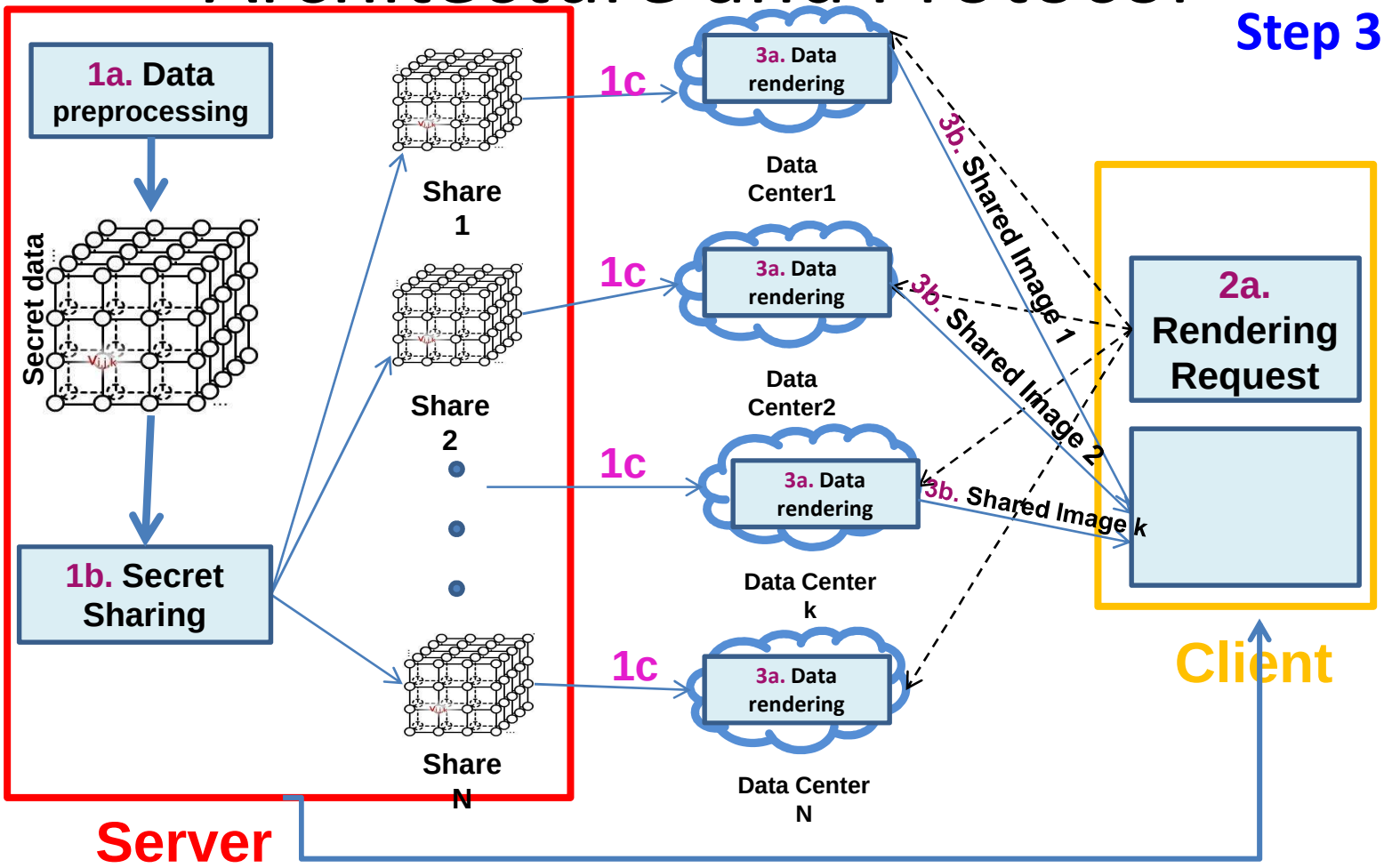
THE UNIVERSITY OF WINNIPEG

Cloud-based Secured Rendering (*CSR*): Architecture and Protocol



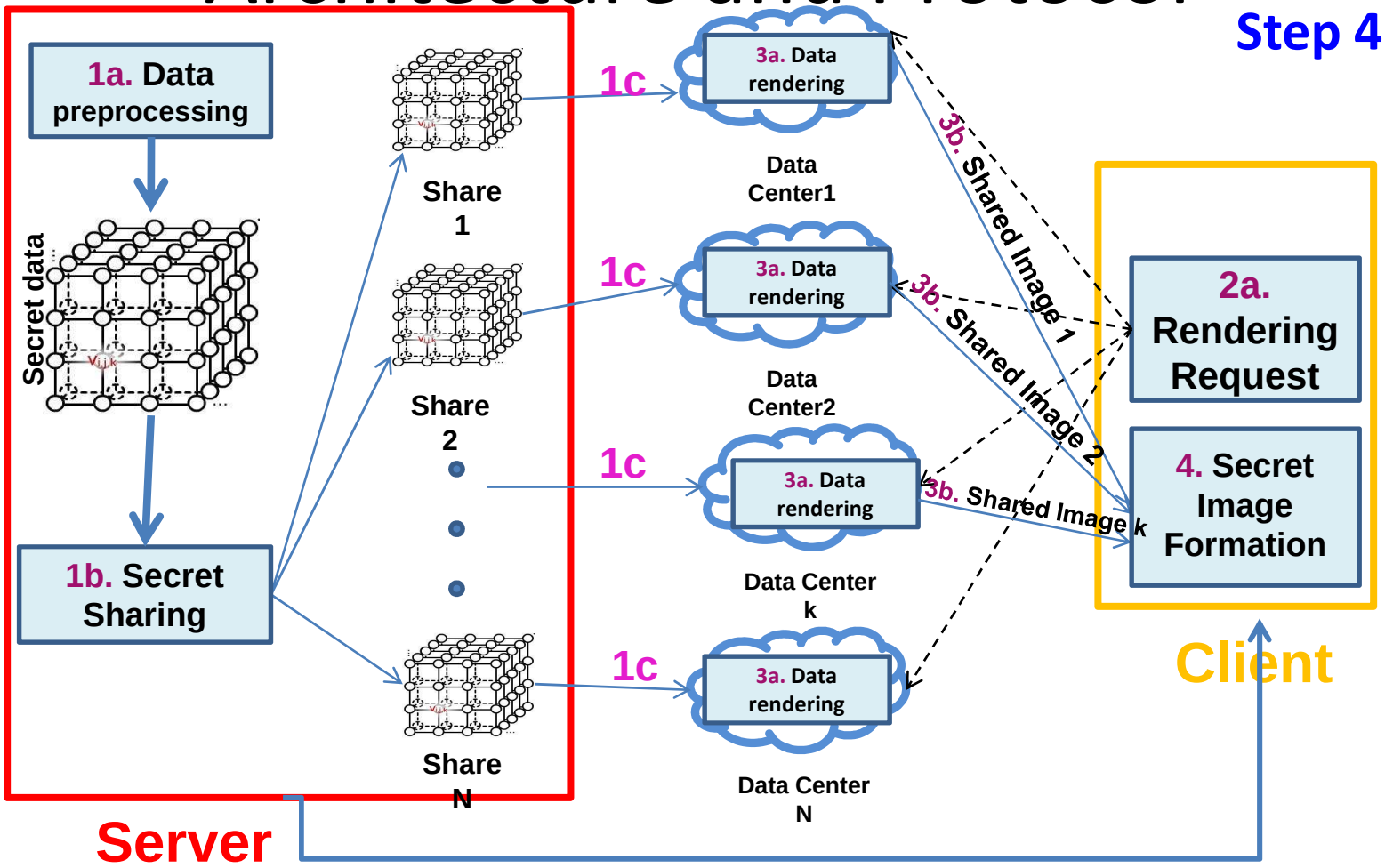
THE UNIVERSITY OF WINNIPEG

Cloud-based Secured Rendering (*CSR*): Architecture and Protocol



THE UNIVERSITY OF WINNIPEG

Cloud-based Secured Rendering (*CSR*): Architecture and Protocol

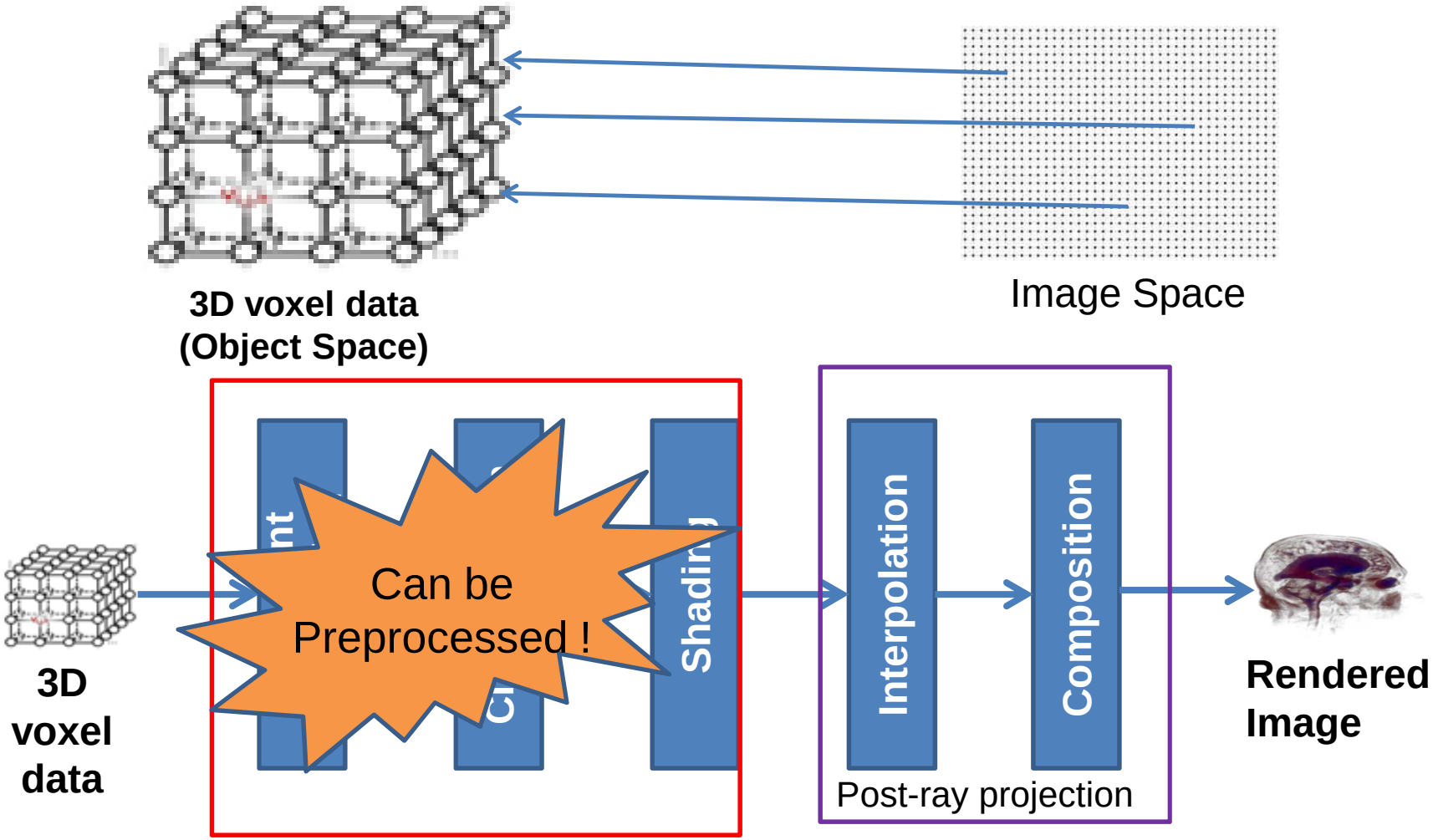


Cloud-based Secured Rendering (*CSR*)

- Observation: data rendering must be integrated into Shamir's Secret Sharing.

- We propose secure volume ray casting by integrating one of the popular 3D data rendering technique, i.e. *pre-classification volume ray-casting* , into secret sharing.

Pre-classification Volume Ray-casting: Pipeline



Secure Volume Ray-casting: Challenges

- **Challenge 1:** Interpolation and composition consists of real number arithmetic operations and Shamir's secret sharing is not compatible with real number
- Solution: Modify pre-classification volume ray-casting to make it compatible with Shamir's secret sharing.
- **Challenge 2:** Which preprocessed information to secret share so that each share voxel grid is render-able and rendering can also be accelerated.
- Solution: Secret share preprocessed data (each RGB component) of pre ray-projection step into *n* number of shares. Opacity value is not shared.

Modification of pre-classification volume ray-casting

- **Goal:** Modify ray-casting so that Shamir's secret sharing is applicable to it.
- Solution:
  - Convert the real data used in interpolation to integer by rounding it off by d decimal places and multiplying 10^d to the rounded off value.
  - Convert the real data used in composition to integer by rounding it off by f decimal places and multiplying 10^f to the rounded off value.
  - In secret sharing, use a prime number that is greater than $255 \times 10^{d+f}$
- *Is this scheme lossless?*
- $C_r(X, V) = C(X, V) + E^{tot}(C(X, V), d, f)$. *where,* $E^{tot}(C(X, V), d, f)$ *is the error in rendered color.*

Cloud-based Secured Rendering (*CSR*)

- Information theoretically secured

- High data overhead

  ✓ Client needs *3kb+8* number of bits to reconstruct color of one pixel (where, *b* is no of bits required by one color component of one pixel of a shared image)

  ✓ **For an acceptable image quality:** Total data size *five* times more than the data size of conventional rendering .

- *CSR* need to be optimized

THE UNIVERSITY OF WINNIPEG

Optimization 1: *CSR-RGB*

- Observation: The rendering operation of individual color component (i.e. *R*, *B*) are sa
  - Se re R, G si unction:

$H(\infty$

- Prime

- Data overhead s bits required for c col mpo of a s ed image)

Data overhead still high
for
latency sensitive applications

Optimization 2: *LW-CSR-RGB*

- An alternate way of integrating secret sharing with pre-classification volume ray-casting
  - Modify Shamir's secret sharing by excluding modular prime operation
  - Pre-classification volume ray-casting is not modified
- Use $(k, k+1)$ secret sharing method
- Restrict the value of x to restrict the pixel value of a share image
- Convert real value of rendered color component to integer by rounding it off by e decimal places and multiplying 10^e to the rounded off value

Optimization 2: *LW-CSR-RGB*

- Requires 35% less no of bits than *CSR-RGB*

- Is it as secure as *CSR* / *CSR-RG*B ?

- No. It does not use modular prime operation

Outline

- Introduction and motivation
- Background and related work
- Proposed framework
- Experiments, results and analysis
- Conclusion and future work

Experimental Setup

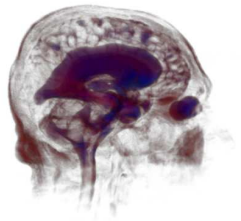
- Hardware
  - Server, Cloud data center, and Client simulated in a note book powered by:
    - Intel Core 2 Duo 2.00 GHz processor
    - 4 GB of RAM
    - Mobile Intel 965 Express Chipset Family display adapter

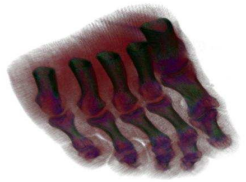
- Software
  - Customized VTK *5.8.0* visualization package that has:
    - Pre-classification volume ray-casting
    - Integrated (3,5) Secret Sharing for *CSR*, *CRS-RGB* and (3,4) secret sharing for *LW-CSR-RGB*.

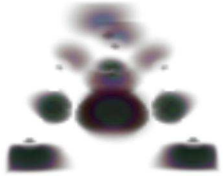
THE UNIVERSITY OF WINNIPEG

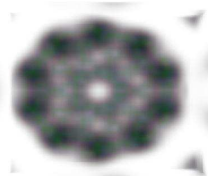
Data Set

	Dimension	Size
Head	256 X 256 X 124	7.8 MB
Foot	256 X 256 X 256	16 MB
Iron port	68 X 68 X 68	307.3 KB
Bucky	32 x 32 X 32	32.2 KB

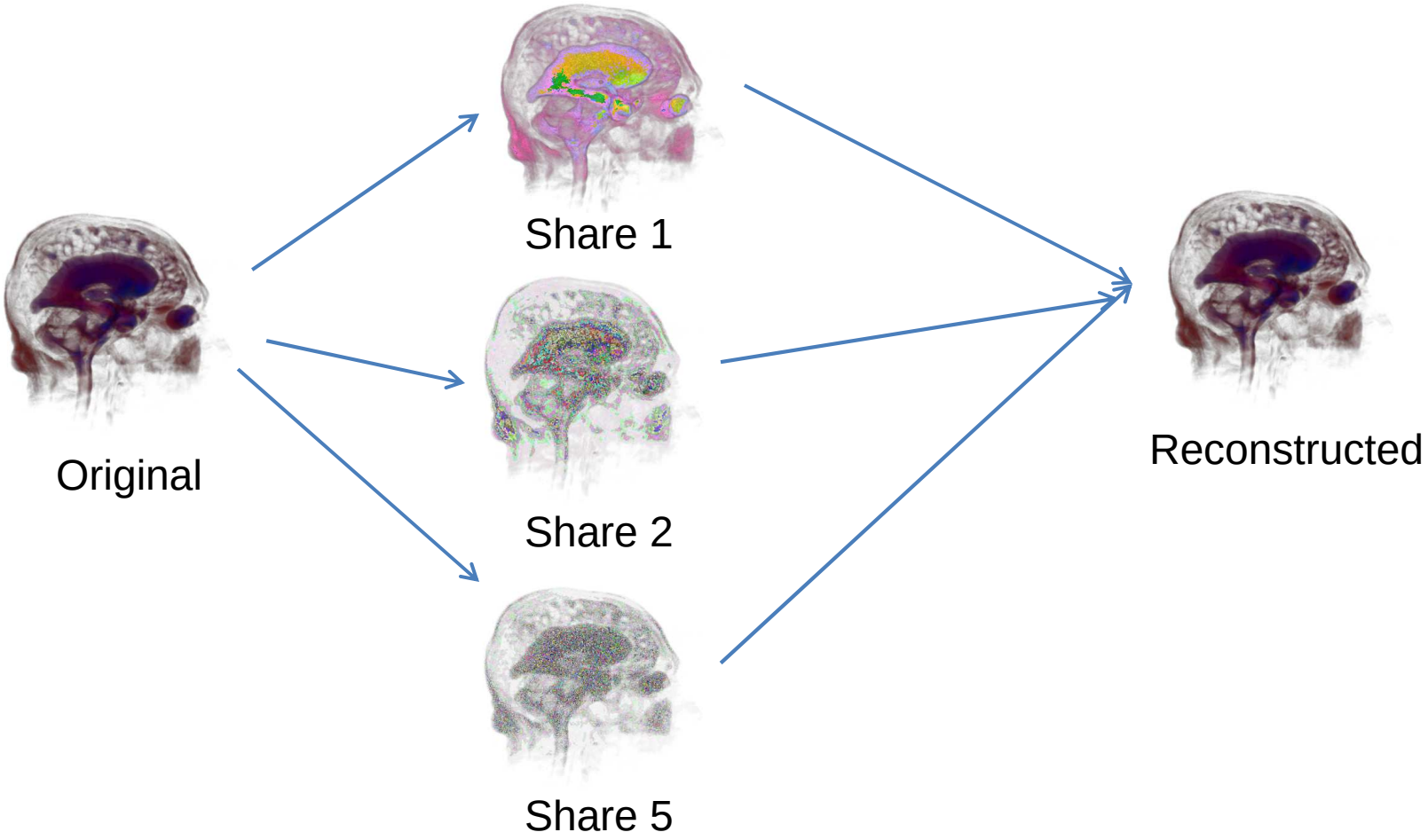




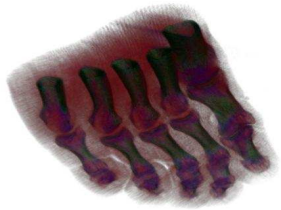


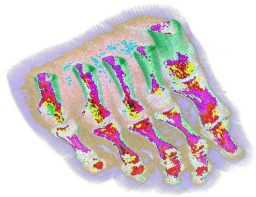


Results: Single view point



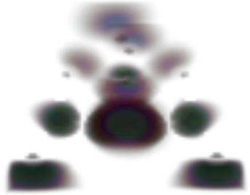
Results: Single view point

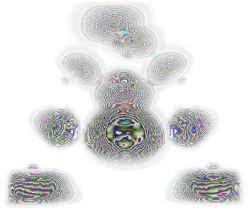




Original (foot)

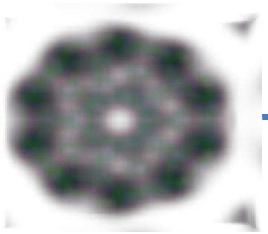
Share

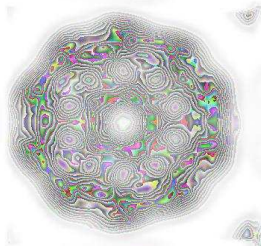




Original (iron port)

Share

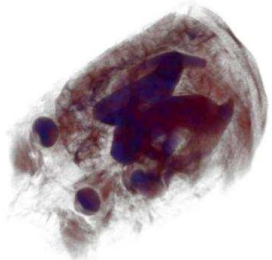


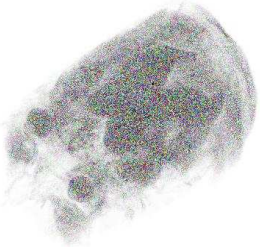


Original (Bucky)

Share

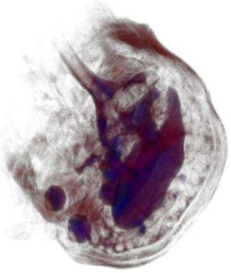
Results: Multi view point

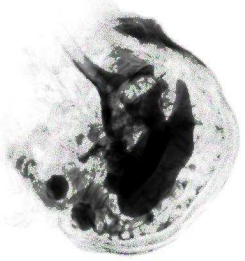




Original (Head View 1)

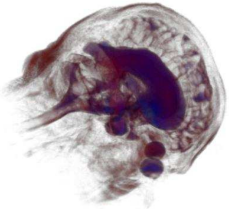
Share 10

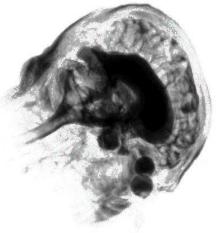




Original (Head View 2)

Share 30





Original (Head View 3)

Share 50

THE UNIVERSITY OF WINNIPEG

Demo

Head MRI volume data

Rendered Image (Secret Image) Conventional Server-Side Rendering	Share Image Rendered in a Data Center Cloud-based Secure Rendering	Image Reconstructed at Client

Foot volume data

Rendered Image (Secret Image) Conventional Server-Side Rendering		

Analysis

We performed:

- ✓ Security Analysis.
- ✓ Privacy Analysis.
- ✓ Error Analysis.
- ✓ Performance Analysis.
- ✓ Latency Analysis.

n **:** total number of available data centers.
k **:** minimum no of data centers required by client

Security Analysis

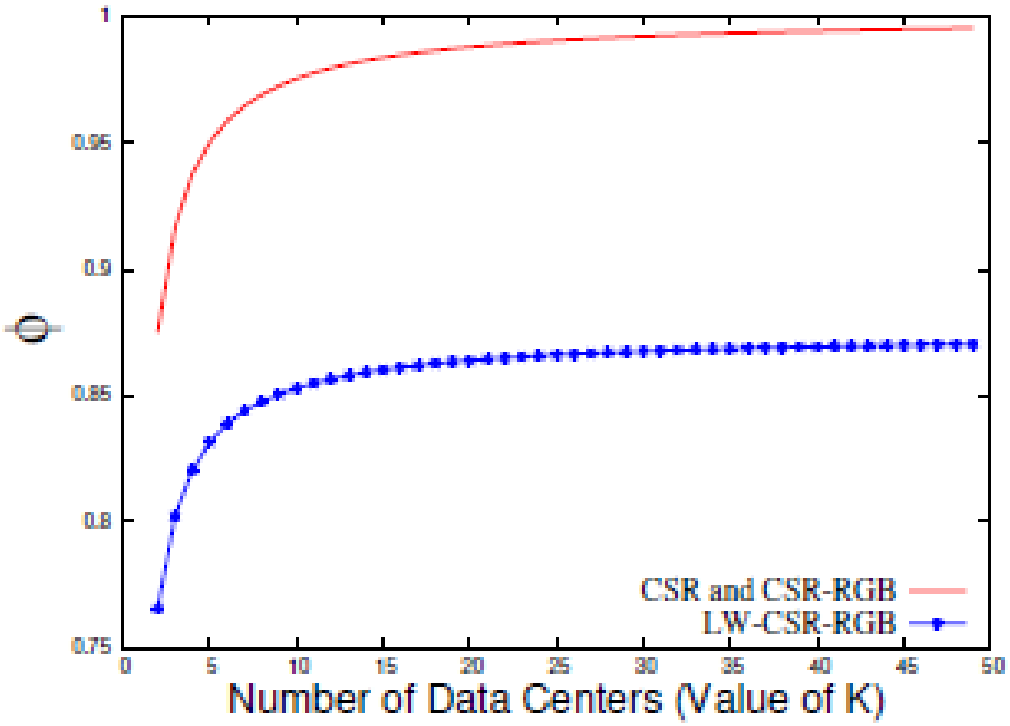
- Information theoretical security:
  - ✓ *CSR* is information theoretically secured – Use of a higher prime number does not affect.
  - ✓ *CSR-RGB* and *LW-CSR-RGB* are information theoretically secured with some information loss - For *LW-CSR-RGB* with $k = 3$, the probability of an adversary being able to infer a secret pixel: ***1 / 1648020.***
- Perseverance of data integrity:
  - ✓ *CSR* and *CSR-RGB* preserve data integrity with probability $\omega_i = 1 - h_a * g_i^n$, where, g_i is the probability that adversary is able to tamper medical data of a single cloud data center and h_a is the probability that all tampering are equivalent and homomorphic to secret sharing.
  - ✓ LW-CSR-RGB preserve data integrity with probability $\omega_i{}' = 1 - h_a * g_i^{k+1}$.
  - ✓ **If $n = k$, then $\omega_i = \omega_i{}' = 1 - g_i$**

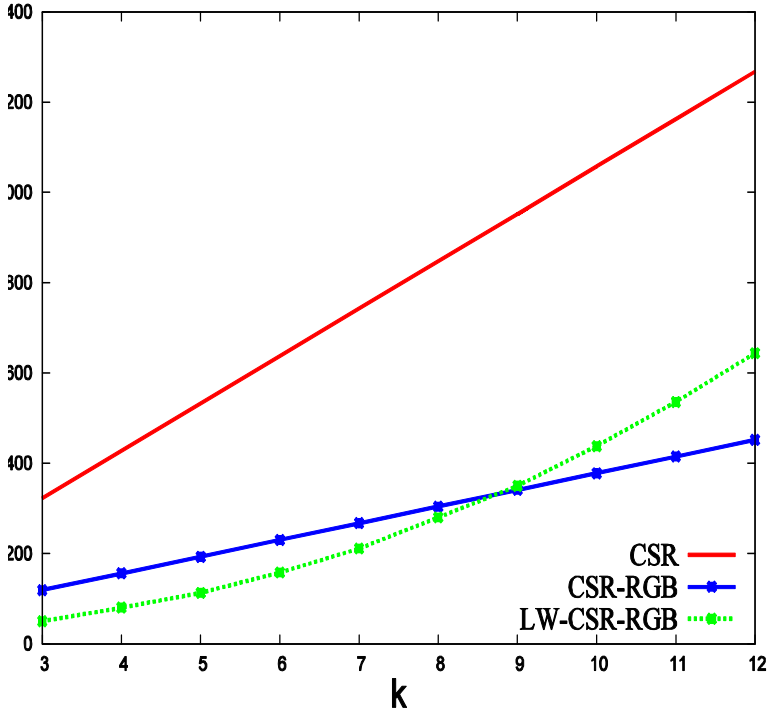
Security Analysis Cont.

- Perseverance of data recoverability:
  - ✓ *CSR* and *CSR-RGB* preserve data recoverability with probability $\omega_r = 1 - g_r^{n-k+1}$, where, g_r is the probability that a cloud data center is unable to send its share image to client.
  - ✓ *LW-CSR-RGB* preserve data recoverability with probability $\omega_r^l = 1 - g_r^2$.
- Perseverance of data confidentiality:
  - ✓ *CSR*, *CSR-RGB*, and *LW-CSR-RGB* preserve data confidentiality with probability $\omega_c = 1 - g_c^k$, where, g_c is the probability that adversary is able to read medical data of one cloud data center.

THE UNIVERSITY OF WINNIPEG

Security Analysis Cont.





$n = 12$, $g_c = 0.2$, $g_i = 0.15$, $g_r = 0.3$, and $h_a = 1$

Effect of *k* on overall security.

Privacy Analysis

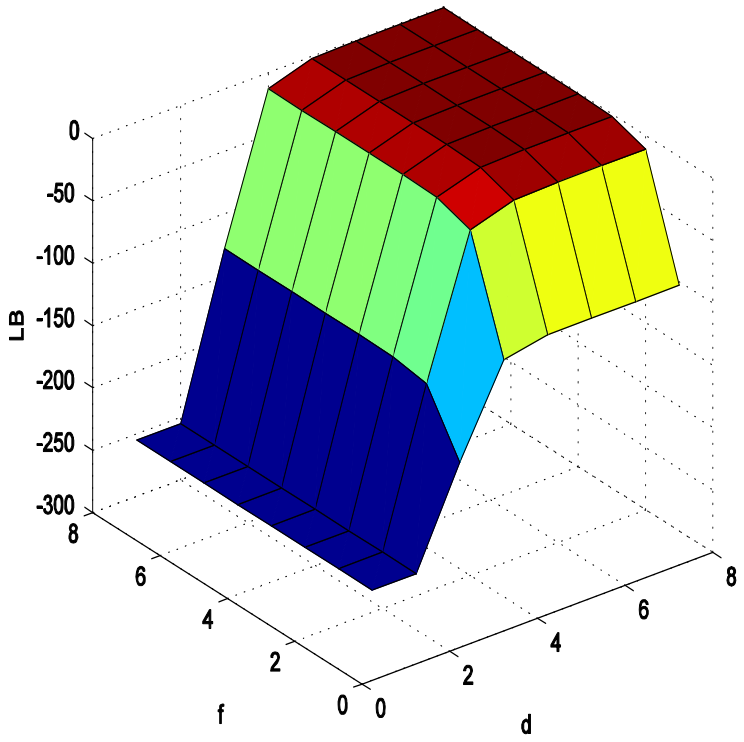
- Privacy loss of a patient $\Gamma = \Gamma_i * \Gamma_d$, where, Γ_i is degree of identity loss and Γ_i is degree of loss of disease information.

- CSR, CSR-RGB, and LW-CSR-RGB minimize Γ by:
  - ✓ not disclosing the explicit identity (I_{who} information) of a patient (minimization of Γ_i) to cloud data center.
  - ✓ not disclosing the disease information of a patient to cloud data center (minimization of Γ_d).

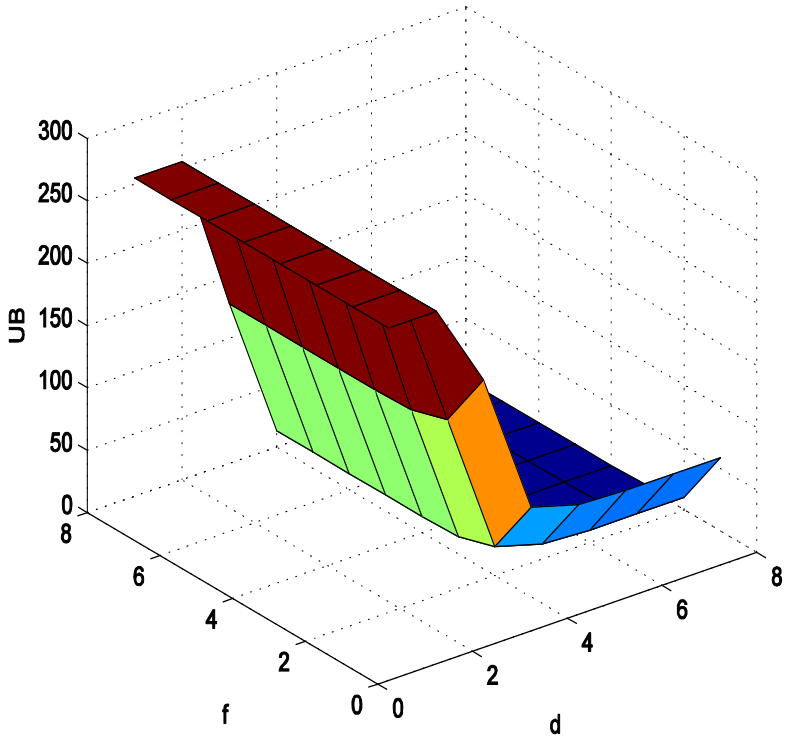
THE UNIVERSITY OF WINNIPEG

Error Analysis

- Error introduced by *CSR* and *CSR-RGB*



Lower bound



Upper bound

Error Analysis

❖Error introduced by *LW-CSR-RGB is bounded by:*

$$\pm\left(\left\lfloor\left|\pm 5\times 10^{-(c+1)}\times\sum_{i=1}^{k} t_i\right|\right\rfloor+1\right)$$

where, t_i is the interpolating factor of i^{th} share image.

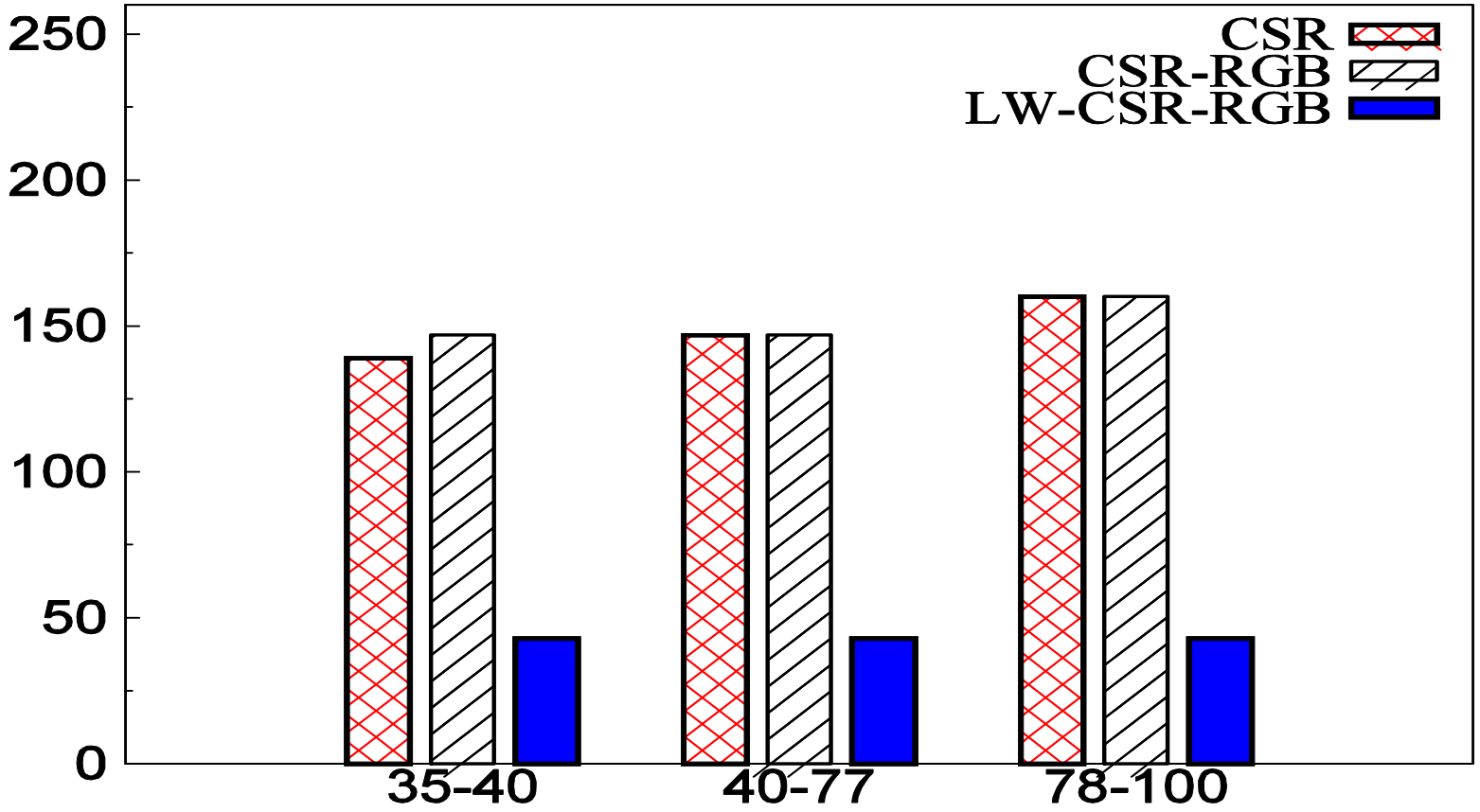
Performance Analysis

- Computation steps :
  - Creation of shares from secret (performed by server as preprocessing step)
  - Ray-casting of shares (Similar to normal non-secure ray-casting)

- Overhead
  - **Two types:** data overhead and computational overhead
  - Both independent of dimension and size of volume data
  - Both overheads proportional to dimension of image space

THE UNIVERSITY OF WINNIPEG

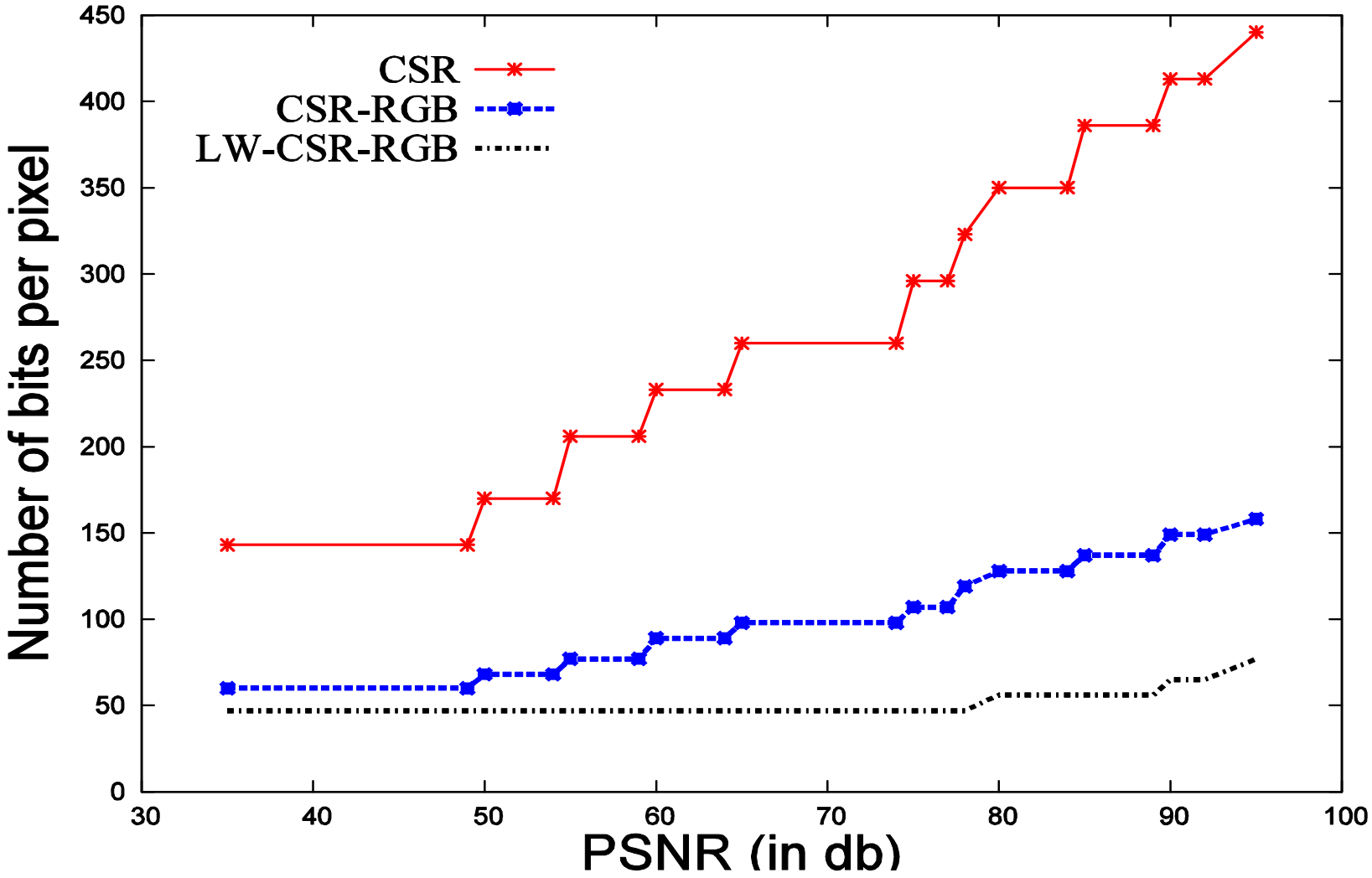
Performance Analysis: Computational Overhead



✓PSNR (X-axis) vs. computational overhead (in ms)

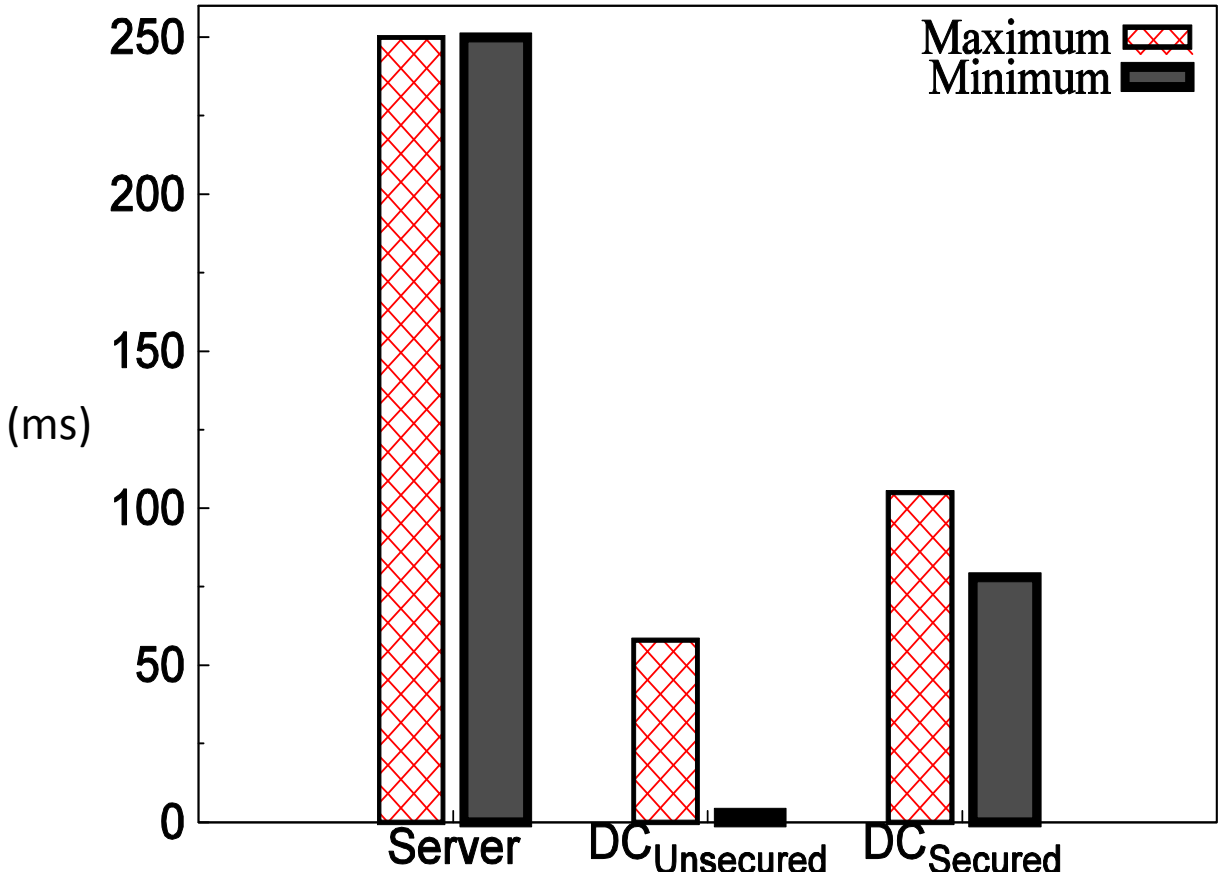
✓ Performed on *512 X 512* image space

Performance Analysis: Data Overhead



THE UNIVERSITY OF WINNIPEG

Latency Analysis: Unlimited bandwidth



1. Server at Singapore
2. Client at Winnipeg
3. Cloud data centers at Toronto, Vancouver, Winnipeg, California, and New York.

Visualization latencies of *Conventional Server-side Rendering*, *Cloud-based Rendering* ($DC_{Unsecured}$), and *Secure Cloud-based Rendering* ($DC_{Secured}$).

Outline

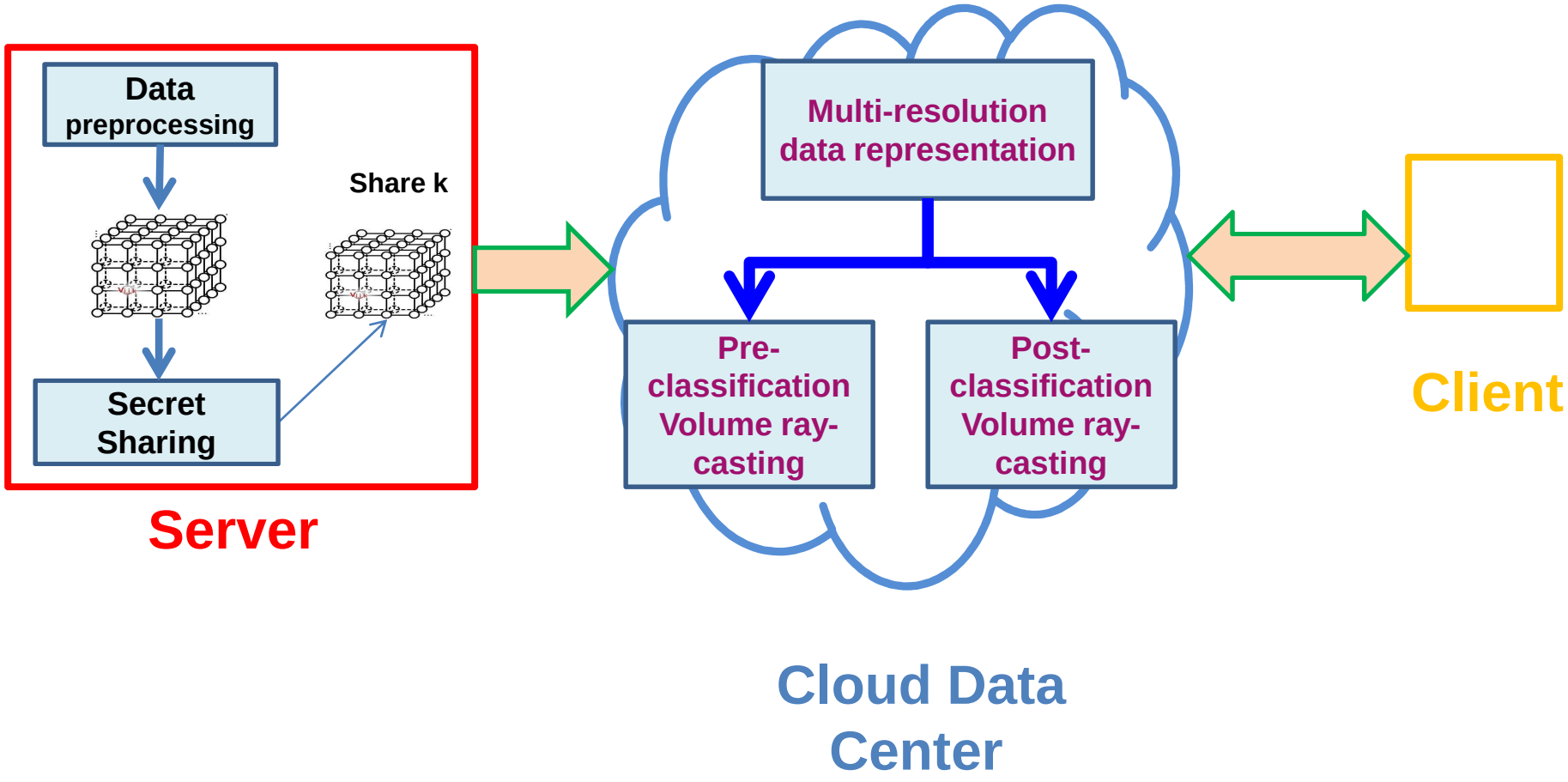
- Introduction and motivation
- Background and related work
- Proposed framework
- Experiments, results and analysis
- Conclusion and future work

Conclusion

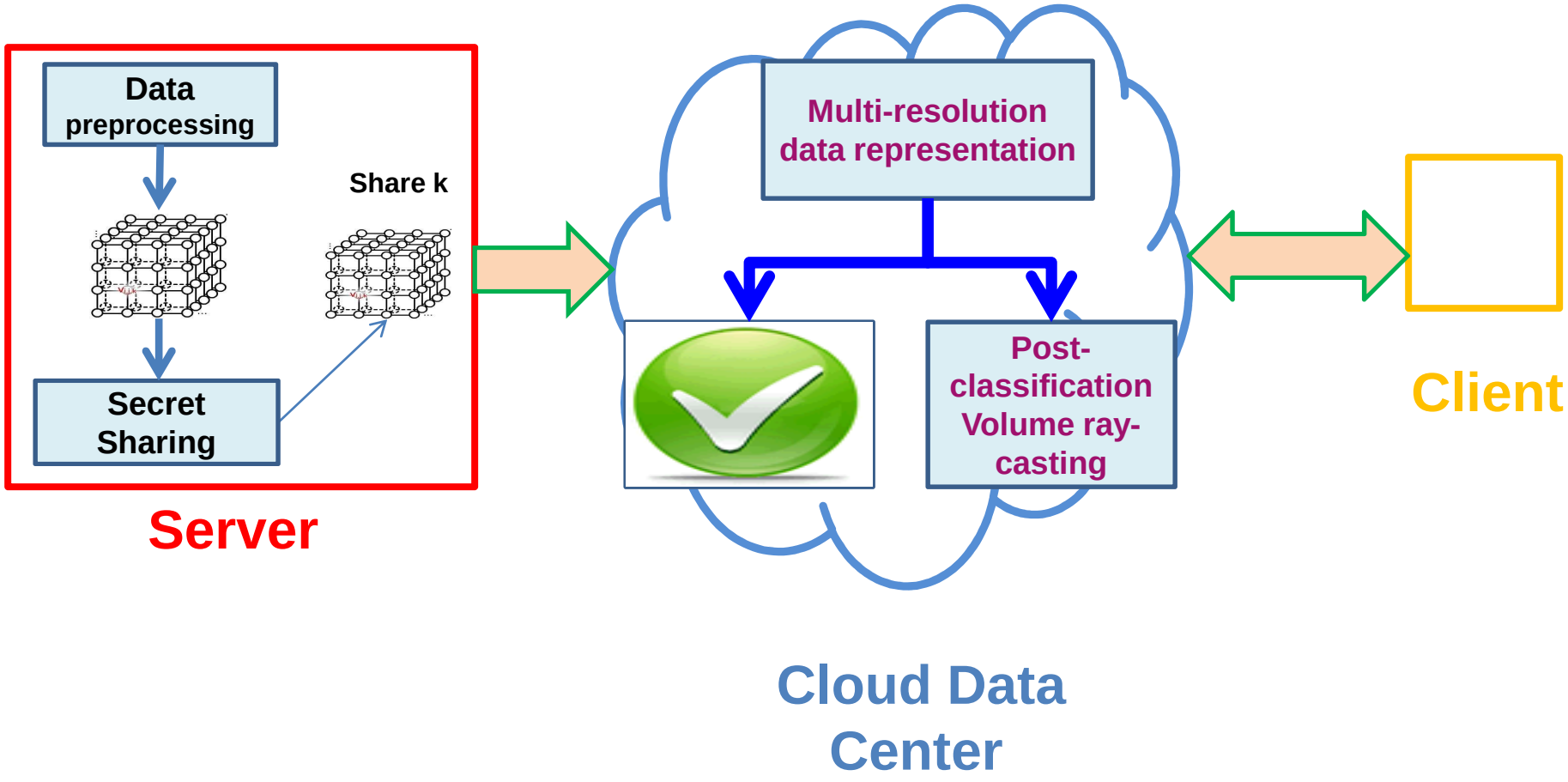
Proposed cloud-based rendering framework is information theoretically secure in a group of data centers and presents minimal computation and data overhead

http://www.writeawriting.com/wp-content/uploads/2011/12/Definition-of-a-Conclusion.jpg

The broader picture !

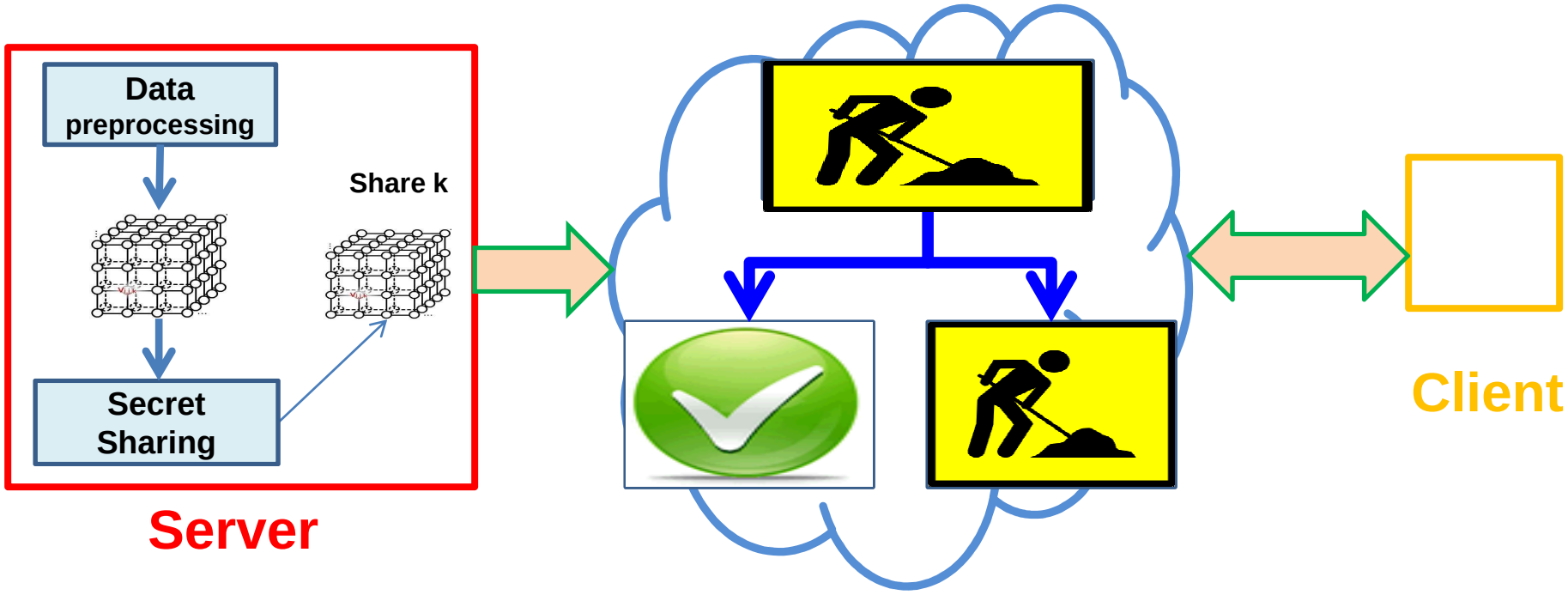


Work done!

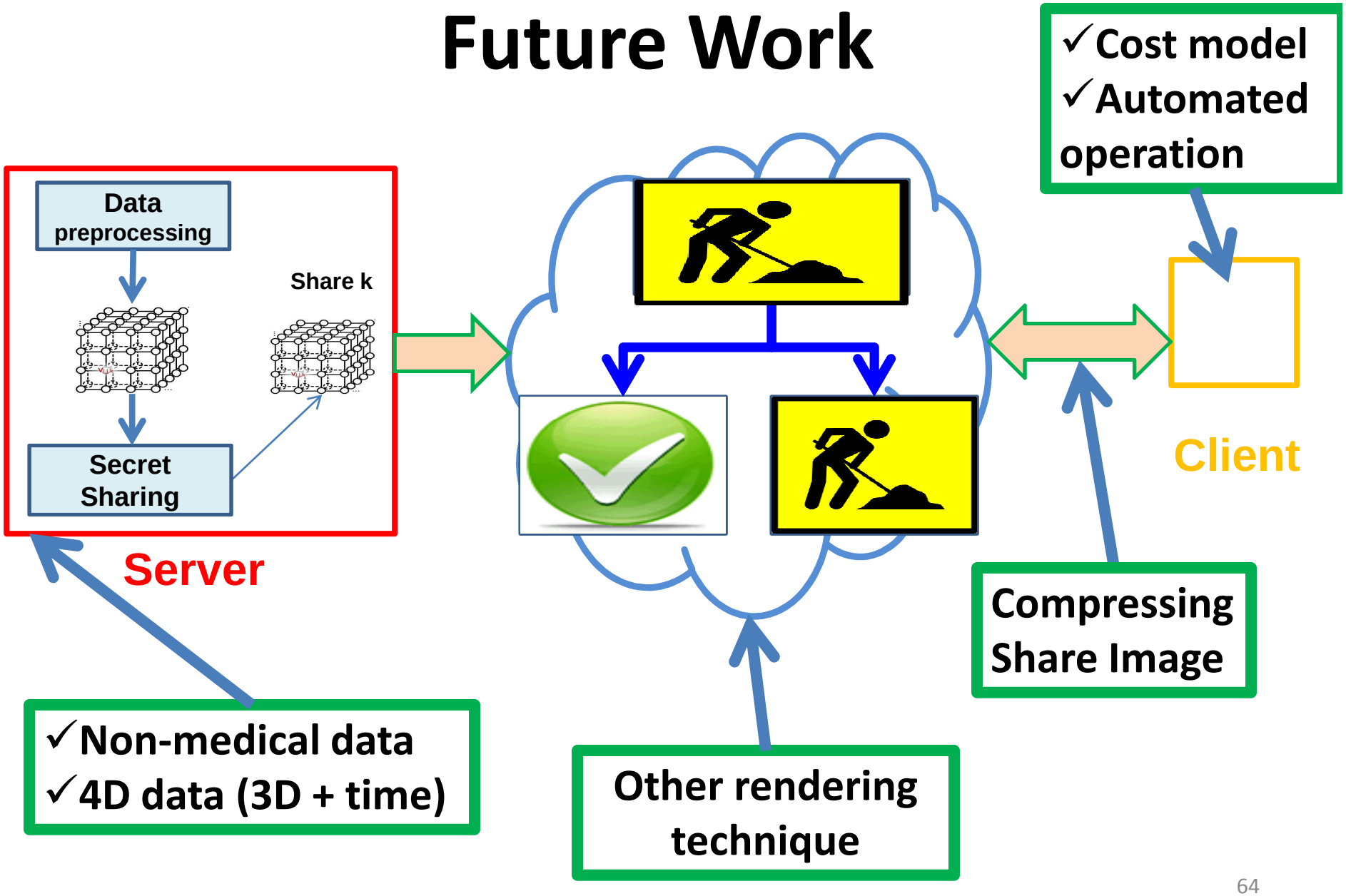


M. Mohanty, P. K. Atrey and W.-T. Ooi. Secure cloud-based medical data visualization. The ACM International Conference on Multimedia (ACMMM'12), October 29-November 2, 2012, Nara, Japan.

On-going Research



Future Work


✓Cost model
✓Automated operation
Data preprocessing
Share k
Secret Sharing
Server
Client
Compressing Share Image
✓Non-medical data
✓4D data (3D + time)
Other rendering technique