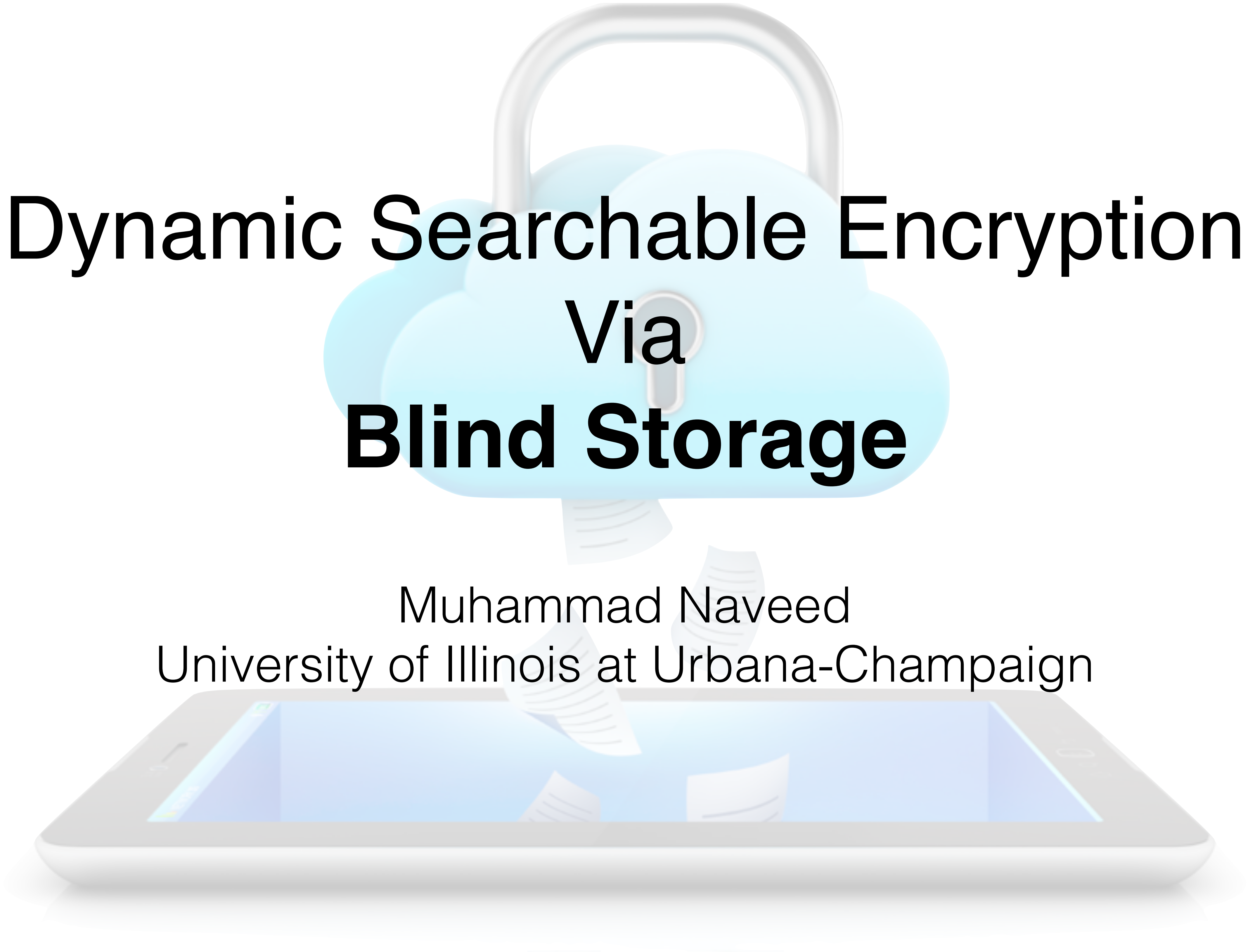


Dynamic Searchable Encryption Via **Blind Storage**

Muhammad Naveed
University of Illinois at Urbana-Champaign

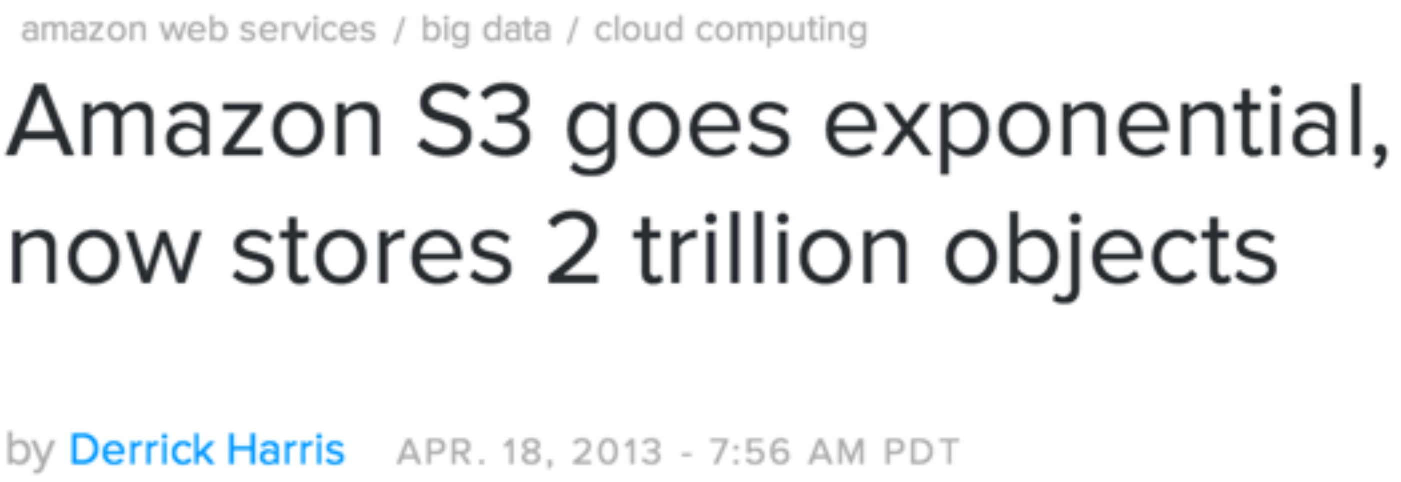
ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN
1867

Joint work with my advisors:

Manoj Prabhakaran

Carl A. Gunter

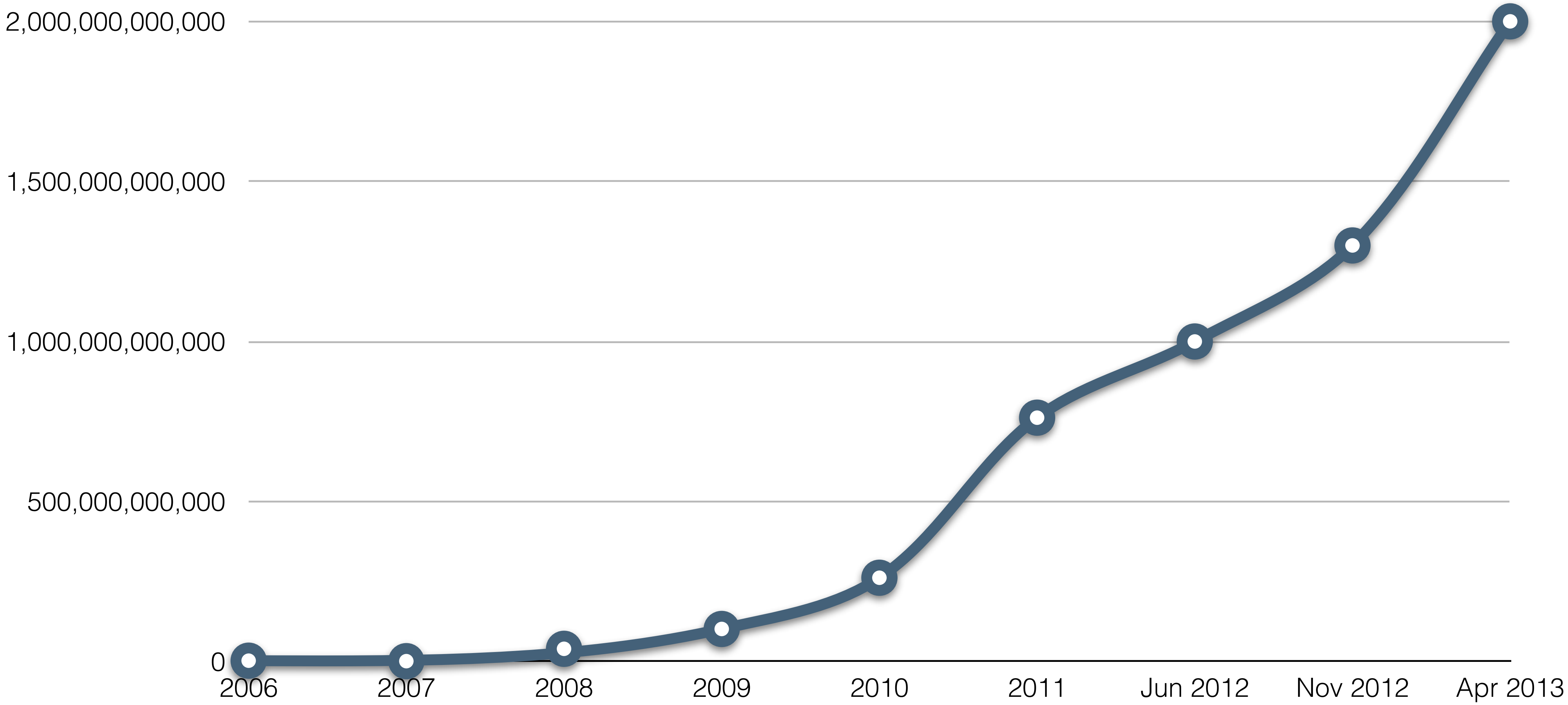
Please Interrupt!

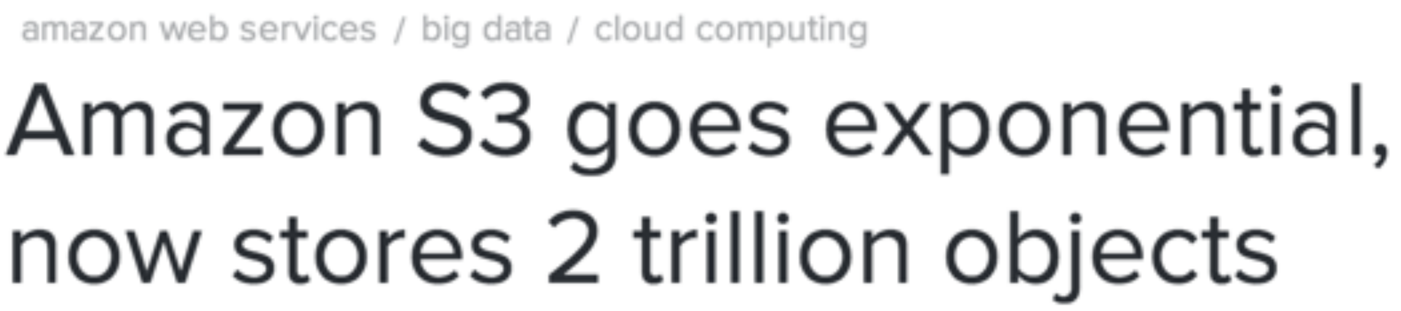


amazon web services / big data / cloud computing

Amazon S3 goes exponential, now stores 2 trillion objects

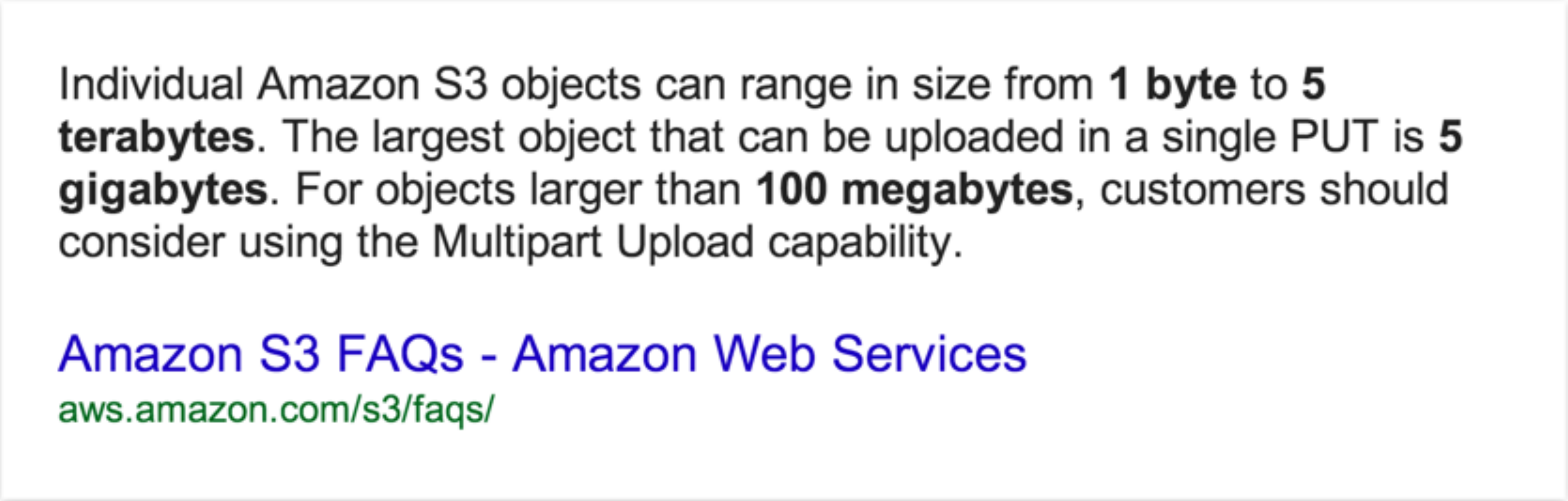
by Derrick Harris APR. 18, 2013 - 7:56 AM PDT





amazon web services / big data / cloud computing

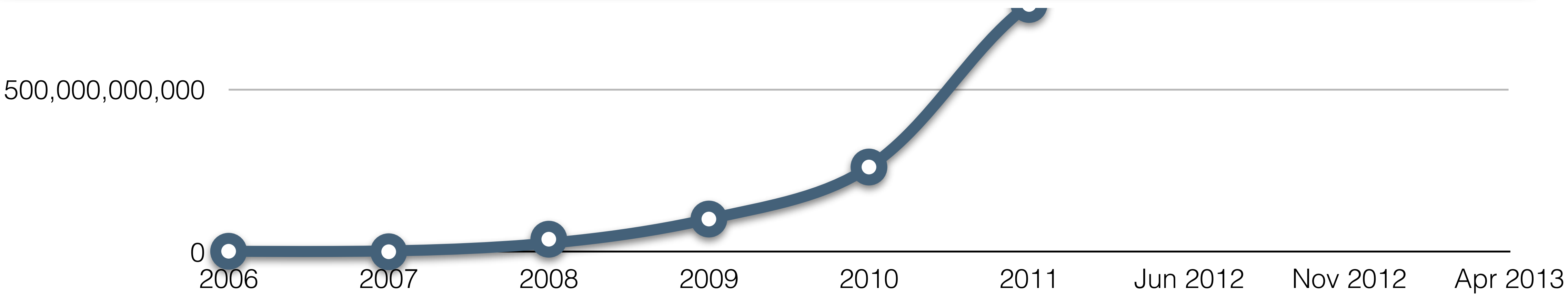
Amazon S3 goes exponential, now stores 2 trillion objects



Individual Amazon S3 objects can range in size from **1 byte** to **5 terabytes**. The largest object that can be uploaded in a single PUT is **5 gigabytes**. For objects larger than **100 megabytes**, customers should consider using the Multipart Upload capability.

Amazon S3 FAQs - Amazon Web Services

aws.amazon.com/s3/faqs/



Great Space Race!

The Great Space Race has ended! You can see the final results below!

Global Leaderboard

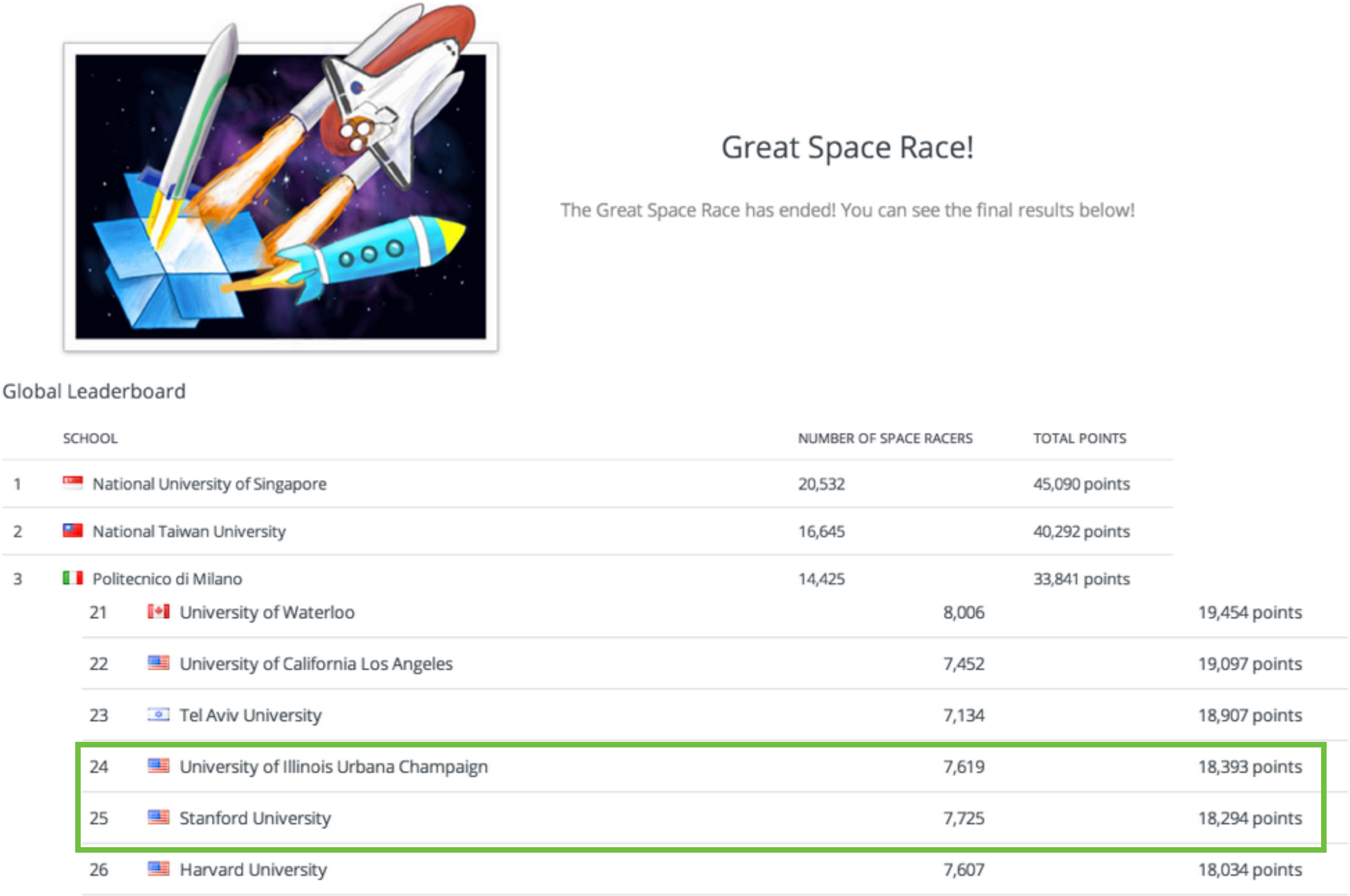
	SCHOOL	NUMBER OF SPACE RACERS	TOTAL POINTS
1	🇸🇬 National University of Singapore	20,532	45,090 points
2	🇹🇼 National Taiwan University	16,645	40,292 points
3	🇮🇹 Politecnico di Milano	14,425	33,841 points
4	🇸🇬 Nanyang Technological University	14,983	33,731 points
5	🇲🇽 Tecnológico de Monterrey	13,368	32,548 points

Great Space Race!

The Great Space Race has ended! You can see the final results below!

Global Leaderboard

	SCHOOL	NUMBER OF SPACE RACERS	TOTAL POINTS
1	🇸🇬 National University of Singapore	20,532	45,090 points
2	🇹🇼 National Taiwan University	16,645	40,292 points
3	🇮🇹 Politecnico di Milano	14,425	33,841 points
21	🇨🇦 University of Waterloo	8,006	19,454 points
22	🇺🇸 University of California Los Angeles	7,452	19,097 points
23	🇮🇱 Tel Aviv University	7,134	18,907 points
24	🇺🇸 University of Illinois Urbana Champaign	7,619	18,393 points
25	🇺🇸 Stanford University	7,725	18,294 points
26	🇺🇸 Harvard University	7,607	18,034 points

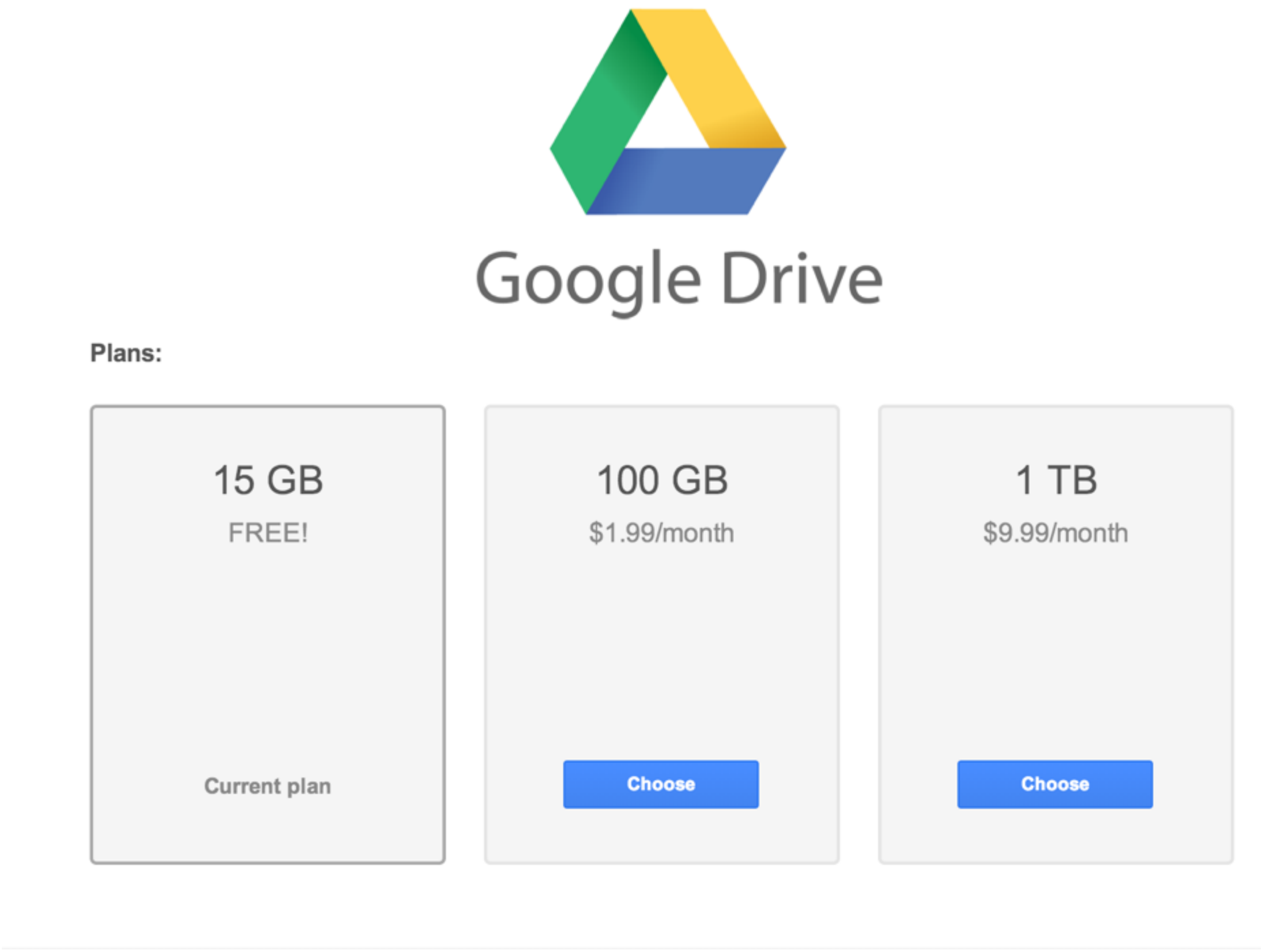


Great Space Race!

The Great Space Race has ended! You can see the final results below!

Global Leaderboard

	SCHOOL	NUMBER OF SPACE RACERS	TOTAL POINTS
1	National University of Singapore	20,532	45,090 points
2	National Taiwan University	16,645	40,292 points
3	Politecnico di Milano	14,425	33,841 points
21	University of Waterloo	8,006	19,454 points
22	University of California Los Angeles	7,452	19,097 points
23	Tel Aviv University	7,134	18,907 points
24	University of Illinois Urbana Champaign	7,619	18,393 points
25	Stanford University	7,725	18,294 points
26	Harvard University	7,607	18,034 points



Google Drive

Plans:

15 GB

FREE!

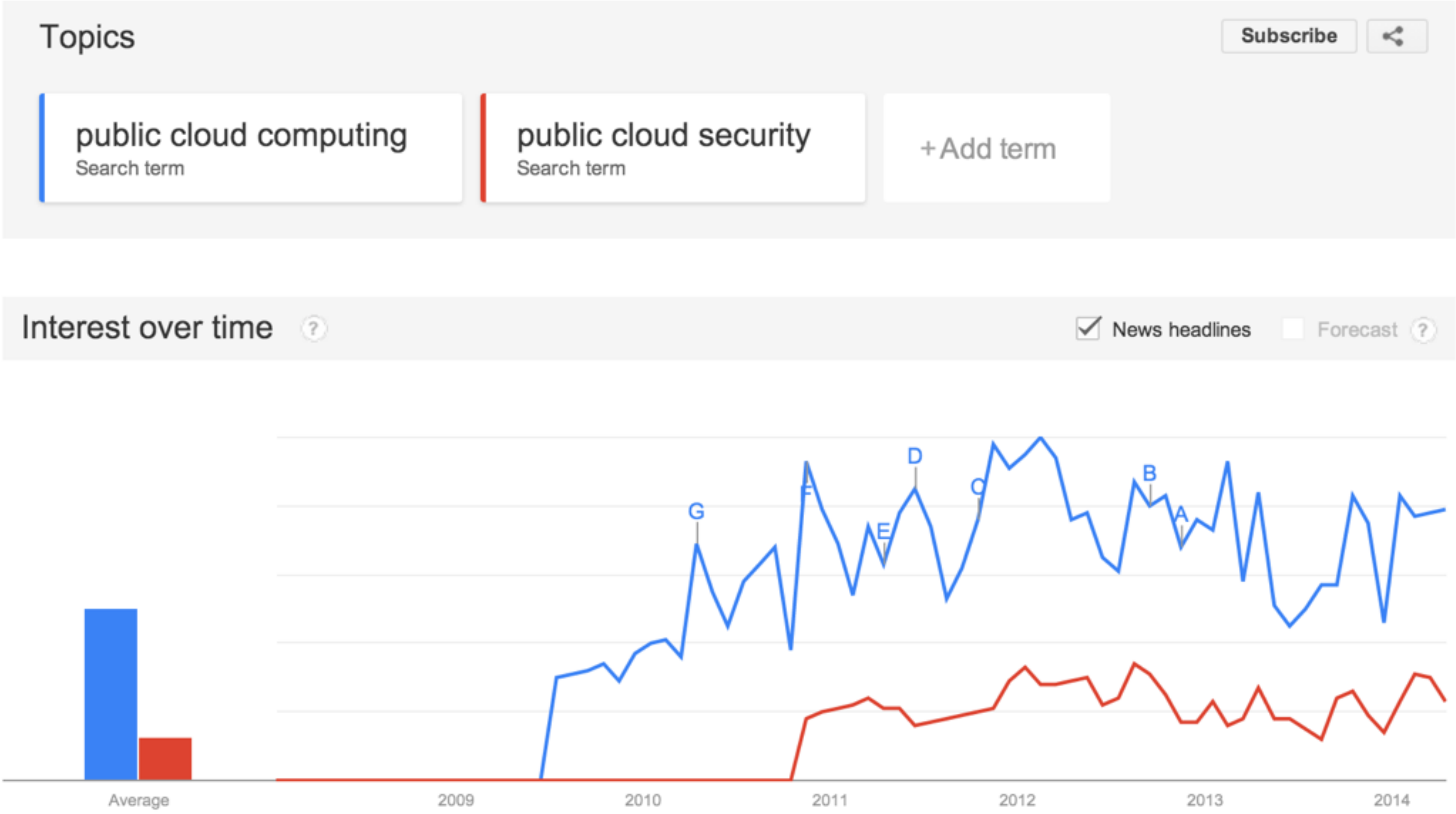
Current plan

100 GB

$1.99/month

1 TB

$9.99/month



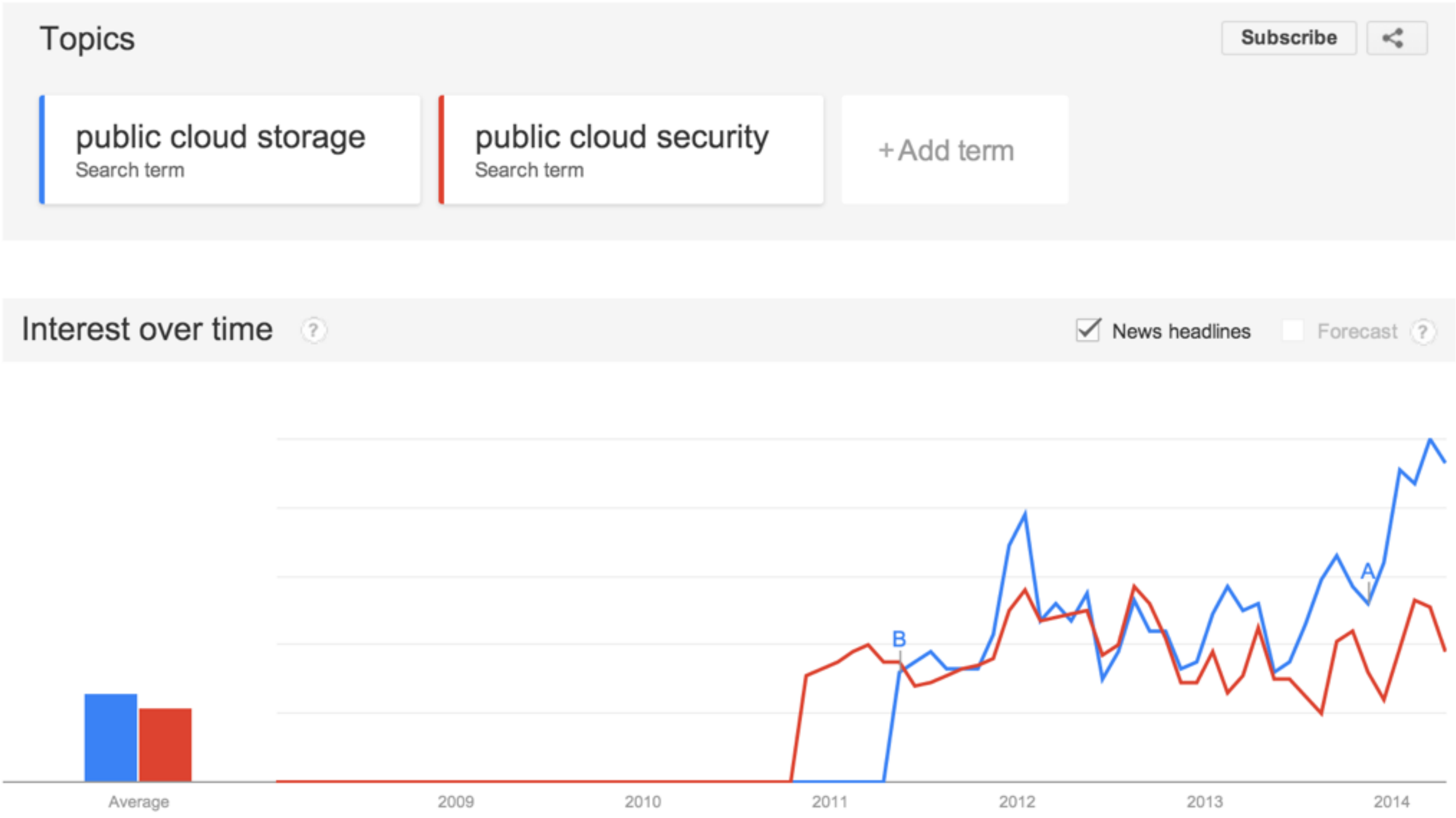
Topics

public cloud computing
Search term

public cloud security
Search term

Interest over time

☑ News headlines □ Forecast



Topics

Subscribe

public cloud storage
Search term

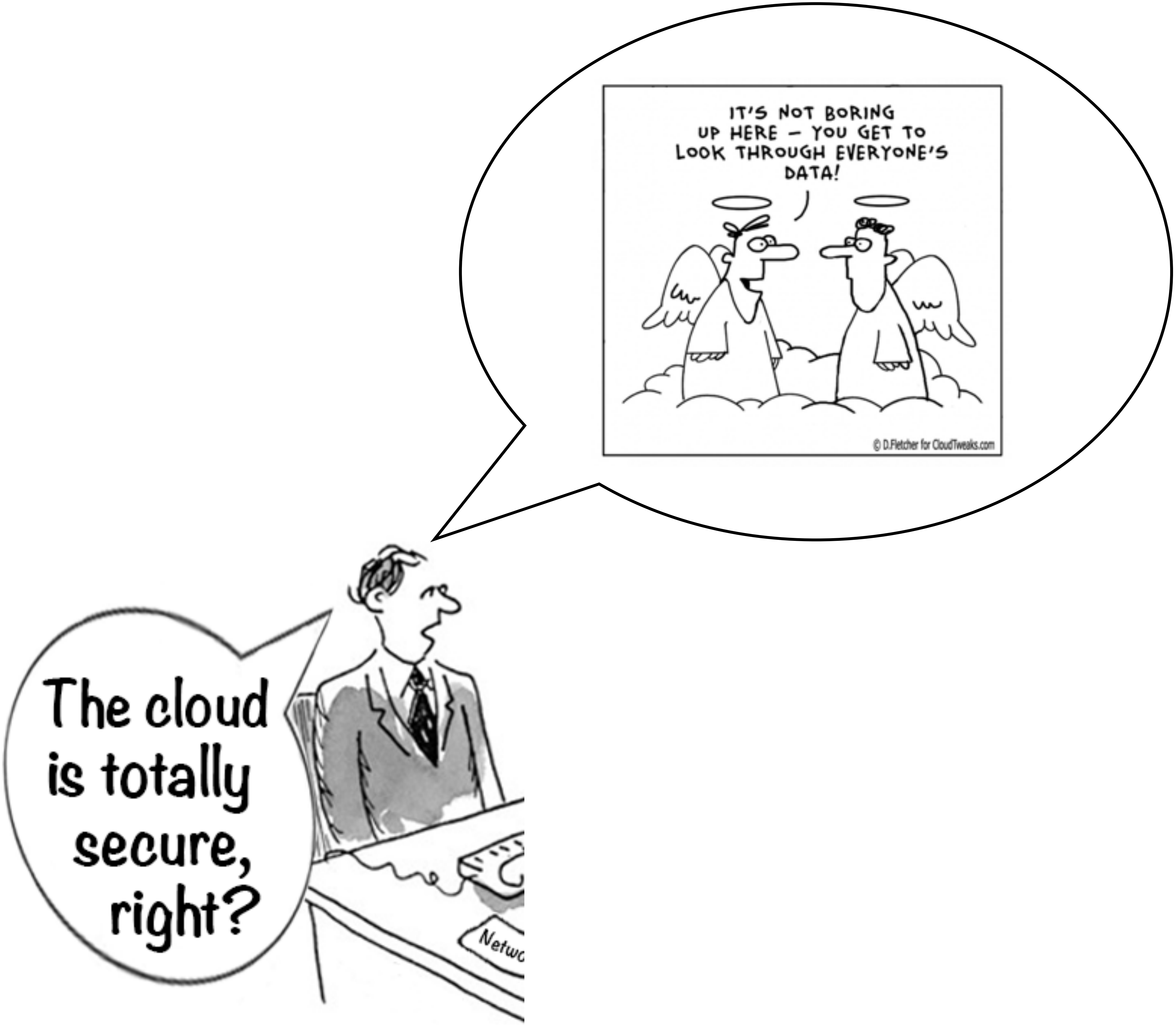
public cloud security
Search term

+ Add term

Interest over time

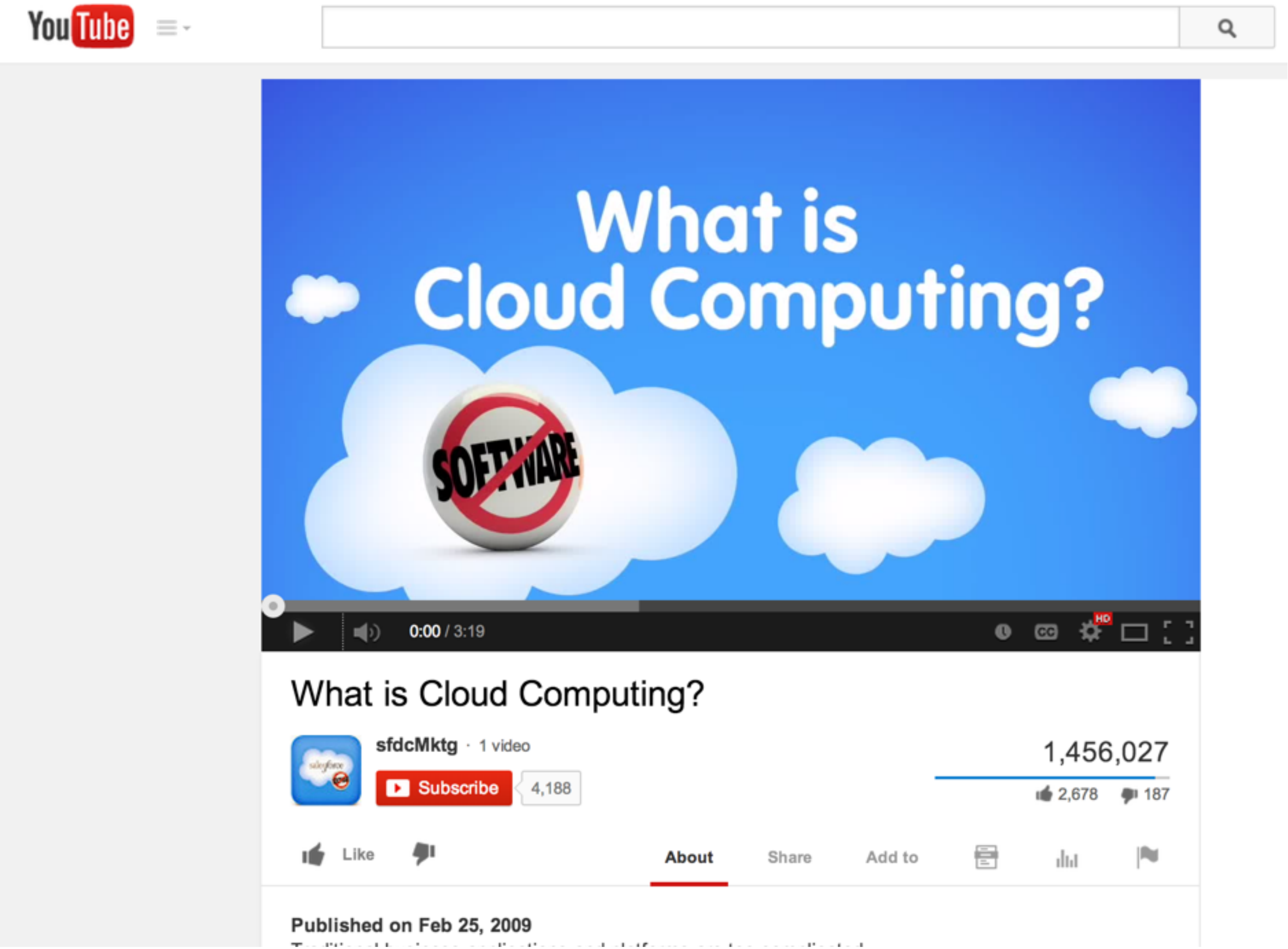
☑ News headlines □ Forecast

Google trends


IT'S NOT BORING UP HERE – YOU GET TO LOOK THROUGH EVERYONE'S DATA!
The cloud is totally secure, right?
Netw

© D.Fletcher for CloudTweaks.com

What do people think about cloud storage?



What is Cloud Computing?

sfdcMktg · 1 video

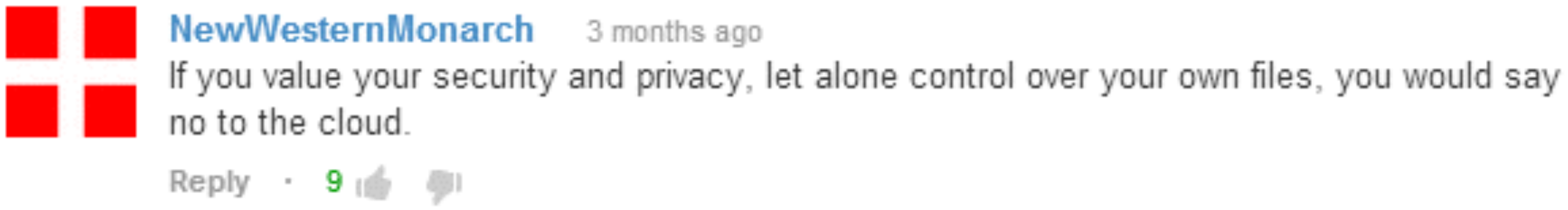
Subscribe 4,188

1,456,027

2,678 187

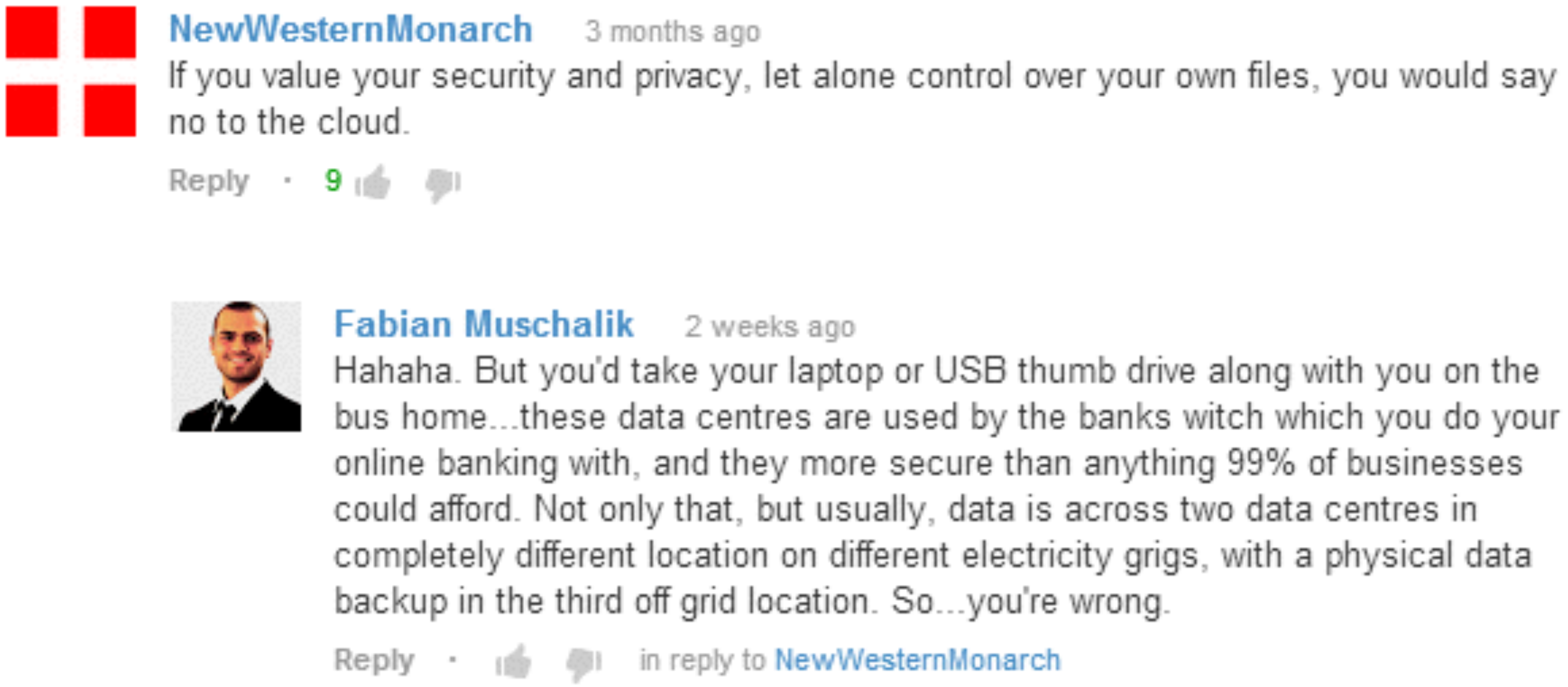
Published on Feb 25, 2009

Traditional business applications and platforms are too complicated



NewWesternMonarch 3 months ago

If you value your security and privacy, let alone control over your own files, you would say no to the cloud.



NewWesternMonarch 3 months ago

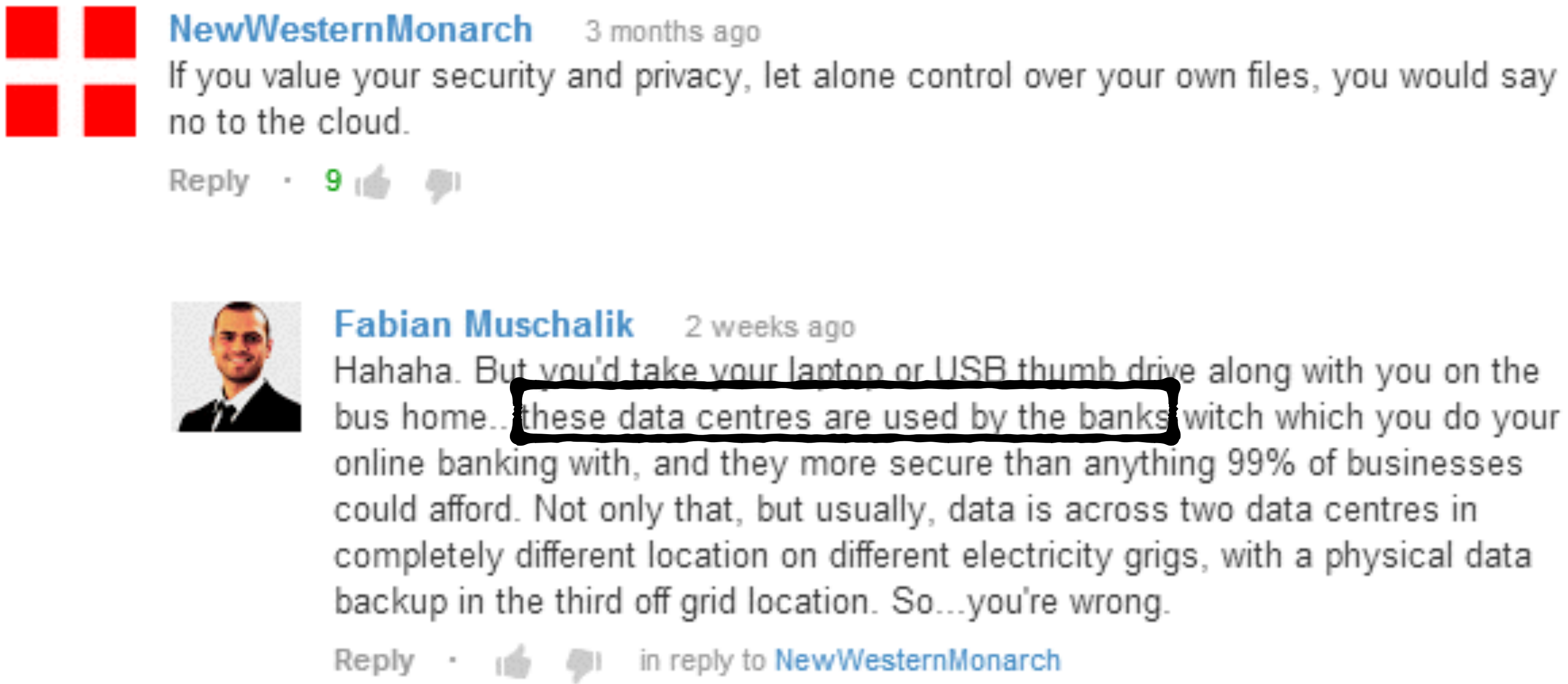
If you value your security and privacy, let alone control over your own files, you would say no to the cloud.

Reply · 9 👍 👎

Fabian Muschalik 2 weeks ago

Hahaha. But you'd take your laptop or USB thumb drive along with you on the bus home...these data centres are used by the banks witch which you do your online banking with, and they more secure than anything 99% of businesses could afford. Not only that, but usually, data is across two data centres in completely different location on different electricity grigs, with a physical data backup in the third off grid location. So...you're wrong.

Reply · 👍 👎 in reply to NewWesternMonarch

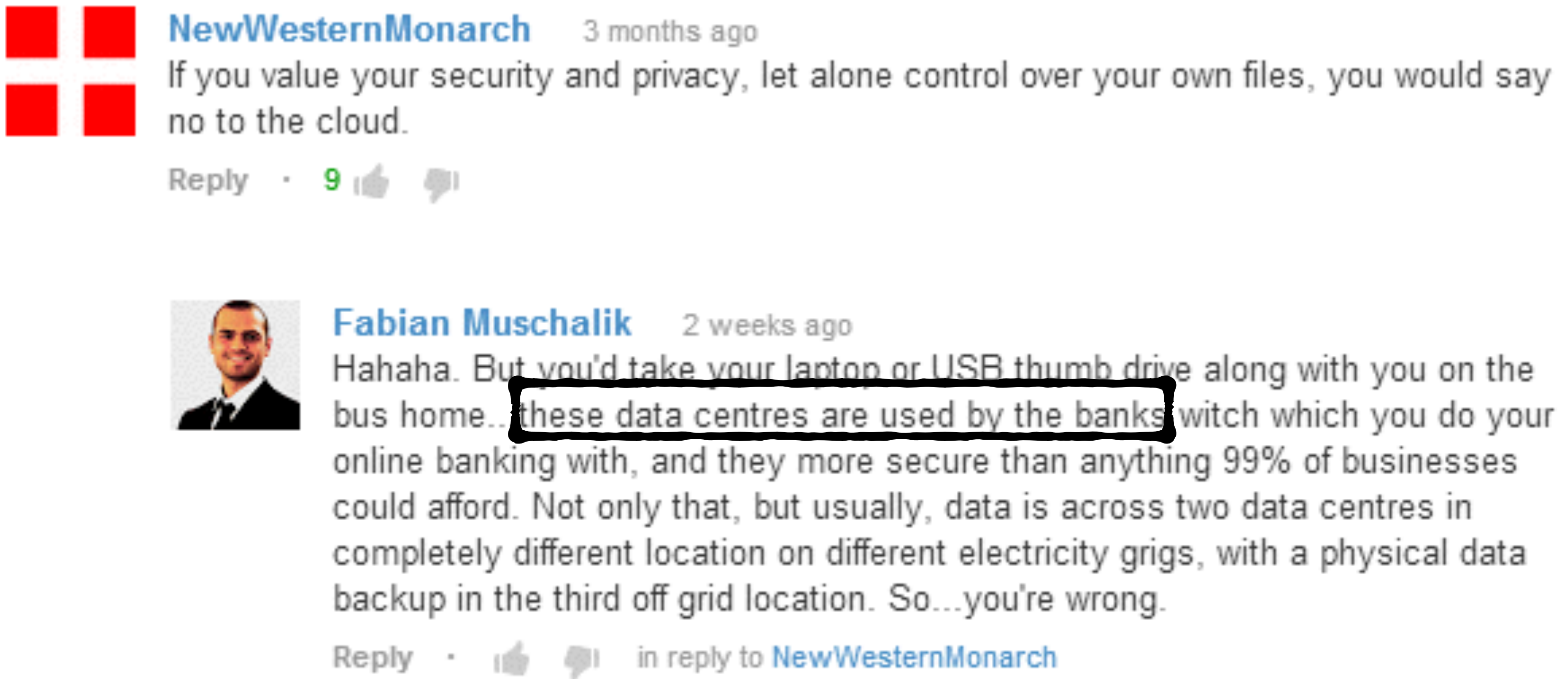


NewWesternMonarch 3 months ago

If you value your security and privacy, let alone control over your own files, you would say no to the cloud.

Fabian Muschalik 2 weeks ago

Hahaha. But you'd take your laptop or USB thumb drive along with you on the bus home...these data centres are used by the banks witch which you do your online banking with, and they more secure than anything 99% of businesses could afford. Not only that, but usually, data is across two data centres in completely different location on different electricity grigs, with a physical data backup in the third off grid location. So...you're wrong.



NewWesternMonarch 3 months ago

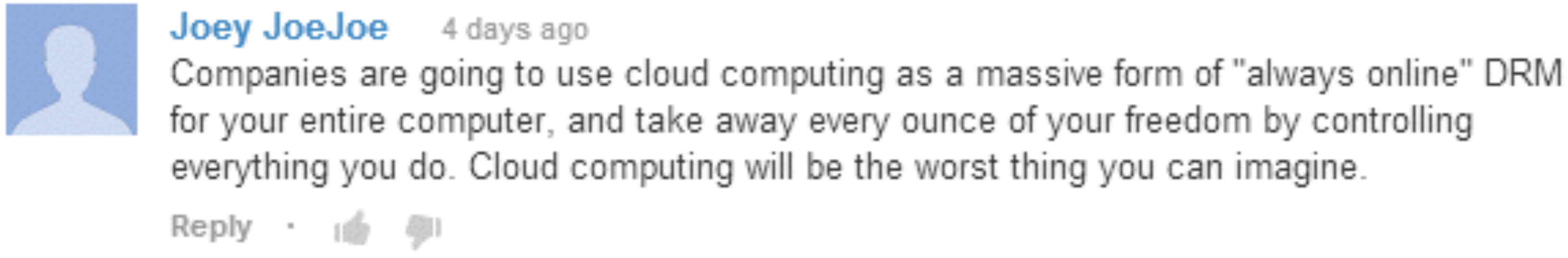
If you value your security and privacy, let alone control over your own files, you would say no to the cloud.

Reply · 9 👍 👎

Fabian Muschalik 2 weeks ago

Hahaha. But you'd take your laptop or USB thumb drive along with you on the bus home...these data centres are used by the banks witch which you do your online banking with, and they more secure than anything 99% of businesses could afford. Not only that, but usually, data is across two data centres in completely different location on different electricity grigs, with a physical data backup in the third off grid location. So...you're wrong.

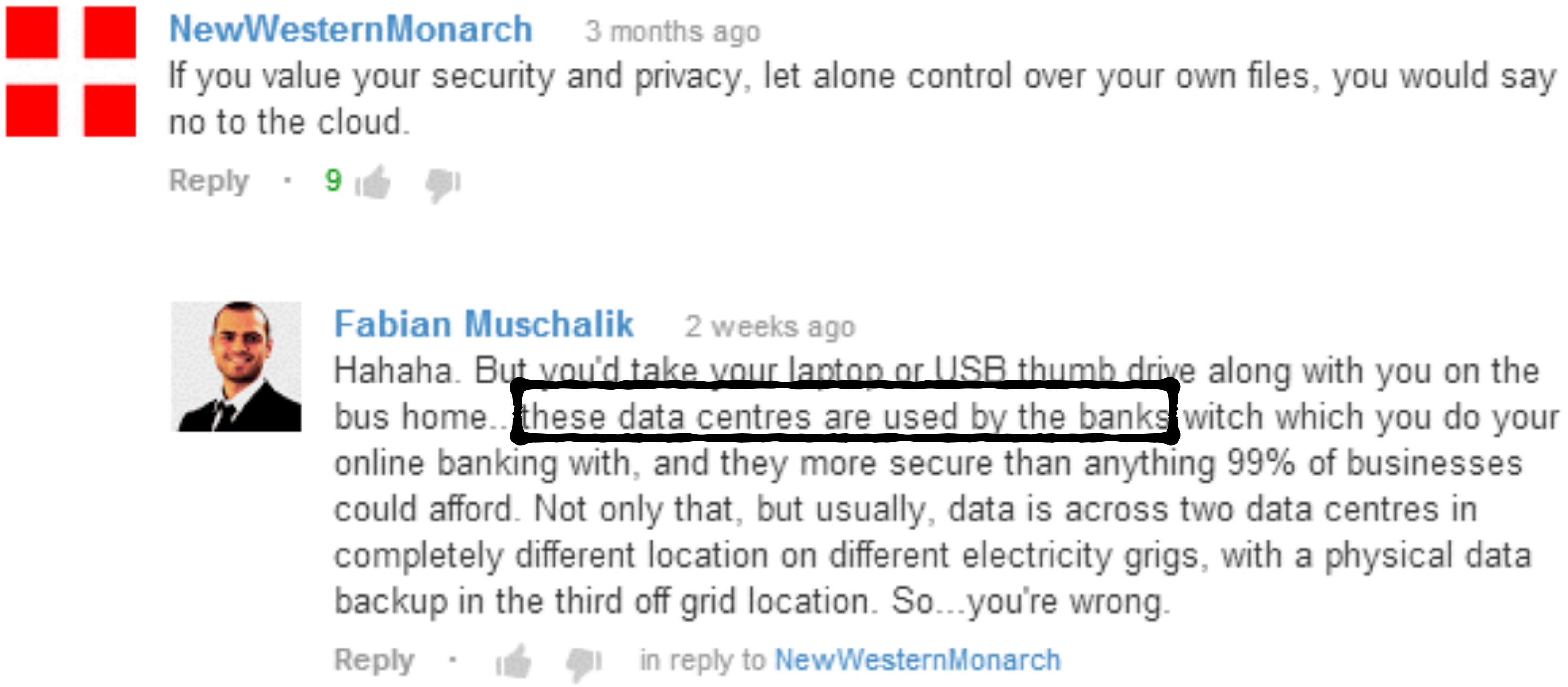
Reply · 👍 👎 in reply to NewWesternMonarch



Joey JoeJoe 4 days ago

Companies are going to use cloud computing as a massive form of "always online" DRM for your entire computer, and take away every ounce of your freedom by controlling everything you do. Cloud computing will be the worst thing you can imagine.

Reply · 👍 👎

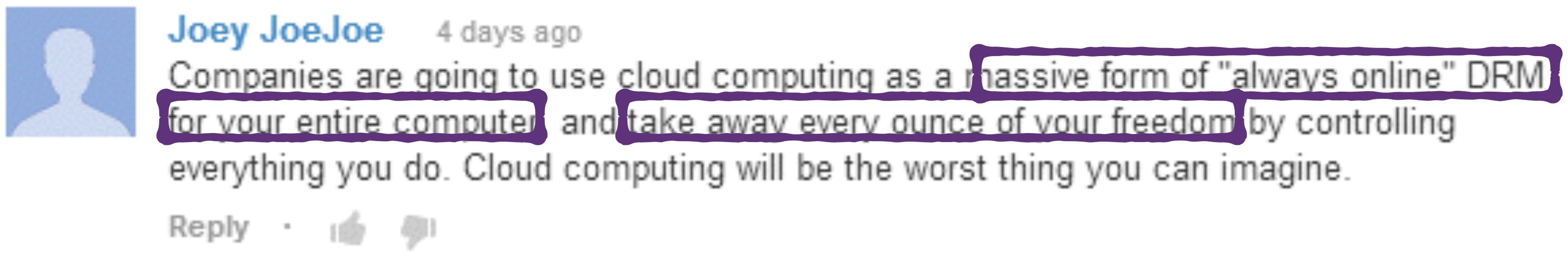


NewWesternMonarch 3 months ago

If you value your security and privacy, let alone control over your own files, you would say no to the cloud.

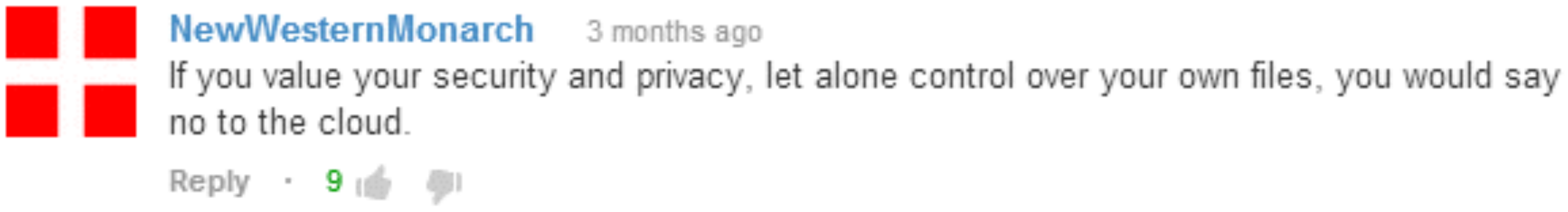
Fabian Muschalik 2 weeks ago

Hahaha. But you'd take your laptop or USB thumb drive along with you on the bus home.. these data centres are used by the banks witch which you do your online banking with, and they more secure than anything 99% of businesses could afford. Not only that, but usually, data is across two data centres in completely different location on different electricity grigs, with a physical data backup in the third off grid location. So...you're wrong.



Joey JoeJoe 4 days ago

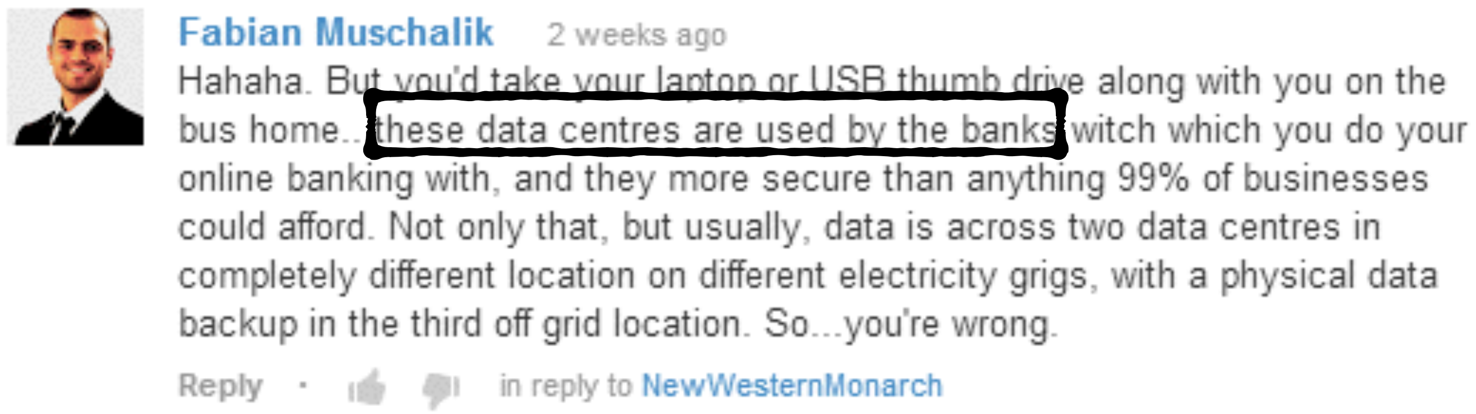
Companies are going to use cloud computing as a massive form of "always online" DRM for your entire computer and take away every ounce of your freedom by controlling everything you do. Cloud computing will be the worst thing you can imagine.



NewWesternMonarch 3 months ago

If you value your security and privacy, let alone control over your own files, you would say no to the cloud.

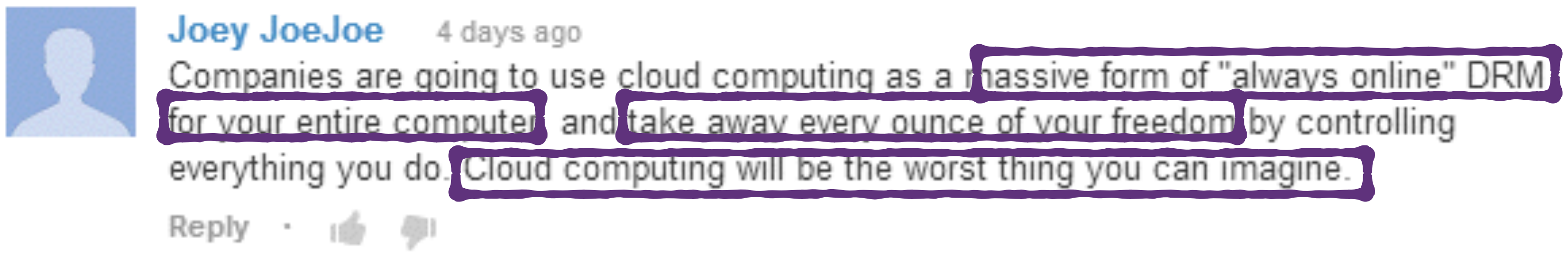
Reply · 9



Fabian Muschalik 2 weeks ago

Hahaha. But you'd take your laptop or USB thumb drive along with you on the bus home.. these data centres are used by the banks witch which you do your online banking with, and they more secure than anything 99% of businesses could afford. Not only that, but usually, data is across two data centres in completely different location on different electricity grigs, with a physical data backup in the third off grid location. So...you're wrong.

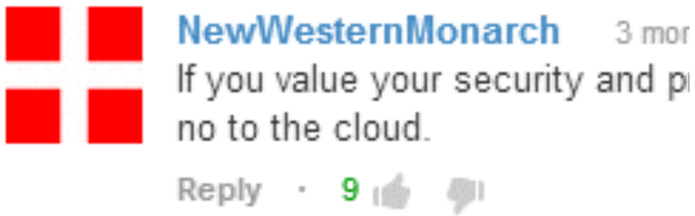
Reply · in reply to NewWesternMonarch



Joey JoeJoe 4 days ago

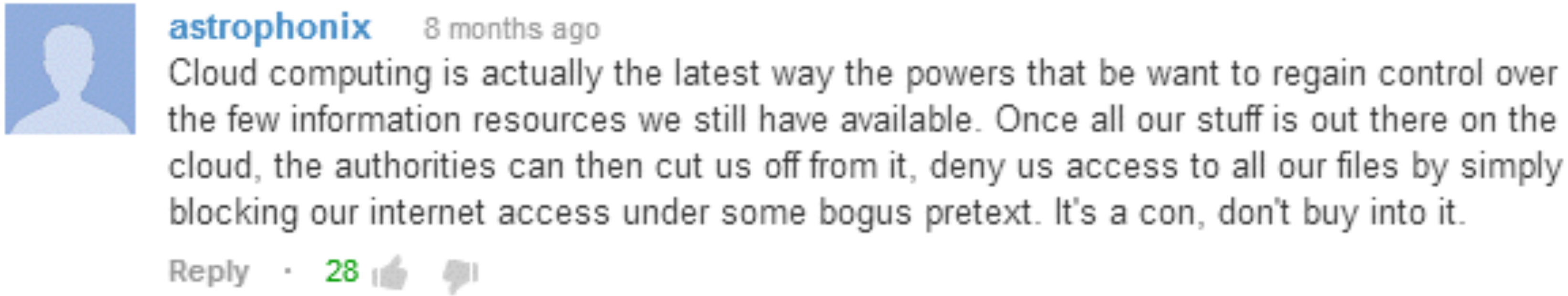
Companies are going to use cloud computing as a massive form of "always online" DRM for your entire computer and take away every ounce of your freedom by controlling everything you do. Cloud computing will be the worst thing you can imagine.

Reply ·



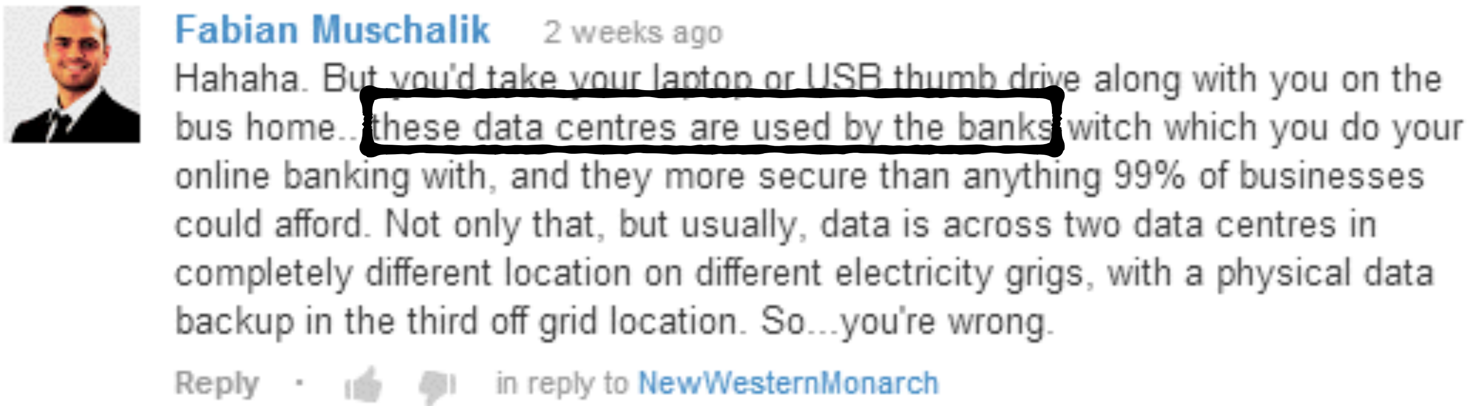
NewWesternMonarch 3 mor

If you value your security and p
no to the cloud.



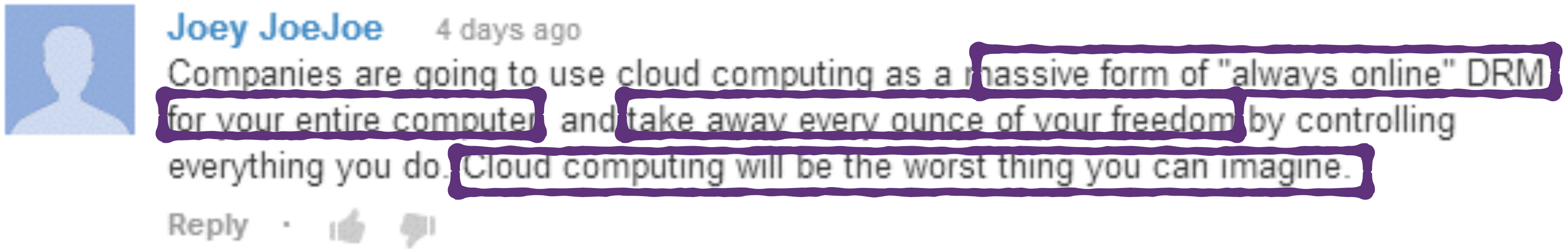
astrophonix 8 months ago

Cloud computing is actually the latest way the powers that be want to regain control over the few information resources we still have available. Once all our stuff is out there on the cloud, the authorities can then cut us off from it, deny us access to all our files by simply blocking our internet access under some bogus pretext. It's a con, don't buy into it.



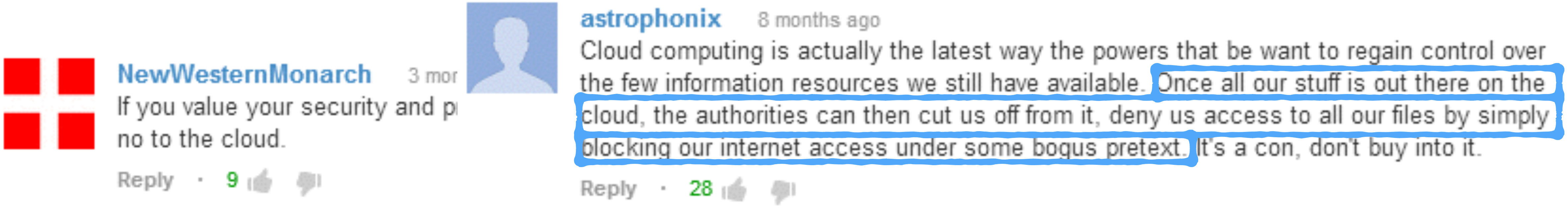
Fabian Muschalik 2 weeks ago

Hahaha. But you'd take your laptop or USB thumb drive along with you on the bus home.. these data centres are used by the banks witch which you do your online banking with, and they more secure than anything 99% of businesses could afford. Not only that, but usually, data is across two data centres in completely different location on different electricity grigs, with a physical data backup in the third off grid location. So...you're wrong.



Joey JoeJoe 4 days ago

Companies are going to use cloud computing as a massive form of "always online" DRM for your entire computer and take away every ounce of your freedom by controlling everything you do. Cloud computing will be the worst thing you can imagine.



NewWesternMonarch 3 mor

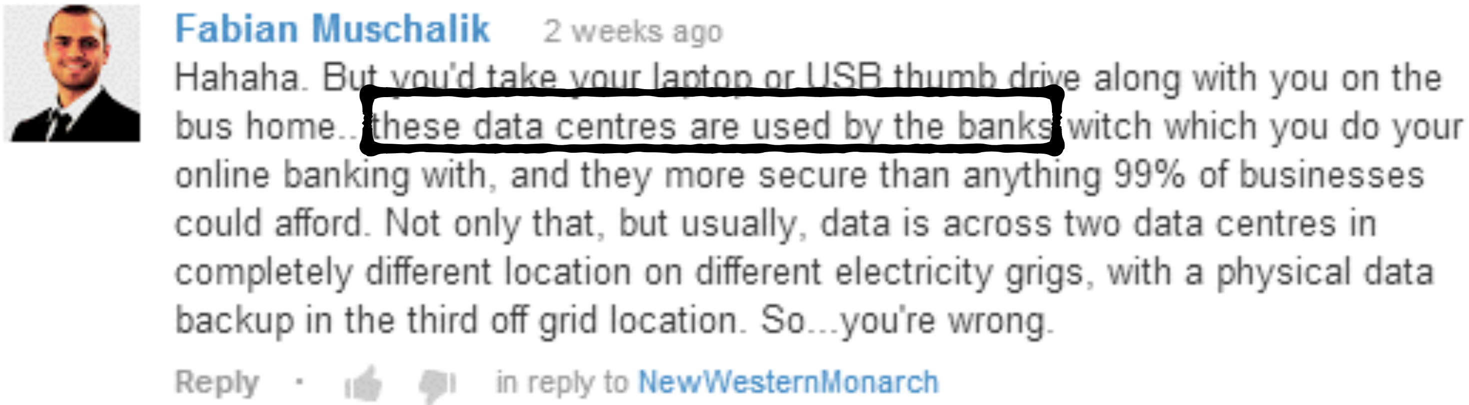
If you value your security and p
no to the cloud.

Reply · 9

astrophonix 8 months ago

Cloud computing is actually the latest way the powers that be want to regain control over the few information resources we still have available. Once all our stuff is out there on the cloud, the authorities can then cut us off from it, deny us access to all our files by simply blocking our internet access under some bogus pretext. It's a con, don't buy into it.

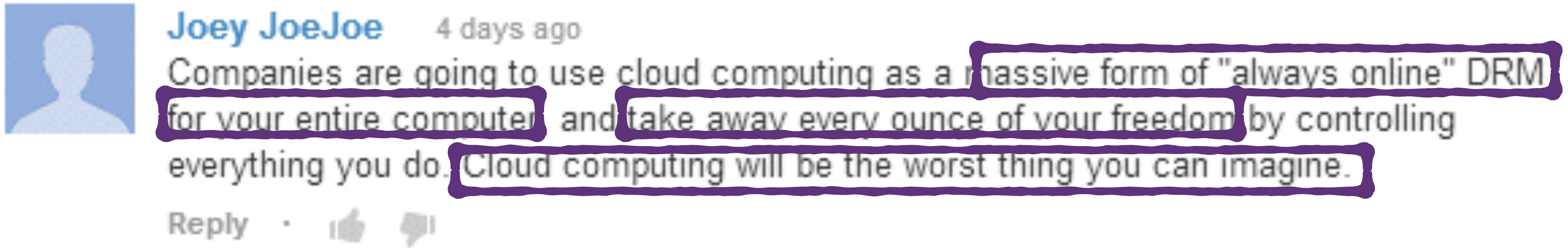
Reply · 28



Fabian Muschalik 2 weeks ago

Hahaha. But you'd take your laptop or USB thumb drive along with you on the bus home.. these data centres are used by the banks witch which you do your online banking with, and they more secure than anything 99% of businesses could afford. Not only that, but usually, data is across two data centres in completely different location on different electricity grigs, with a physical data backup in the third off grid location. So...you're wrong.

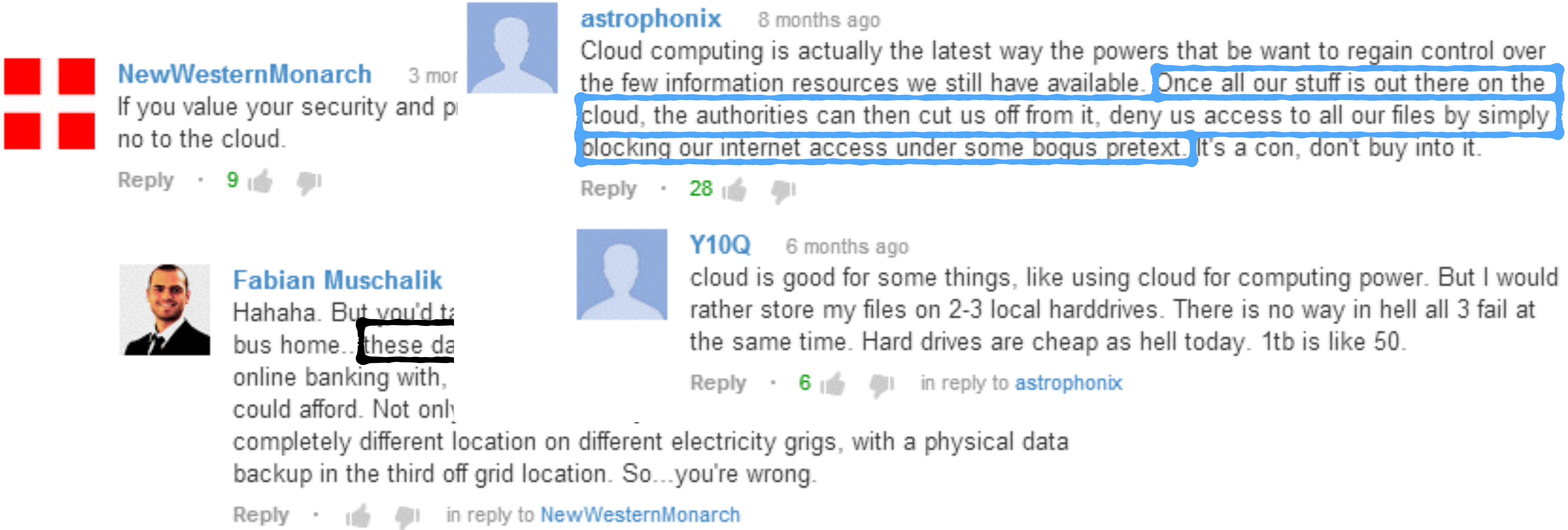
Reply · in reply to NewWesternMonarch



Joey JoeJoe 4 days ago

Companies are going to use cloud computing as a massive form of "always online" DRM for your entire computer and take away every ounce of your freedom by controlling everything you do. Cloud computing will be the worst thing you can imagine.

Reply ·



NewWesternMonarch 3 mor

If you value your security and p

no to the cloud.

Reply · 9 👍 👎

astrophonix 8 months ago

Cloud computing is actually the latest way the powers that be want to regain control over the few information resources we still have available. Once all our stuff is out there on the cloud, the authorities can then cut us off from it, deny us access to all our files by simply blocking our internet access under some bogus pretext. It's a con, don't buy into it.

Reply · 28 👍 👎

Fabian Muschalik

Hahaha. But you'd ta

bus home.. these da

online banking with,

could afford. Not onl

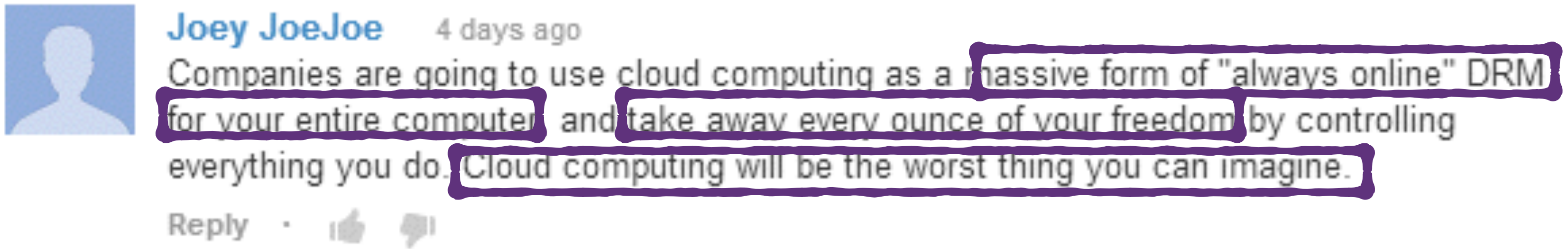
completely different location on different electricity grigs, with a physical data backup in the third off grid location. So...you're wrong.

Reply · 👍 👎 in reply to NewWesternMonarch

Y10Q 6 months ago

cloud is good for some things, like using cloud for computing power. But I would rather store my files on 2-3 local harddrives. There is no way in hell all 3 fail at the same time. Hard drives are cheap as hell today. 1tb is like 50.

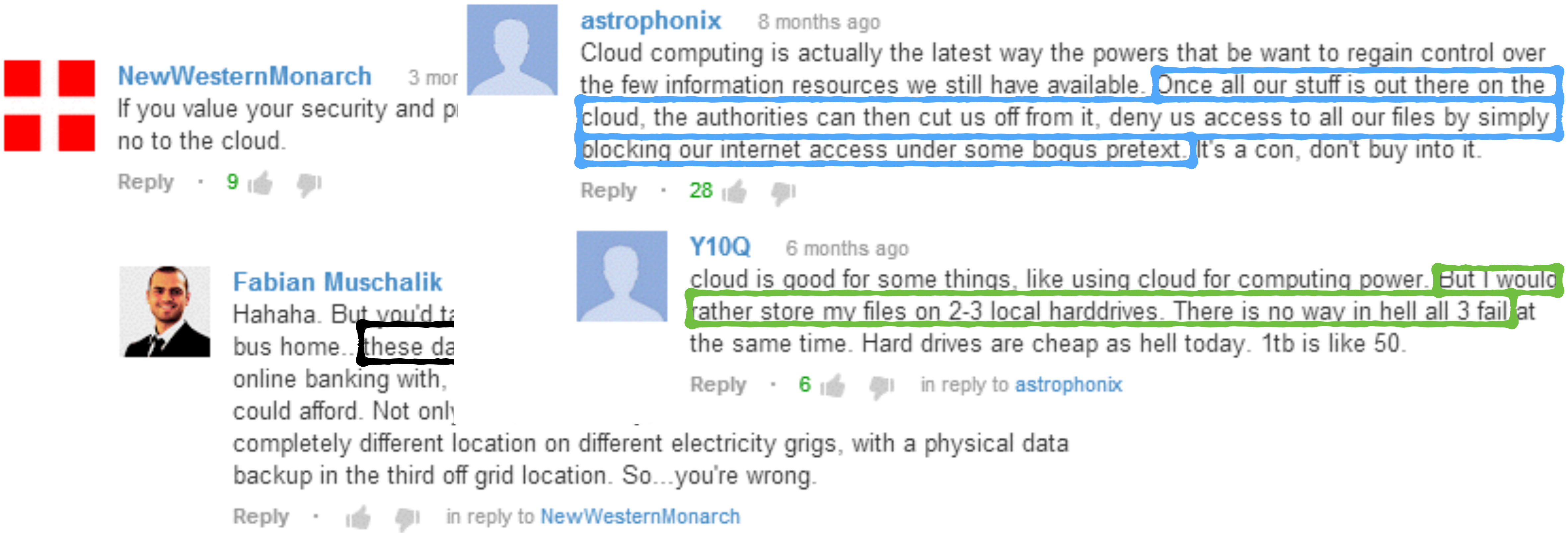
Reply · 6 👍 👎 in reply to astrophonix



Joey JoeJoe 4 days ago

Companies are going to use cloud computing as a massive form of "always online" DRM for your entire computer and take away every ounce of your freedom by controlling everything you do. Cloud computing will be the worst thing you can imagine.

Reply · 👍 👎

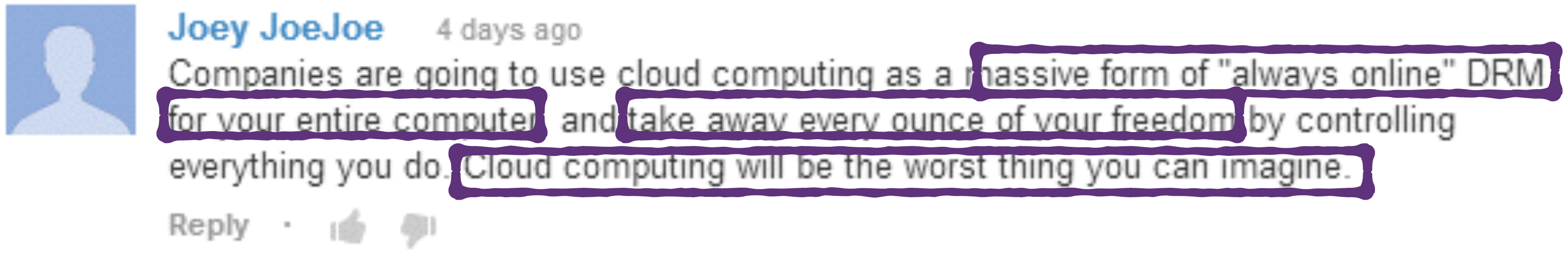


NewWesternMonarch 3 mor
If you value your security and p
no to the cloud.
Reply · 9

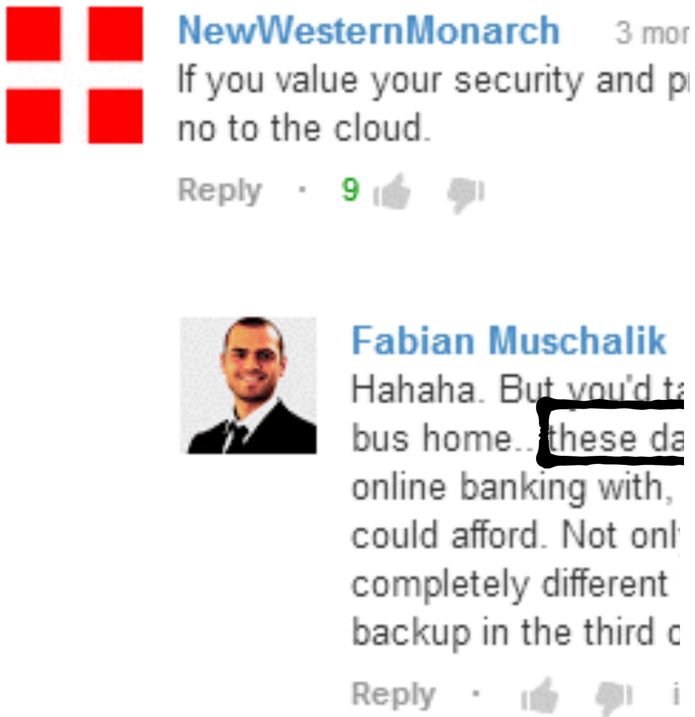
astrophonix 8 months ago
Cloud computing is actually the latest way the powers that be want to regain control over the few information resources we still have available. Once all our stuff is out there on the cloud, the authorities can then cut us off from it, deny us access to all our files by simply blocking our internet access under some bogus pretext. It's a con, don't buy into it.
Reply · 28

Y10Q 6 months ago
cloud is good for some things, like using cloud for computing power. But I would rather store my files on 2-3 local harddrives. There is no way in hell all 3 fail at the same time. Hard drives are cheap as hell today. 1tb is like 50.
Reply · 6 in reply to astrophonix

Fabian Muschalik
Hahaha. But you'd t
bus home...these da
online banking with,
could afford. Not onl
completely different location on different electricity grigs, with a physical data backup in the third off grid location. So...you're wrong.
Reply · in reply to NewWesternMonarch



Joey JoeJoe 4 days ago
Companies are going to use cloud computing as a massive form of "always online" DRM for your entire computer and take away every ounce of your freedom by controlling everything you do. Cloud computing will be the worst thing you can imagine.
Reply ·



NewWesternMonarch 3 mor

If you value your security and p

no to the cloud.

Reply · 9

Fabian Muschalik

Hahaha. But you'd ta

bus home.. these da

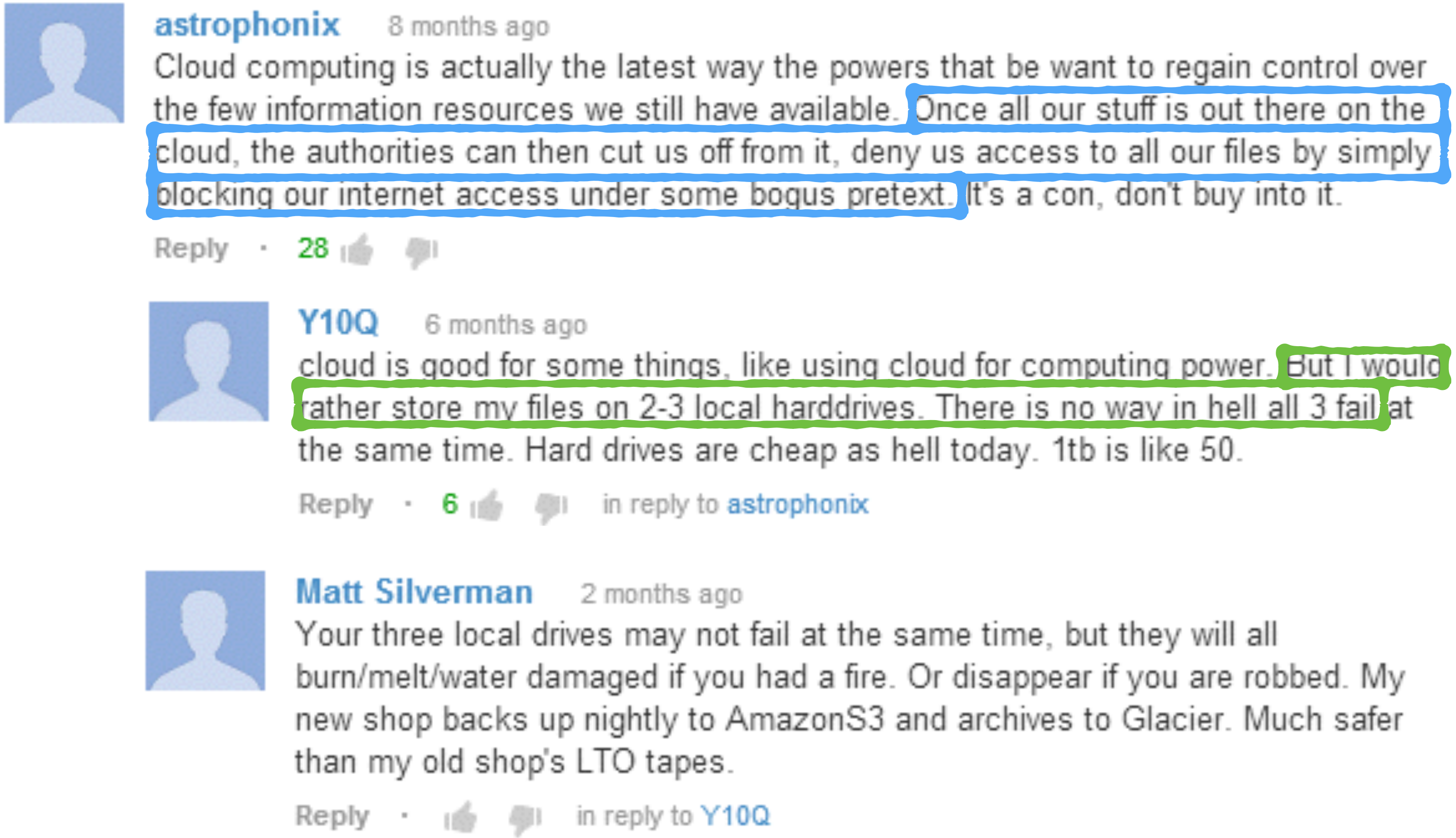
online banking with,

could afford. Not onl

completely different

backup in the third c

Reply · i



astrophonix 8 months ago

Cloud computing is actually the latest way the powers that be want to regain control over the few information resources we still have available. Once all our stuff is out there on the cloud, the authorities can then cut us off from it, deny us access to all our files by simply blocking our internet access under some bogus pretext. It's a con, don't buy into it.

Reply · 28

Y10Q 6 months ago

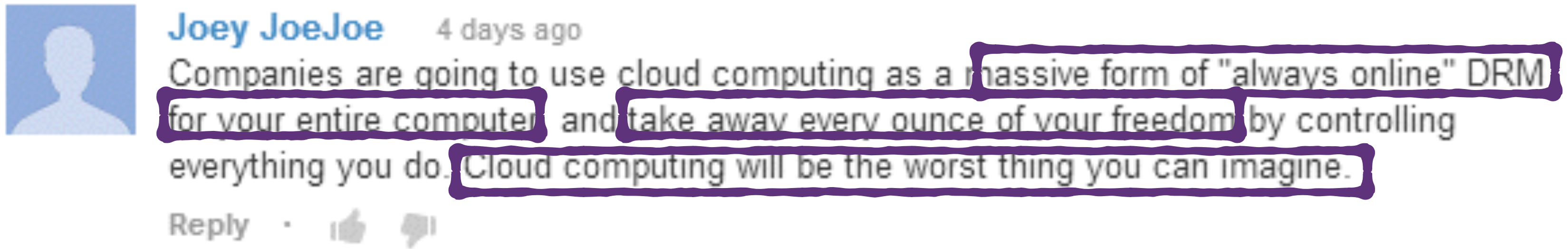
cloud is good for some things, like using cloud for computing power. But I would rather store my files on 2-3 local harddrives. There is no way in hell all 3 fail at the same time. Hard drives are cheap as hell today. 1tb is like 50.

Reply · 6 in reply to astrophonix

Matt Silverman 2 months ago

Your three local drives may not fail at the same time, but they will all burn/melt/water damaged if you had a fire. Or disappear if you are robbed. My new shop backs up nightly to AmazonS3 and archives to Glacier. Much safer than my old shop's LTO tapes.

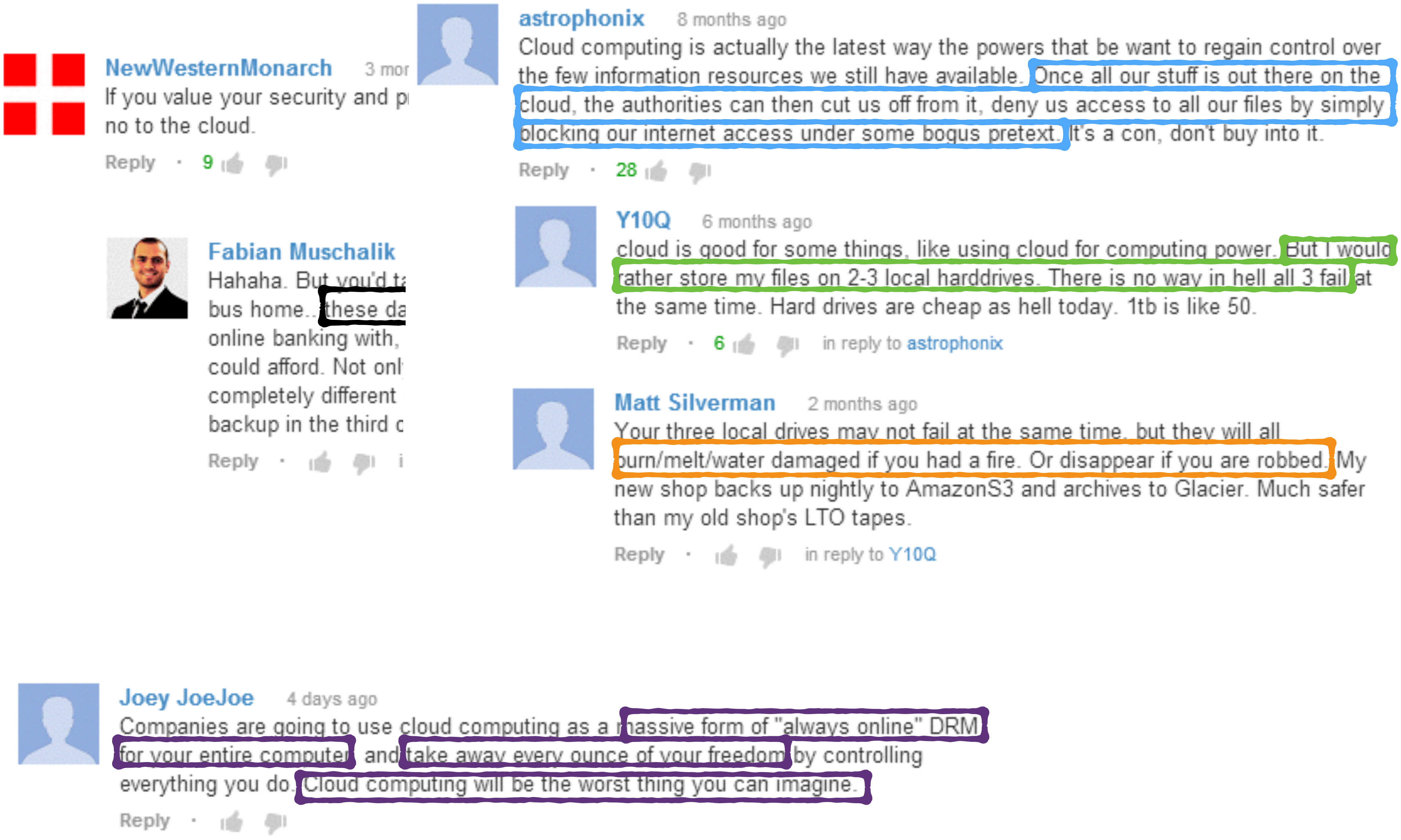
Reply · in reply to Y10Q



Joey JoeJoe 4 days ago

Companies are going to use cloud computing as a massive form of "always online" DRM for your entire computer and take away every ounce of your freedom by controlling everything you do. Cloud computing will be the worst thing you can imagine.

Reply ·



NewWesternMonarch 3 mor

If you value your security and pi
no to the cloud.

Reply · 9

Fabian Muschalik

Hahaha. But you'd ta
bus home.. these da
online banking with,
could afford. Not onl
completely different
backup in the third c

Reply · i

astrophonix 8 months ago

Cloud computing is actually the latest way the powers that be want to regain control over the few information resources we still have available. Once all our stuff is out there on the cloud, the authorities can then cut us off from it, deny us access to all our files by simply blocking our internet access under some bogus pretext. It's a con, don't buy into it.

Reply · 28

Y10Q 6 months ago

cloud is good for some things, like using cloud for computing power. But I would rather store my files on 2-3 local harddrives. There is no way in hell all 3 fail at the same time. Hard drives are cheap as hell today. 1tb is like 50.

Reply · 6 in reply to astrophonix

Matt Silverman 2 months ago

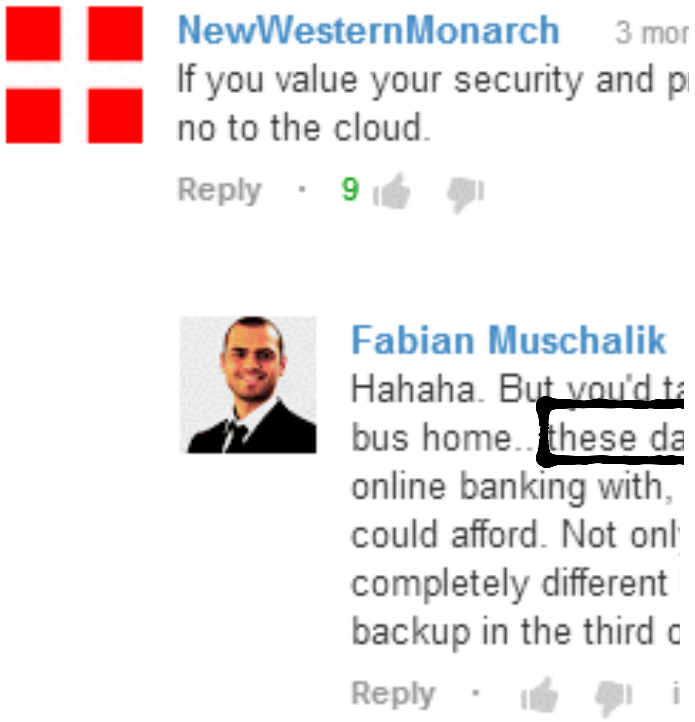
Your three local drives may not fail at the same time, but they will all burn/melt/water damaged if you had a fire. Or disappear if you are robbed. My new shop backs up nightly to AmazonS3 and archives to Glacier. Much safer than my old shop's LTO tapes.

Reply · in reply to Y10Q

Joey JoeJoe 4 days ago

Companies are going to use cloud computing as a massive form of "always online" DRM for your entire computer and take away every ounce of your freedom by controlling everything you do. Cloud computing will be the worst thing you can imagine.

Reply ·



NewWesternMonarch 3 mor

If you value your security and p

no to the cloud.

Reply · 9

Fabian Muschalik

Hahaha. But you'd ta

bus home.. these da

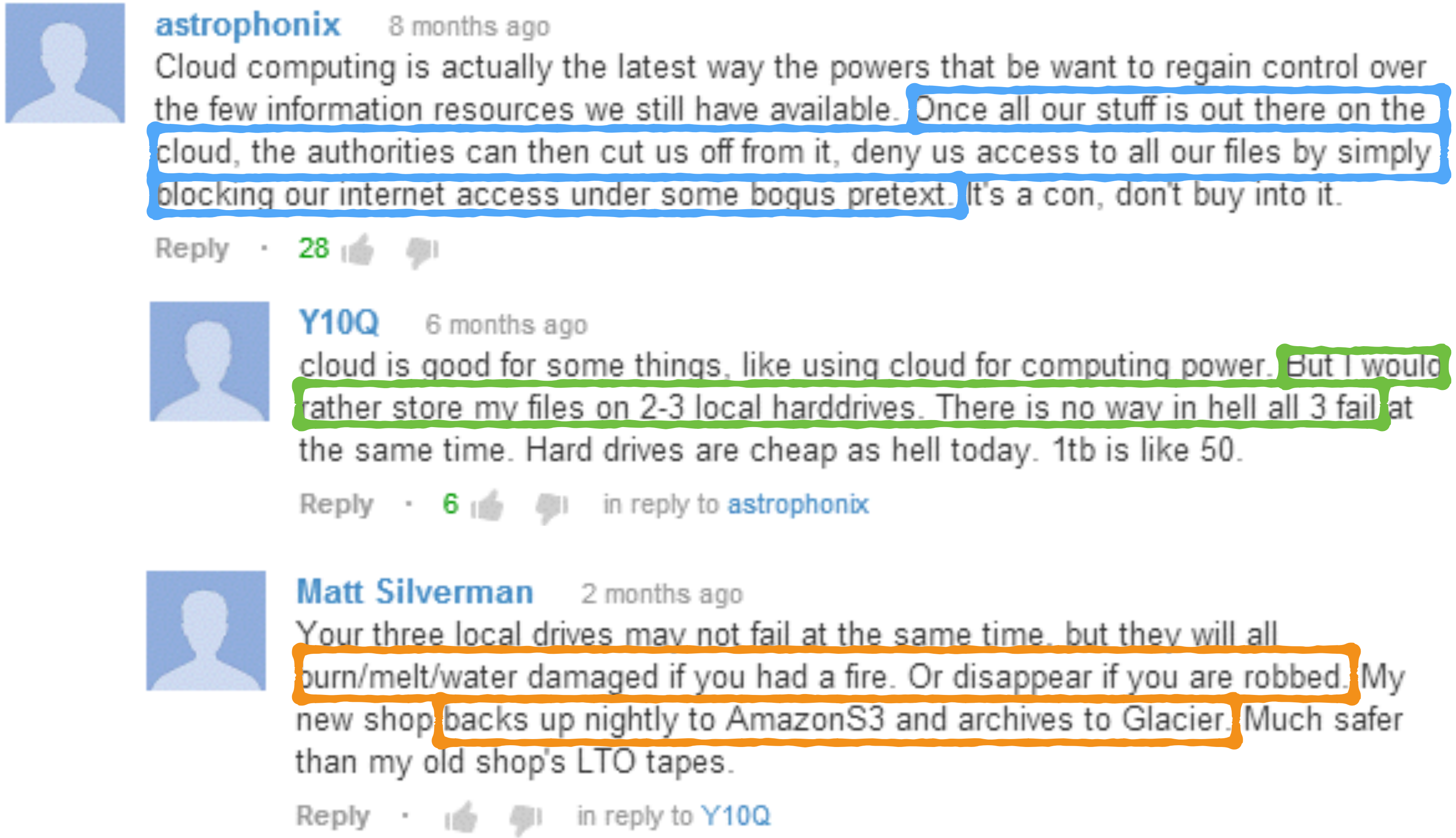
online banking with,

could afford. Not onl

completely different

backup in the third c

Reply · i



astrophonix 8 months ago

Cloud computing is actually the latest way the powers that be want to regain control over the few information resources we still have available. Once all our stuff is out there on the cloud, the authorities can then cut us off from it, deny us access to all our files by simply blocking our internet access under some bogus pretext. It's a con, don't buy into it.

Reply · 28

Y10Q 6 months ago

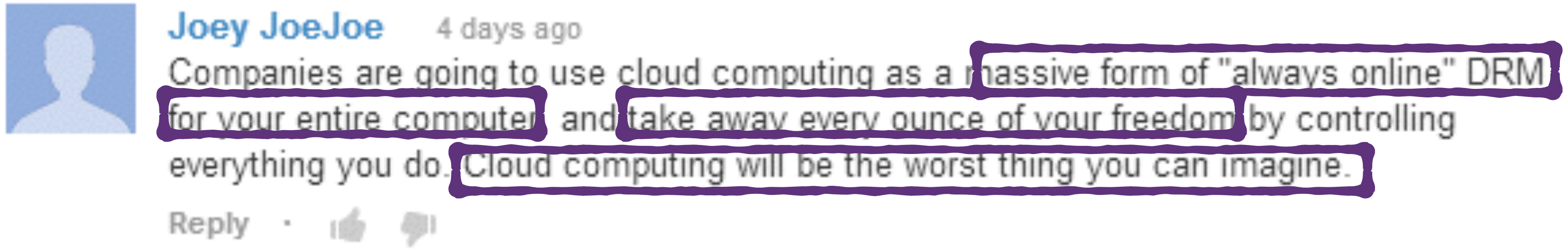
cloud is good for some things, like using cloud for computing power. But I would rather store my files on 2-3 local harddrives. There is no way in hell all 3 fail at the same time. Hard drives are cheap as hell today. 1tb is like 50.

Reply · 6 in reply to astrophonix

Matt Silverman 2 months ago

Your three local drives may not fail at the same time, but they will all burn/melt/water damaged if you had a fire. Or disappear if you are robbed. My new shop backs up nightly to AmazonS3 and archives to Glacier. Much safer than my old shop's LTO tapes.

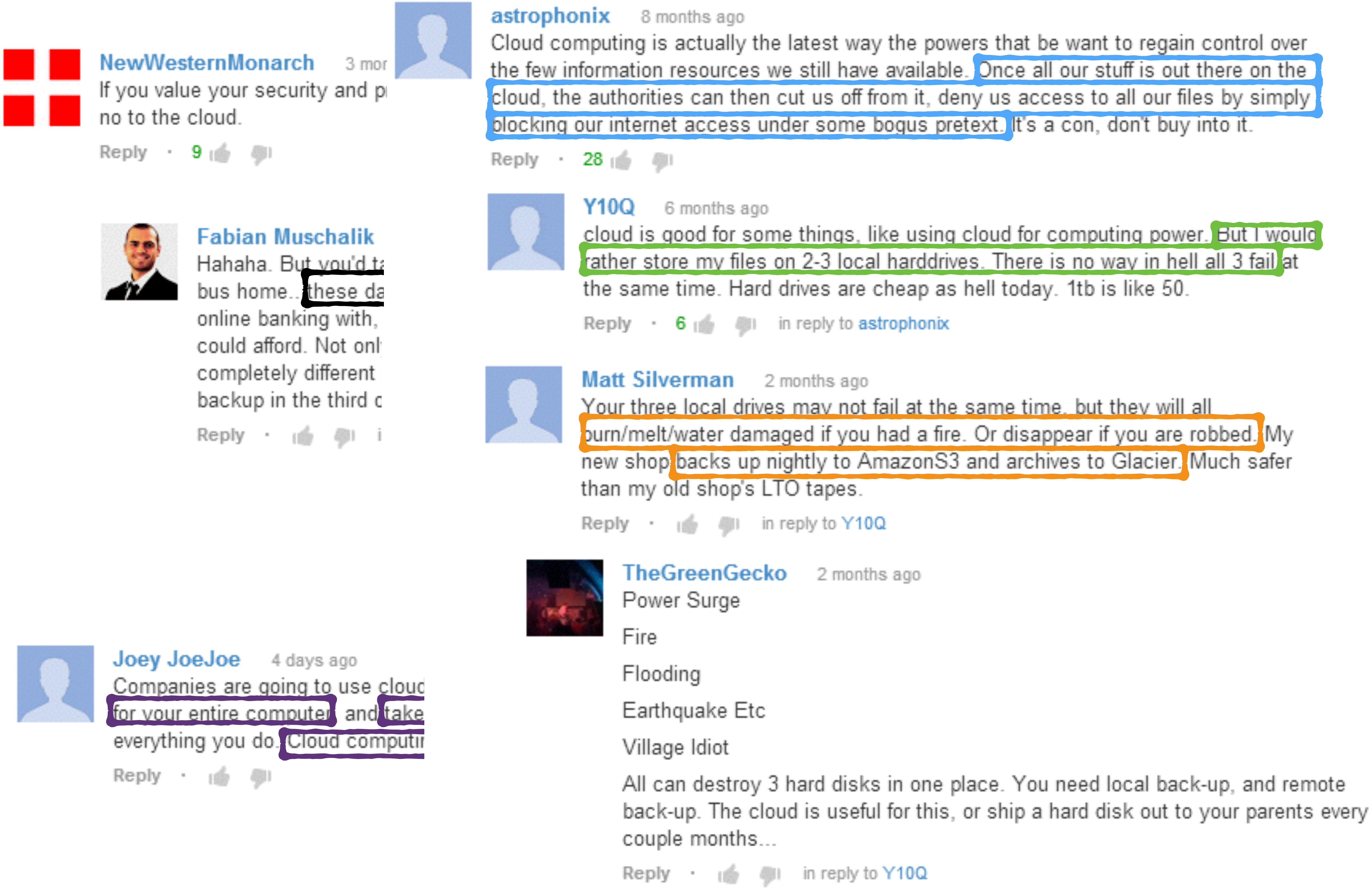
Reply · in reply to Y10Q



Joey JoeJoe 4 days ago

Companies are going to use cloud computing as a massive form of "always online" DRM for your entire computer and take away every ounce of your freedom by controlling everything you do. Cloud computing will be the worst thing you can imagine.

Reply ·



NewWesternMonarch 3 mor
If you value your security and pı
no to the cloud.
Reply · 9

Fabian Muschalik
Hahaha. But you'd ta
bus home.. these da
online banking with,
could afford. Not onl
completely different
backup in the third c
Reply · i

Joey JoeJoe 4 days ago
Companies are going to use cloud
for your entire computer and take
everything you do. Cloud computir
Reply ·

astrophonix 8 months ago
Cloud computing is actually the latest way the powers that be want to regain control over the few information resources we still have available. Once all our stuff is out there on the cloud, the authorities can then cut us off from it, deny us access to all our files by simply blocking our internet access under some bogus pretext. It's a con, don't buy into it.
Reply · 28

Y10Q 6 months ago
cloud is good for some things, like using cloud for computing power. But I would rather store my files on 2-3 local harddrives. There is no way in hell all 3 fail at the same time. Hard drives are cheap as hell today. 1tb is like 50.
Reply · 6 in reply to astrophonix

Matt Silverman 2 months ago
Your three local drives may not fail at the same time, but they will all burn/melt/water damaged if you had a fire. Or disappear if you are robbed. My new shop backs up nightly to AmazonS3 and archives to Glacier. Much safer than my old shop's LTO tapes.
Reply · in reply to Y10Q

TheGreenGecko 2 months ago
Power Surge

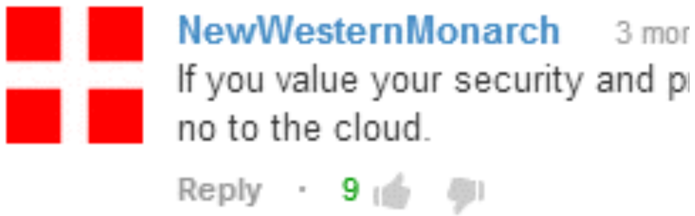
Fire

Flooding

Earthquake Etc

Village Idiot

All can destroy 3 hard disks in one place. You need local back-up, and remote back-up. The cloud is useful for this, or ship a hard disk out to your parents every couple months...
Reply · in reply to Y10Q

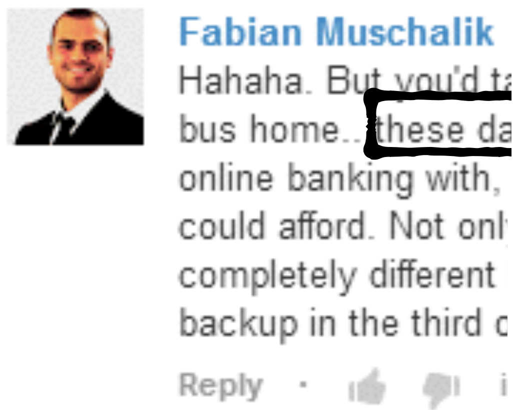


NewWesternMonarch 3 mor

If you value your security and p

no to the cloud.

Reply · 9



Fabian Muschalik

Hahaha. But you'd ta

bus home.. these da

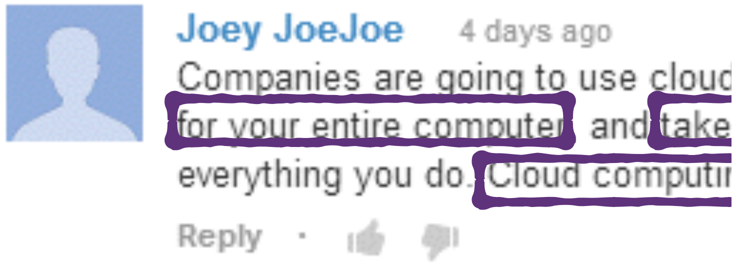
online banking with,

could afford. Not onl

completely different

backup in the third c

Reply · i



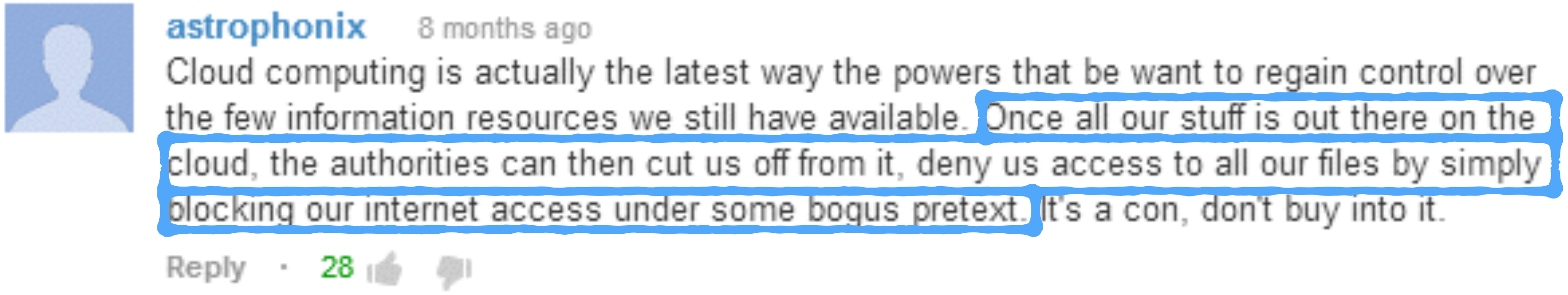
Joey JoeJoe 4 days ago

Companies are going to use cloud

for your entire computer and take

everything you do. Cloud computi

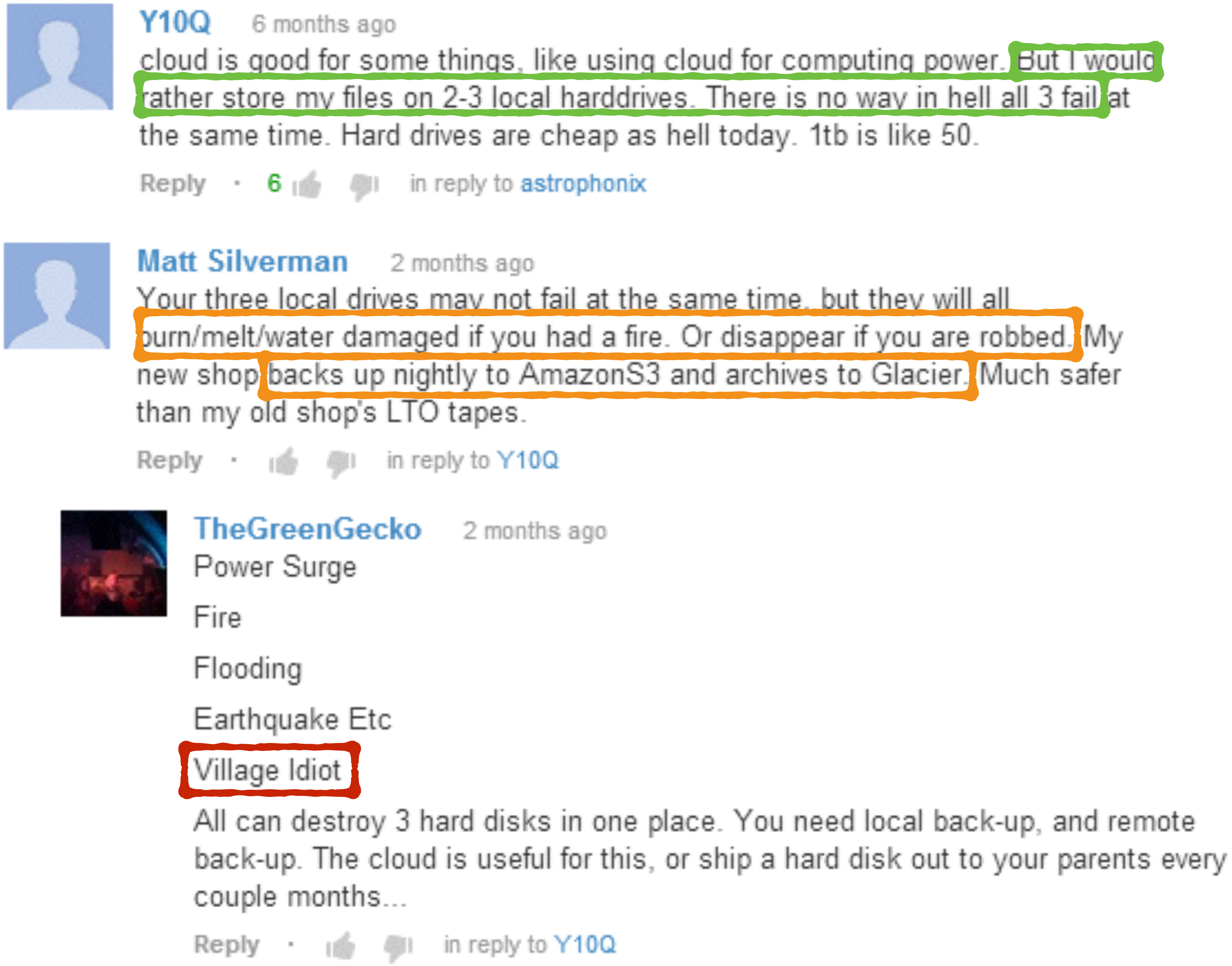
Reply ·



astrophonix 8 months ago

Cloud computing is actually the latest way the powers that be want to regain control over the few information resources we still have available. Once all our stuff is out there on the cloud, the authorities can then cut us off from it, deny us access to all our files by simply blocking our internet access under some bogus pretext. It's a con, don't buy into it.

Reply · 28



Y10Q 6 months ago

cloud is good for some things, like using cloud for computing power. But I would rather store my files on 2-3 local harddrives. There is no way in hell all 3 fail at the same time. Hard drives are cheap as hell today. 1tb is like 50.

Reply · 6 in reply to astrophonix

Matt Silverman 2 months ago

Your three local drives may not fail at the same time, but they will all burn/melt/water damaged if you had a fire. Or disappear if you are robbed. My new shop backs up nightly to AmazonS3 and archives to Glacier. Much safer than my old shop's LTO tapes.

Reply · in reply to Y10Q

TheGreenGecko 2 months ago

Power Surge

Fire

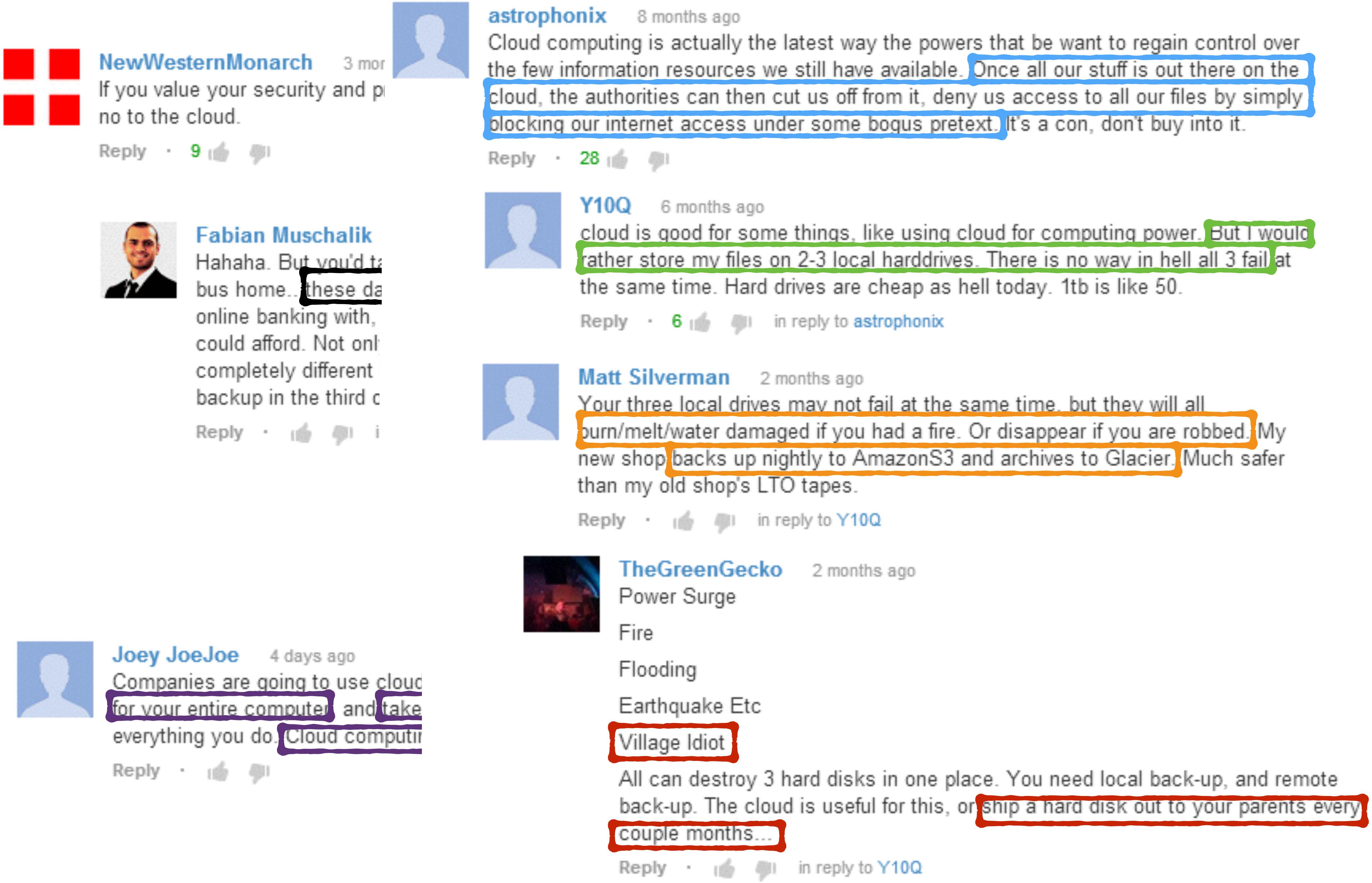
Flooding

Earthquake Etc

Village Idiot

All can destroy 3 hard disks in one place. You need local back-up, and remote back-up. The cloud is useful for this, or ship a hard disk out to your parents every couple months...

Reply · in reply to Y10Q



NewWesternMonarch 3 mor
If you value your security and p
no to the cloud.
Reply · 9

Fabian Muschalik
Hahaha. But you'd ta
bus home.. these da
online banking with,
could afford. Not onl
completely different
backup in the third c
Reply · i

astrophonix 8 months ago
Cloud computing is actually the latest way the powers that be want to regain control over the few information resources we still have available. Once all our stuff is out there on the cloud, the authorities can then cut us off from it, deny us access to all our files by simply blocking our internet access under some bogus pretext. It's a con, don't buy into it.
Reply · 28

Y10Q 6 months ago
cloud is good for some things, like using cloud for computing power. But I would rather store my files on 2-3 local harddrives. There is no way in hell all 3 fail at the same time. Hard drives are cheap as hell today. 1tb is like 50.
Reply · 6 in reply to astrophonix

Matt Silverman 2 months ago
Your three local drives may not fail at the same time, but they will all burn/melt/water damaged if you had a fire. Or disappear if you are robbed. My new shop backs up nightly to AmazonS3 and archives to Glacier. Much safer than my old shop's LTO tapes.
Reply · in reply to Y10Q

TheGreenGecko 2 months ago
Power Surge

Fire

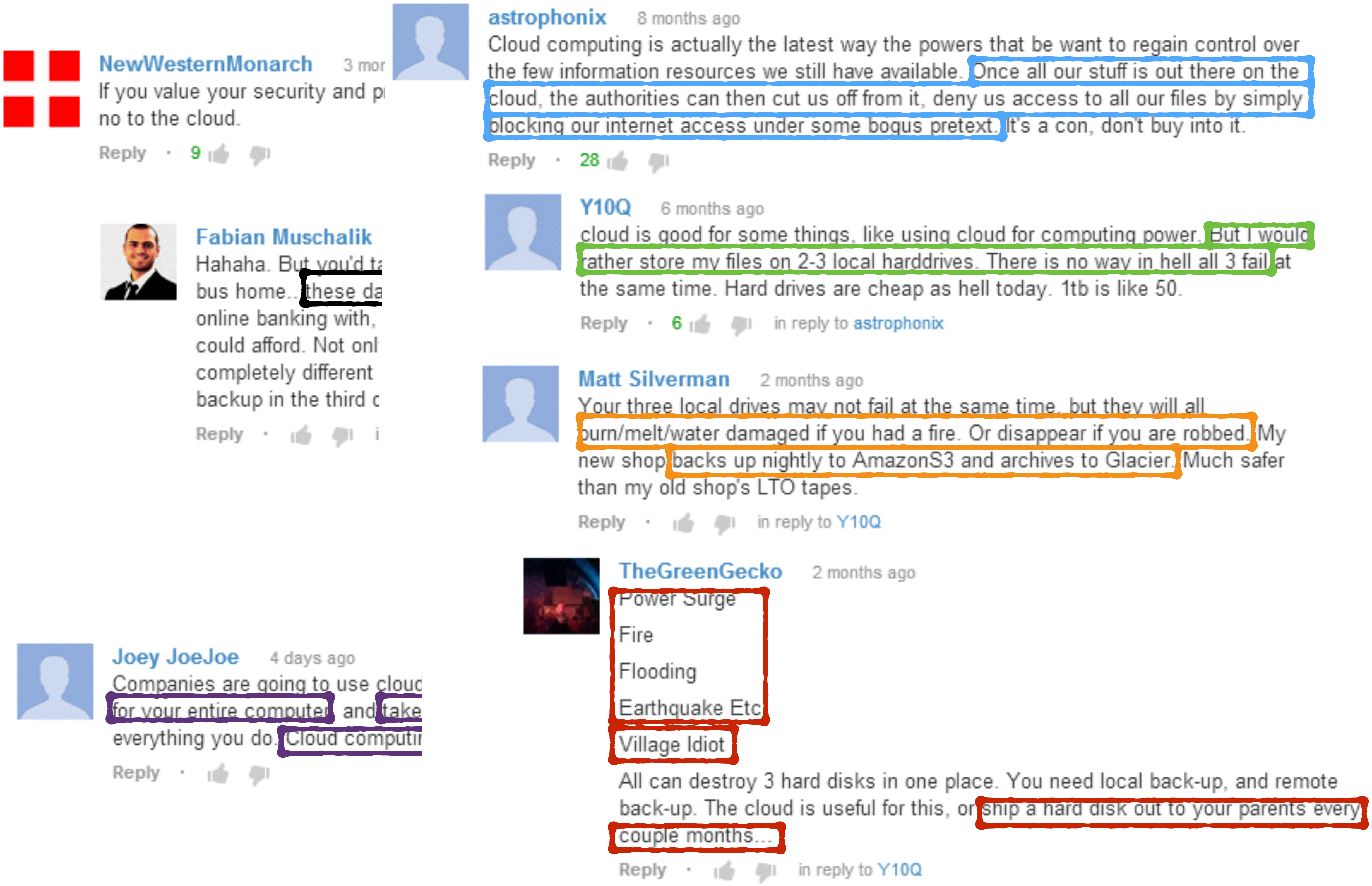
Flooding

Earthquake Etc

Village Idiot

All can destroy 3 hard disks in one place. You need local back-up, and remote back-up. The cloud is useful for this, or ship a hard disk out to your parents every couple months...
Reply · in reply to Y10Q

Joey JoeJoe 4 days ago
Companies are going to use cloud
for your entire computer and take
everything you do. Cloud computi
Reply ·



NewWesternMonarch 3 mor

If you value your security and p

no to the cloud.

Reply · 9

Fabian Muschalik

Hahaha. But you'd ta

bus home.. these da

online banking with,

could afford. Not onl

completely different

backup in the third c

Reply · i

Joey JoeJoe 4 days ago

Companies are going to use cloud

for your entire computer and take

everything you do. Cloud computi

Reply ·

astrophonix 8 months ago

Cloud computing is actually the latest way the powers that be want to regain control over the few information resources we still have available. Once all our stuff is out there on the cloud, the authorities can then cut us off from it, deny us access to all our files by simply blocking our internet access under some bogus pretext. It's a con, don't buy into it.

Reply · 28

Y10Q 6 months ago

cloud is good for some things, like using cloud for computing power. But I would rather store my files on 2-3 local harddrives. There is no way in hell all 3 fail at the same time. Hard drives are cheap as hell today. 1tb is like 50.

Reply · 6 in reply to astrophonix

Matt Silverman 2 months ago

Your three local drives may not fail at the same time, but they will all burn/melt/water damaged if you had a fire. Or disappear if you are robbed. My new shop backs up nightly to AmazonS3 and archives to Glacier. Much safer than my old shop's LTO tapes.

Reply · in reply to Y10Q

TheGreenGecko 2 months ago

Power Surge

Fire

Flooding

Earthquake Etc

Village Idiot

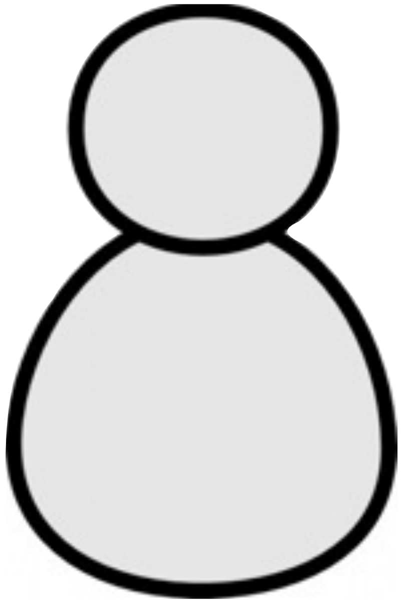
All can destroy 3 hard disks in one place. You need local back-up, and remote back-up. The cloud is useful for this, or ship a hard disk out to your parents every couple months...

Reply · in reply to Y10Q

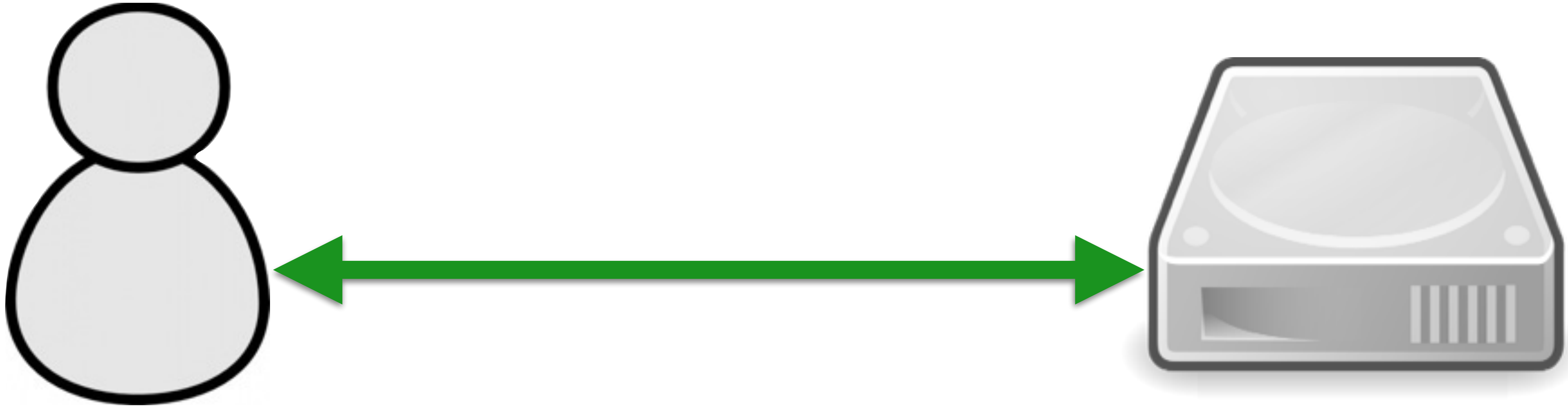
Storage Outsourcing

In-premises Storage

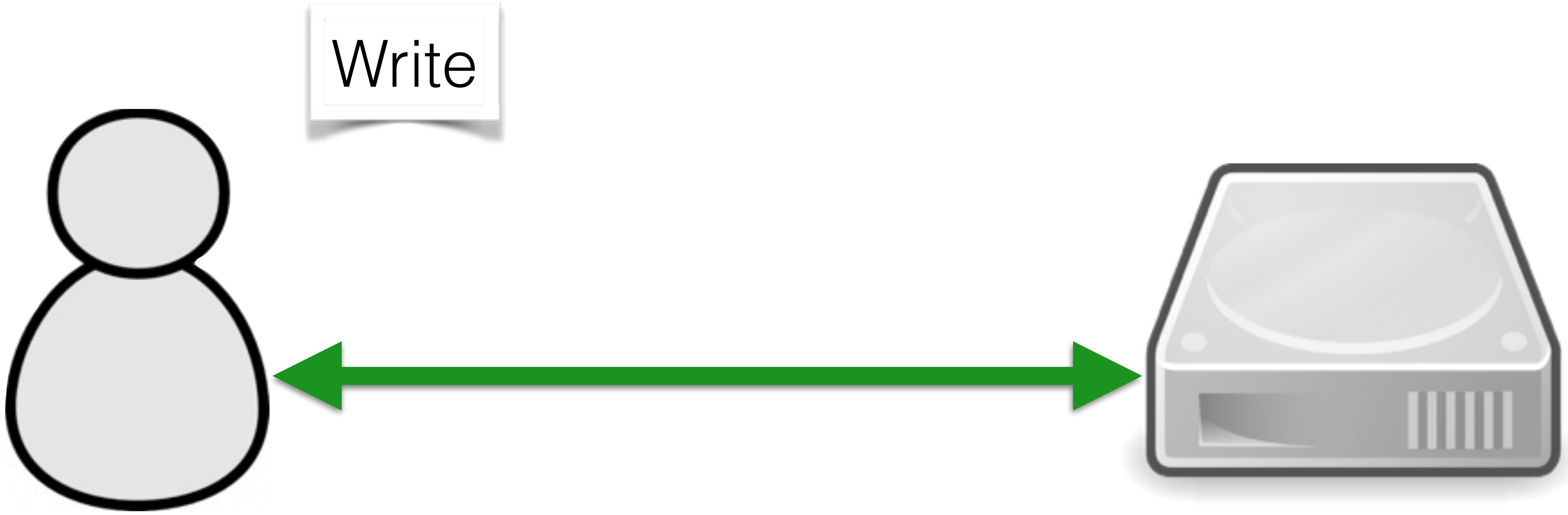
In-premises Storage



In-premises Storage

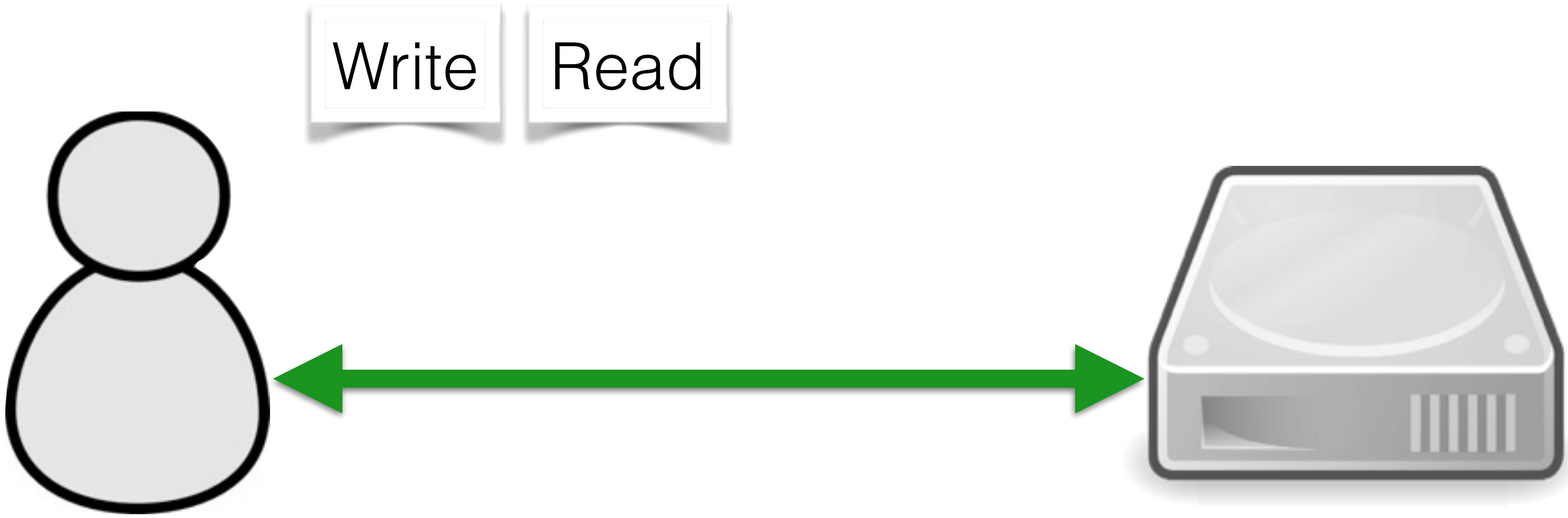


In-premises Storage



Write

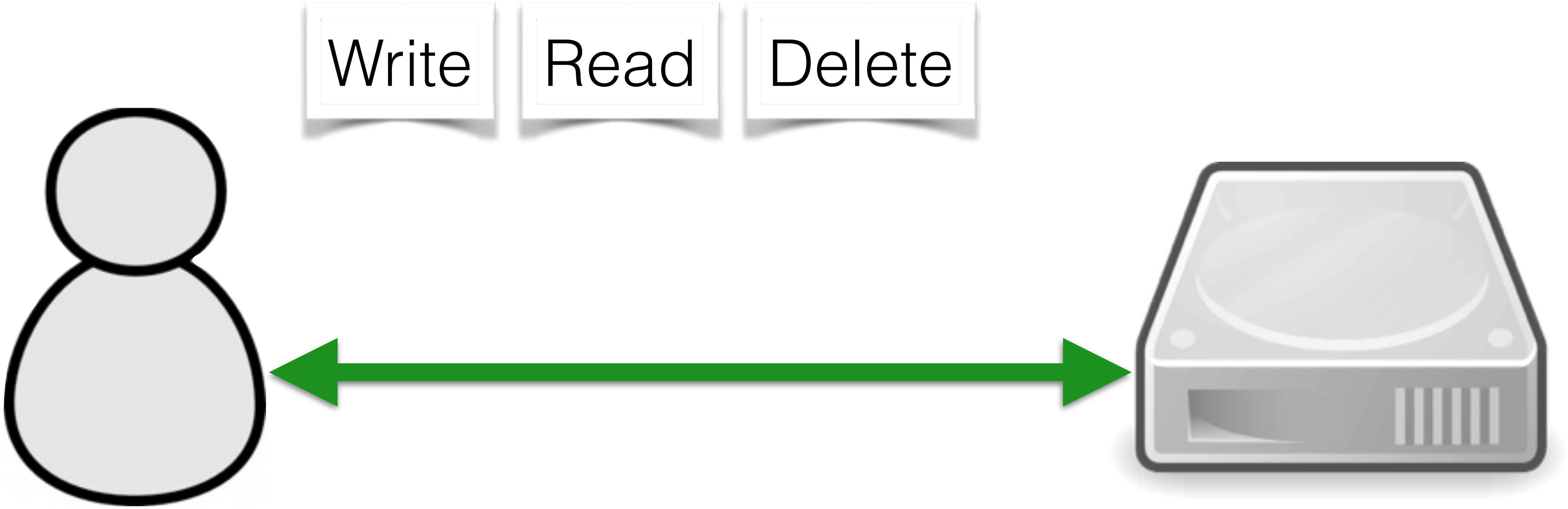
In-premises Storage



Write

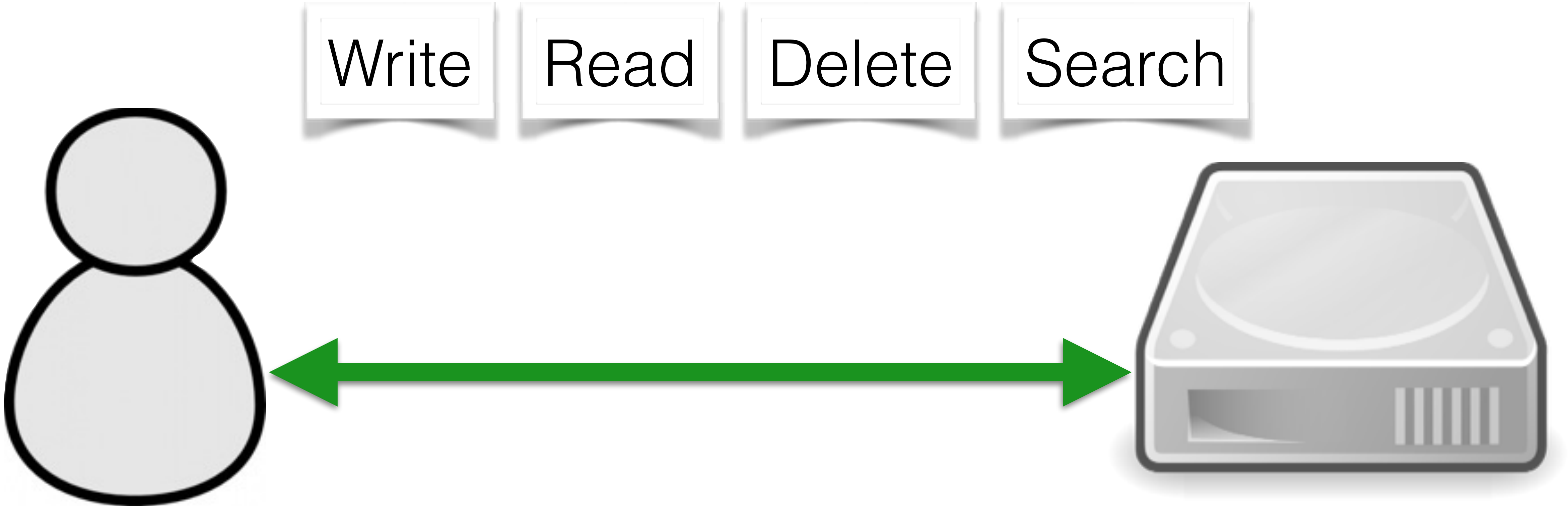
Read

In-premises Storage



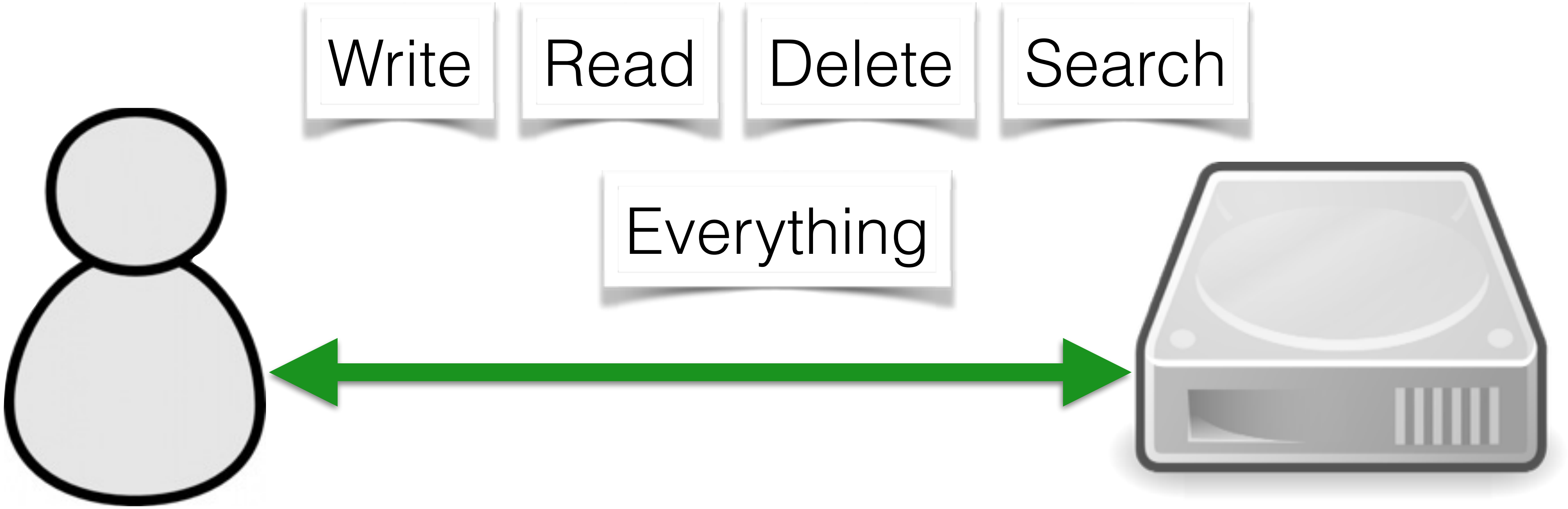
Write Read Delete

In-premises Storage



Write Read Delete Search

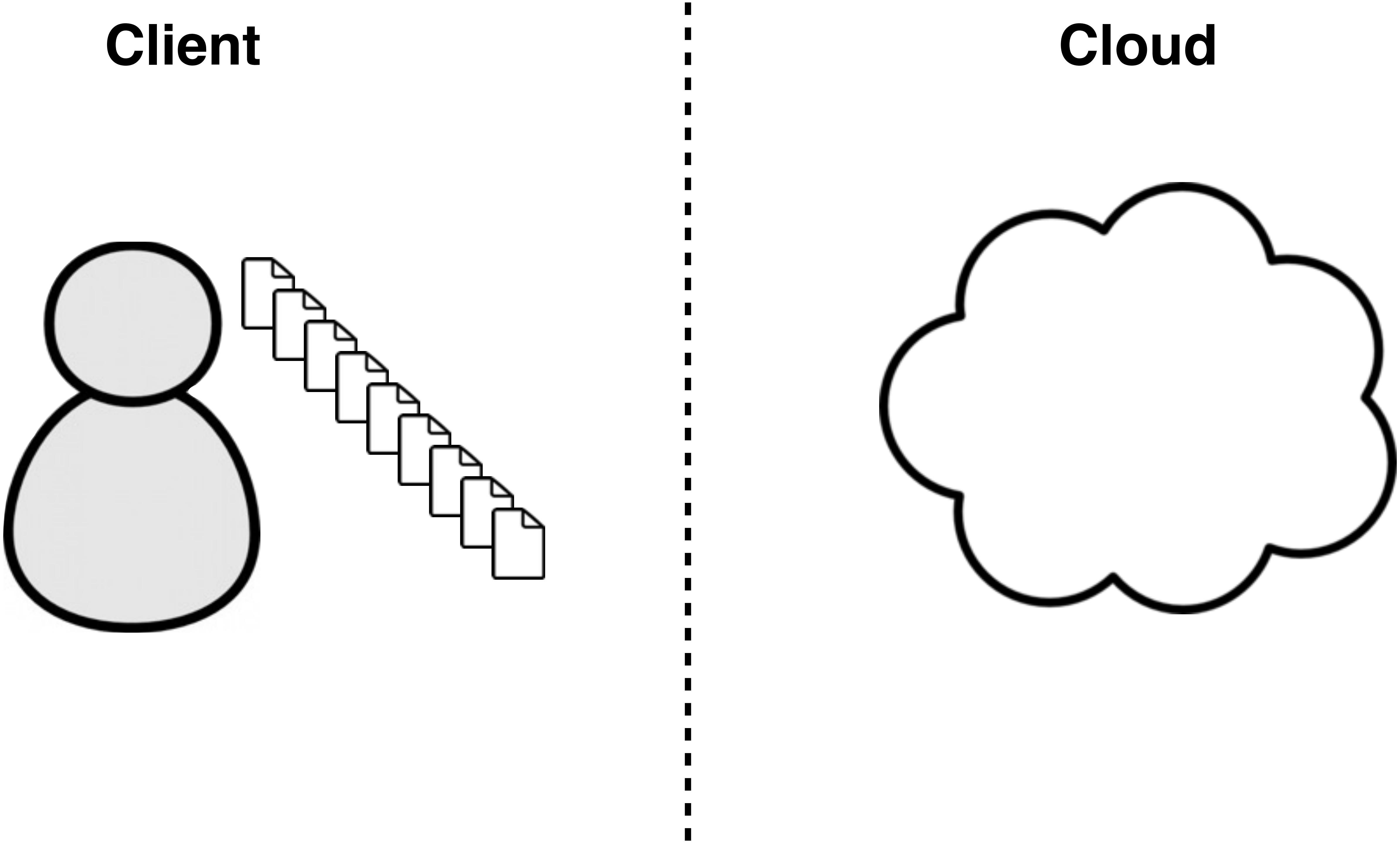
In-premises Storage



Write Read Delete Search

Everything

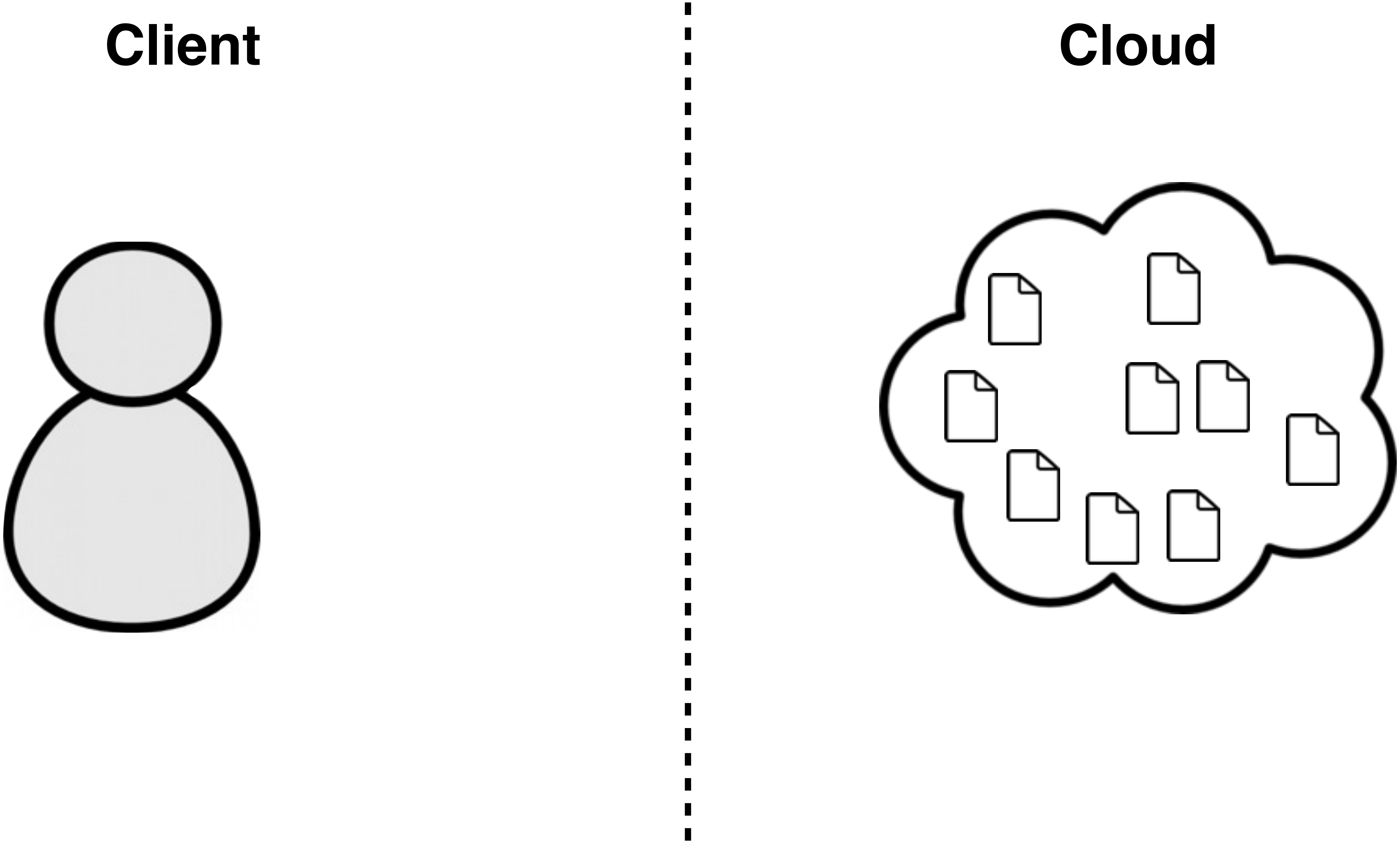
Storage Outsourcing



Client

Cloud

Storage Outsourcing



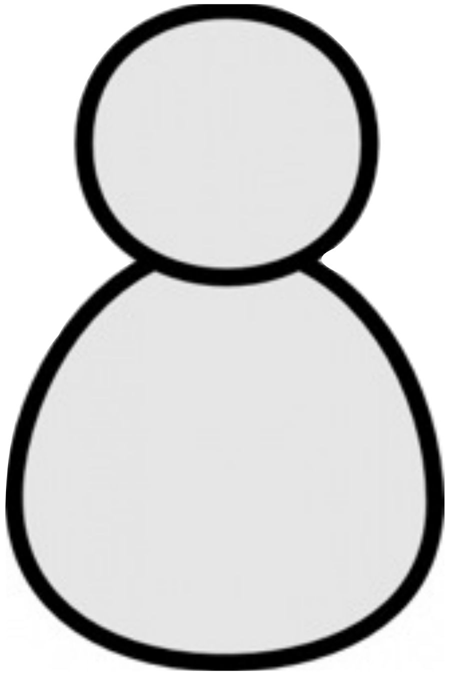
Client

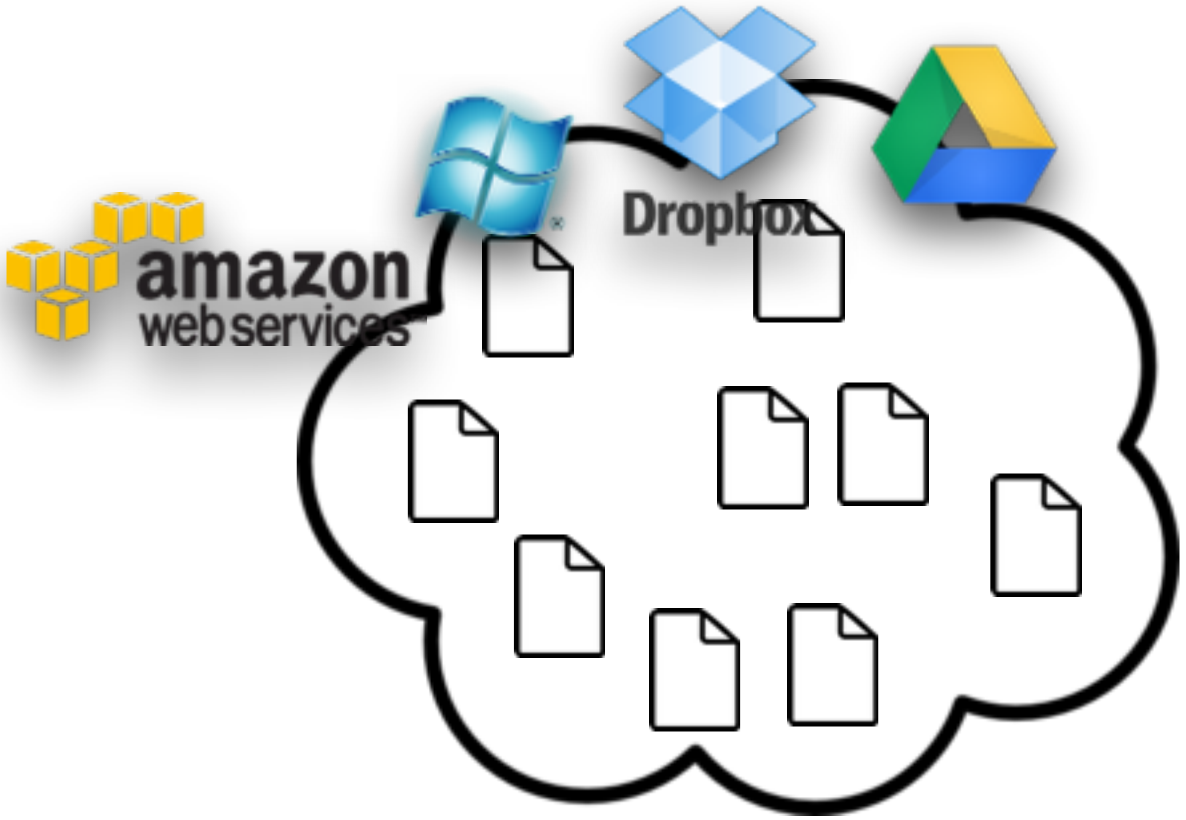
Cloud

Storage Outsourcing

Client

Cloud





Storage Outsourcing

Client

Cloud

Storage Outsourcing

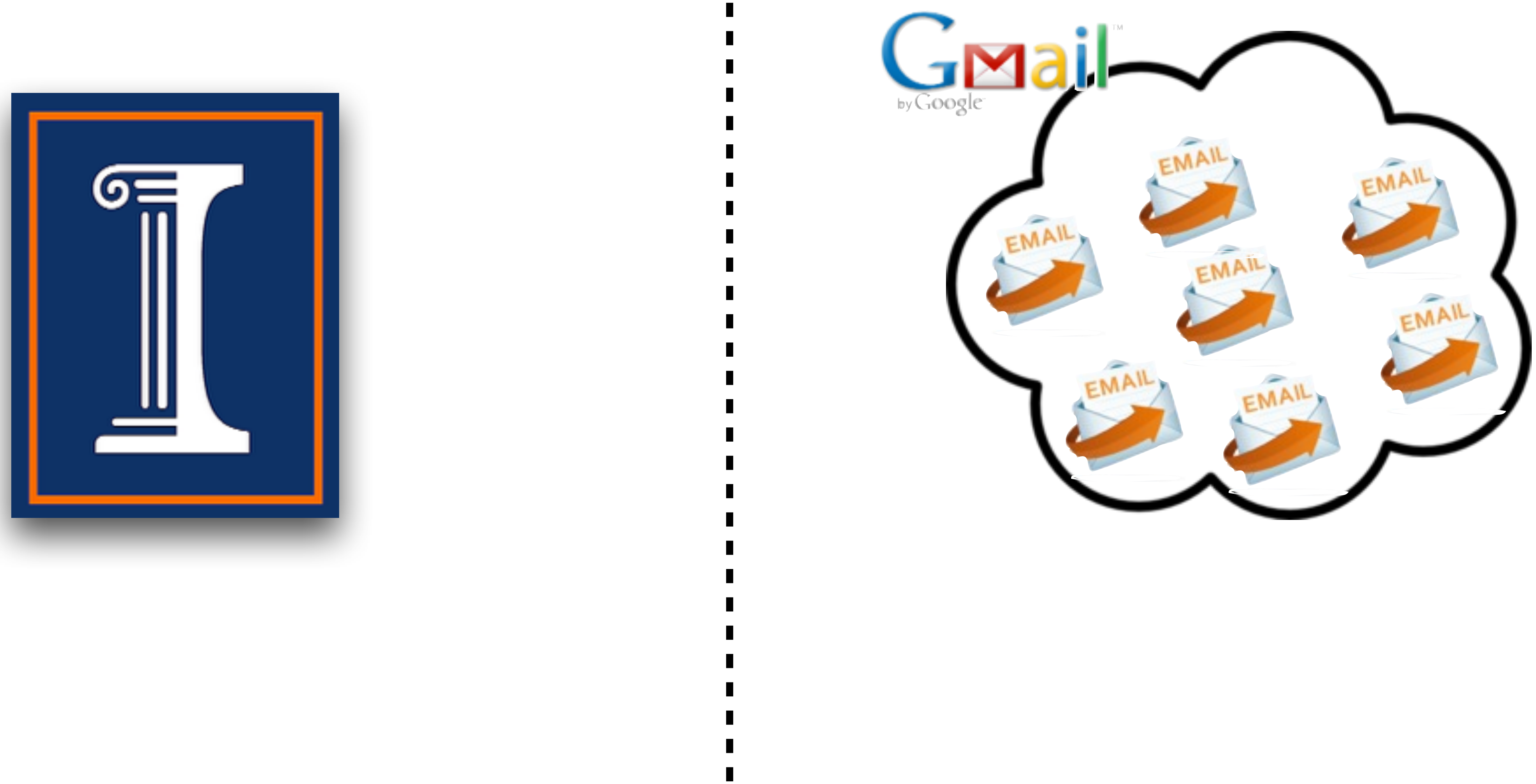
Client

Cloud

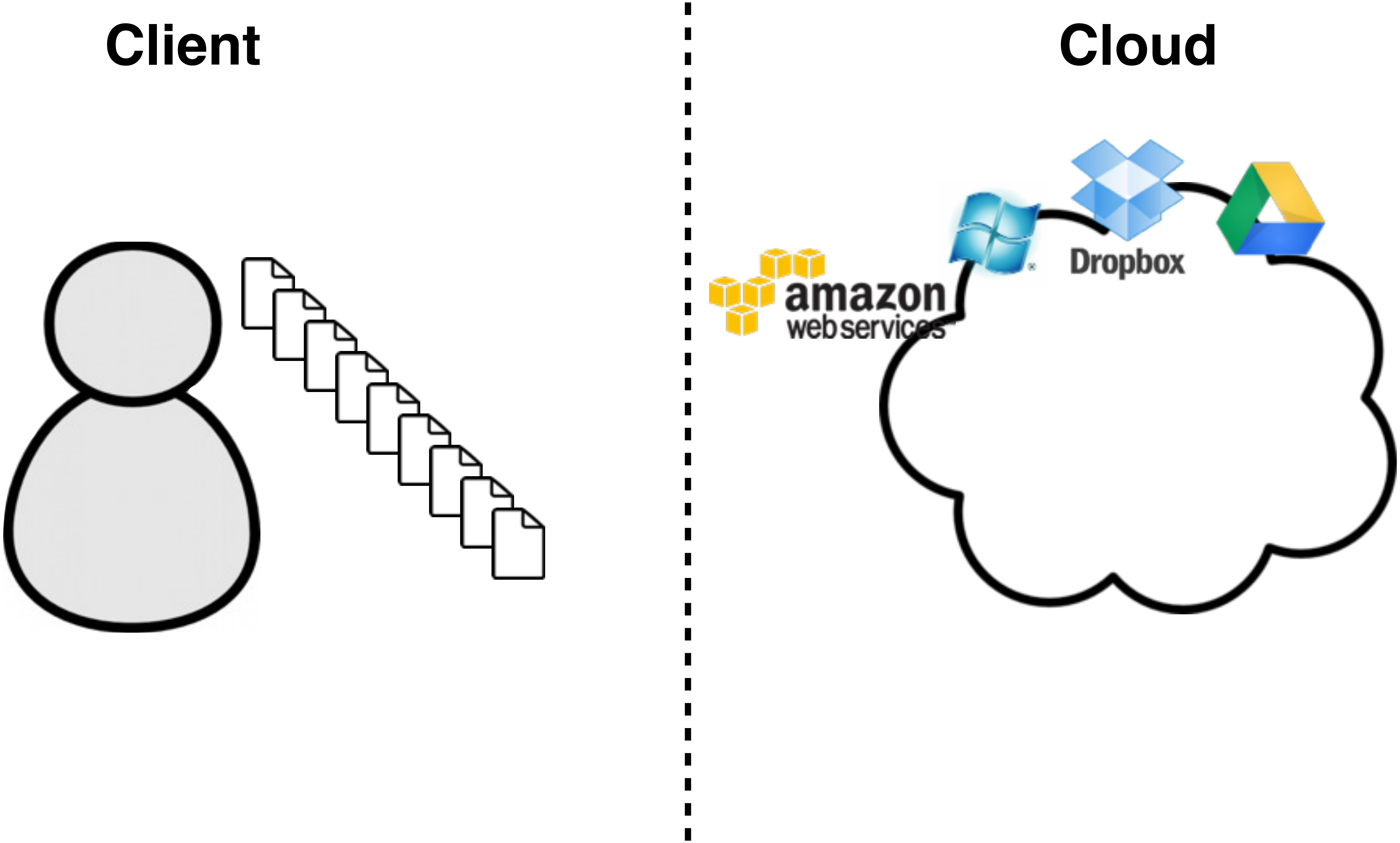
Storage Outsourcing

Client

Cloud



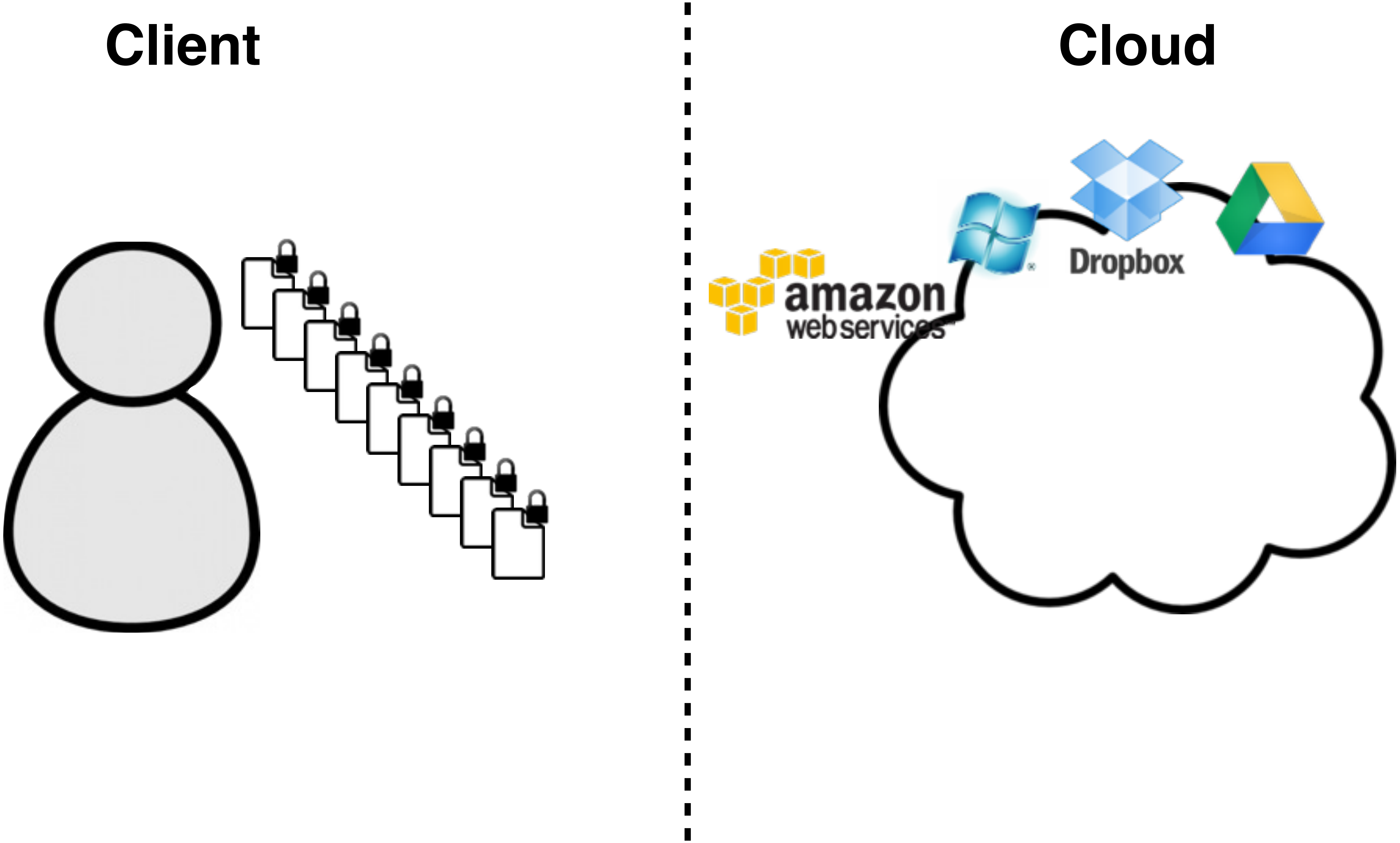
Naive Encryption?



Client

Cloud

Naive Encryption?



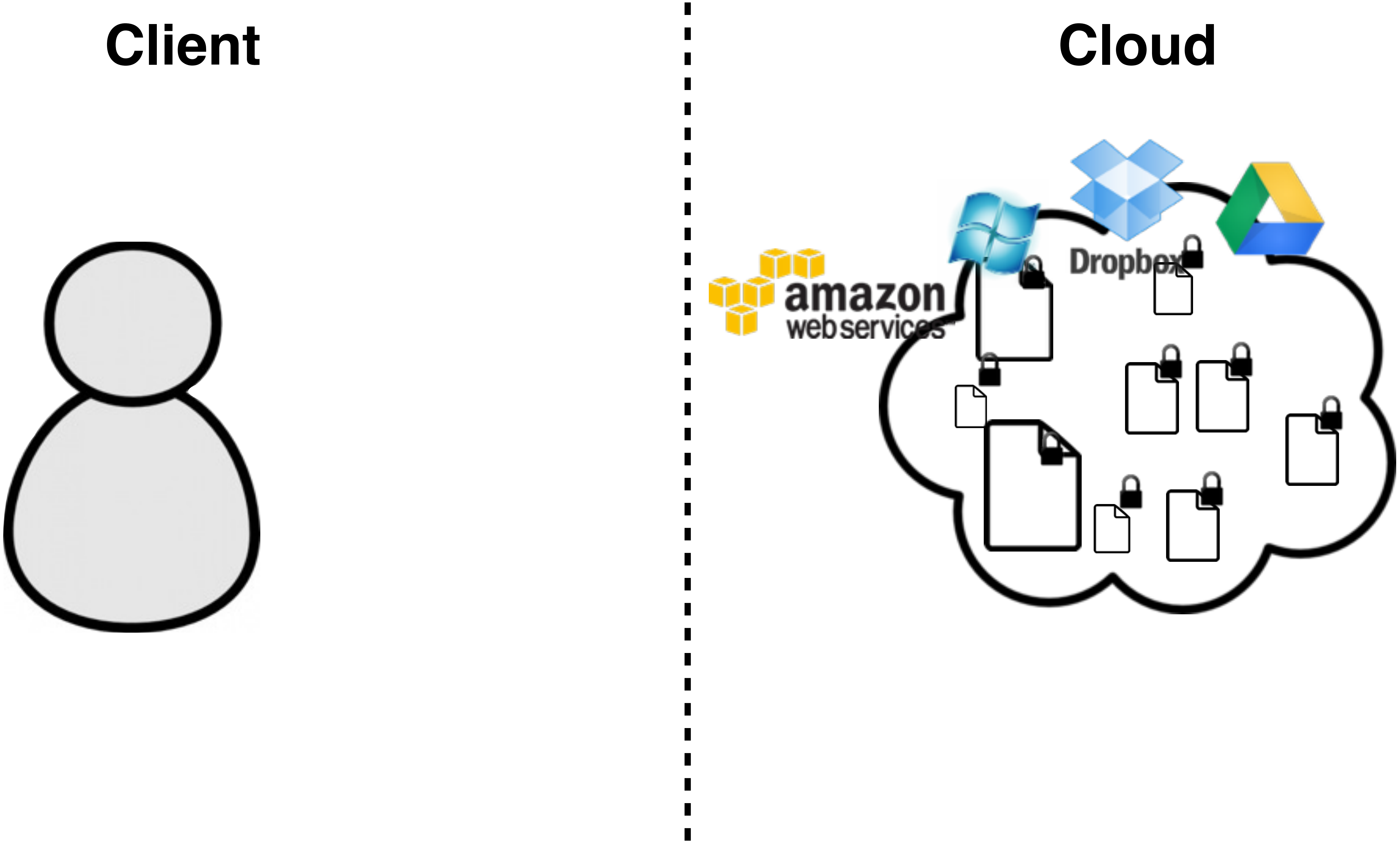
Client

Cloud

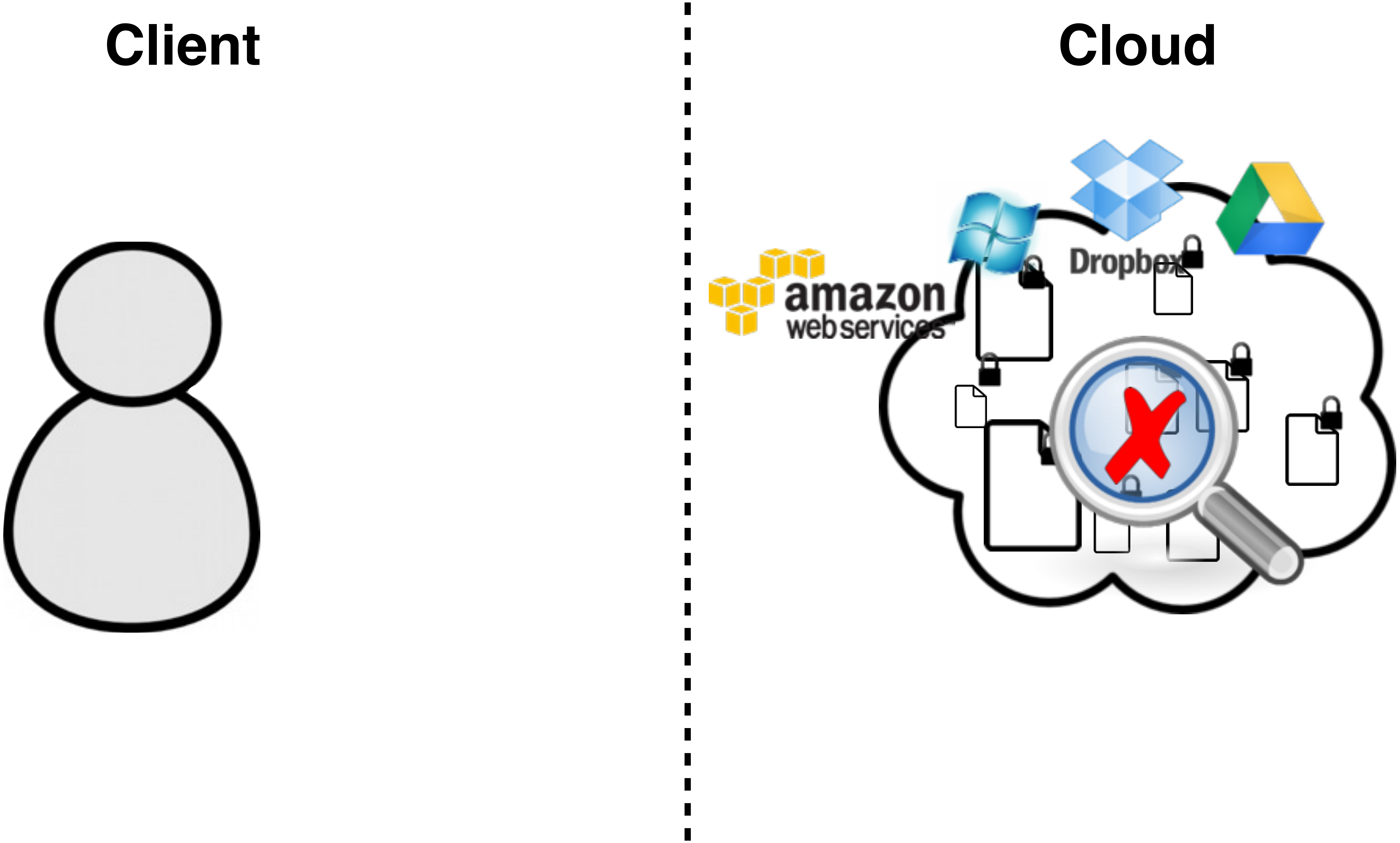
Naive Encryption?

Client

Cloud



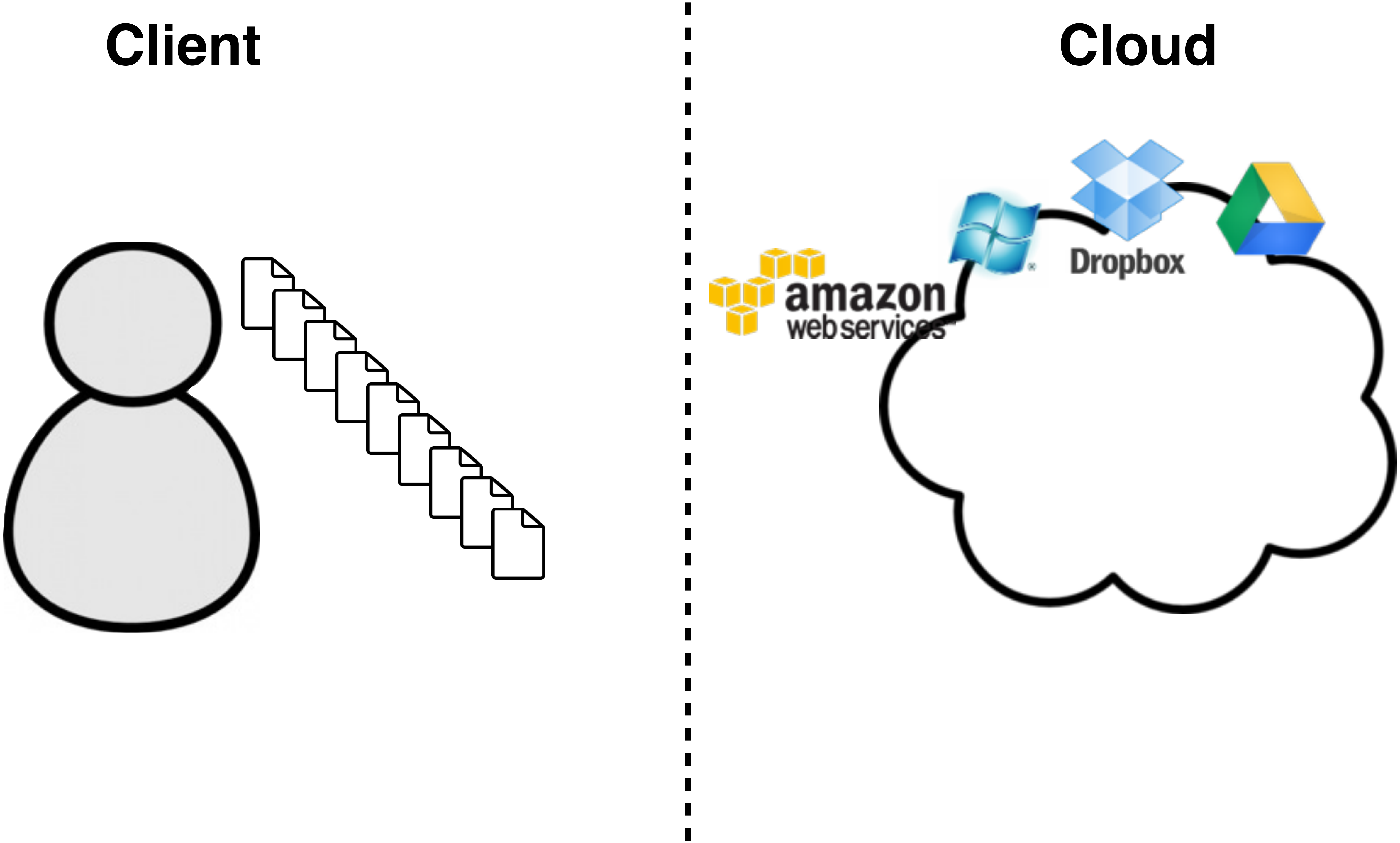
Naive Encryption?



Client

Cloud

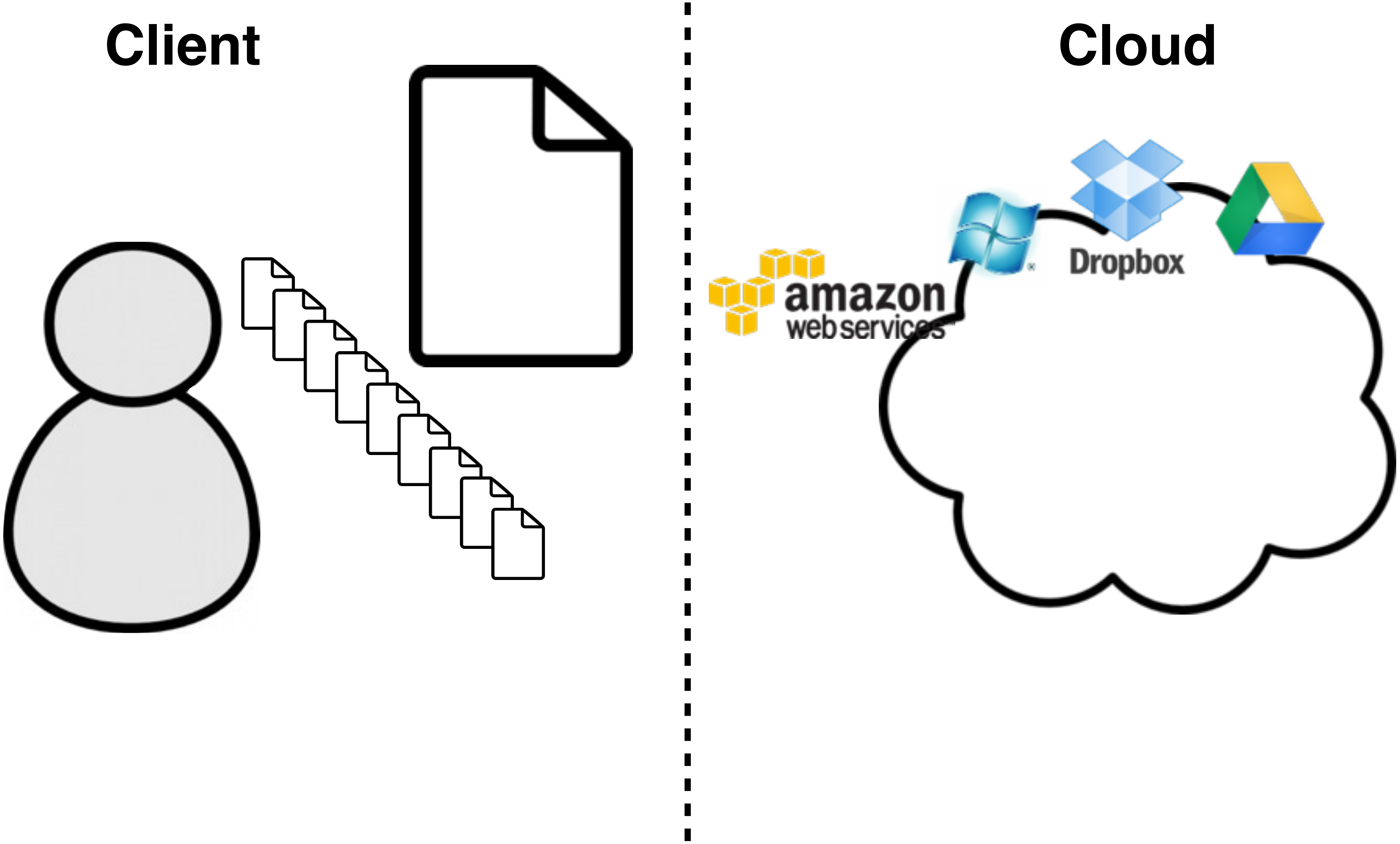
Naive Encryption



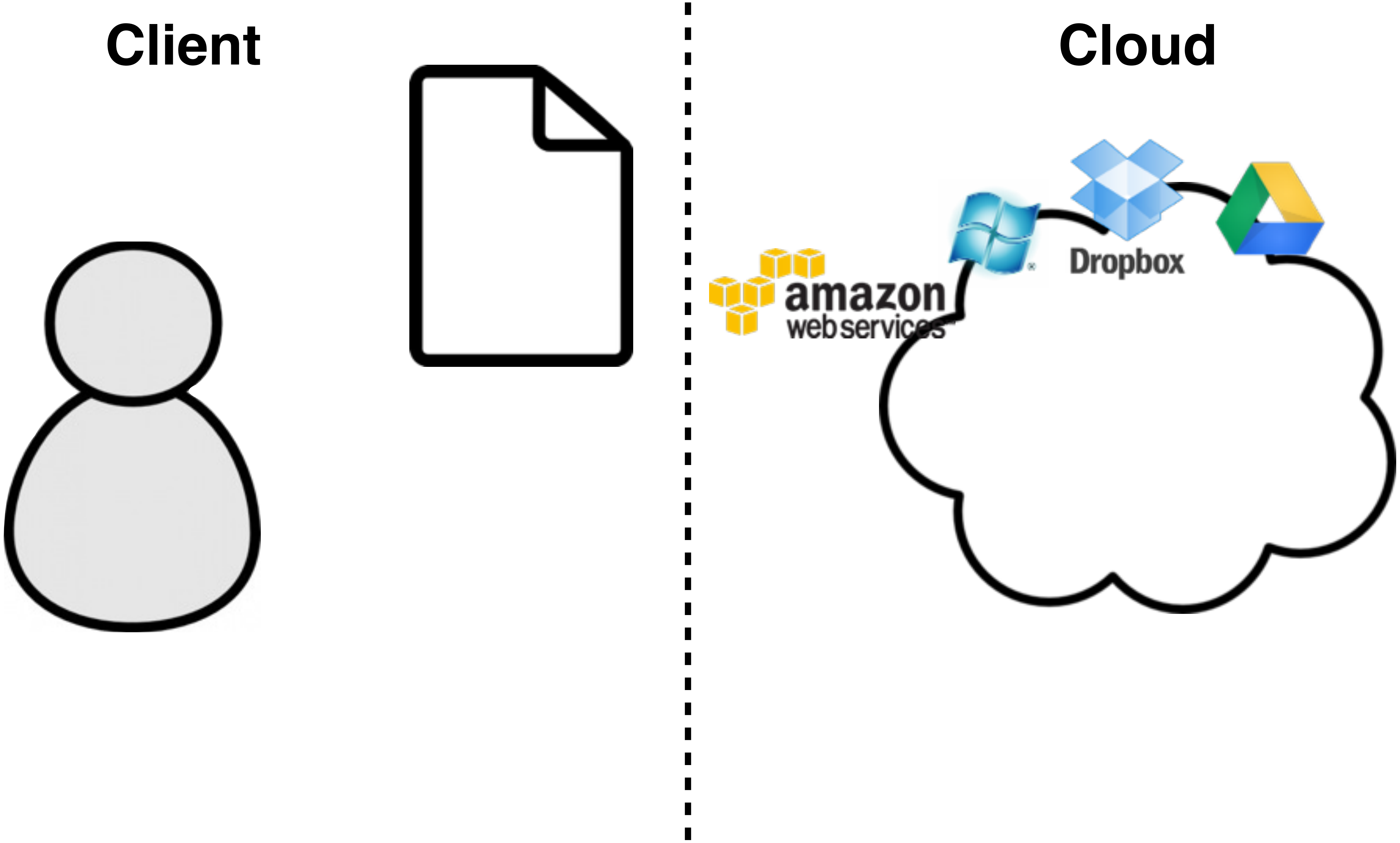
Client

Cloud

Naive Encryption



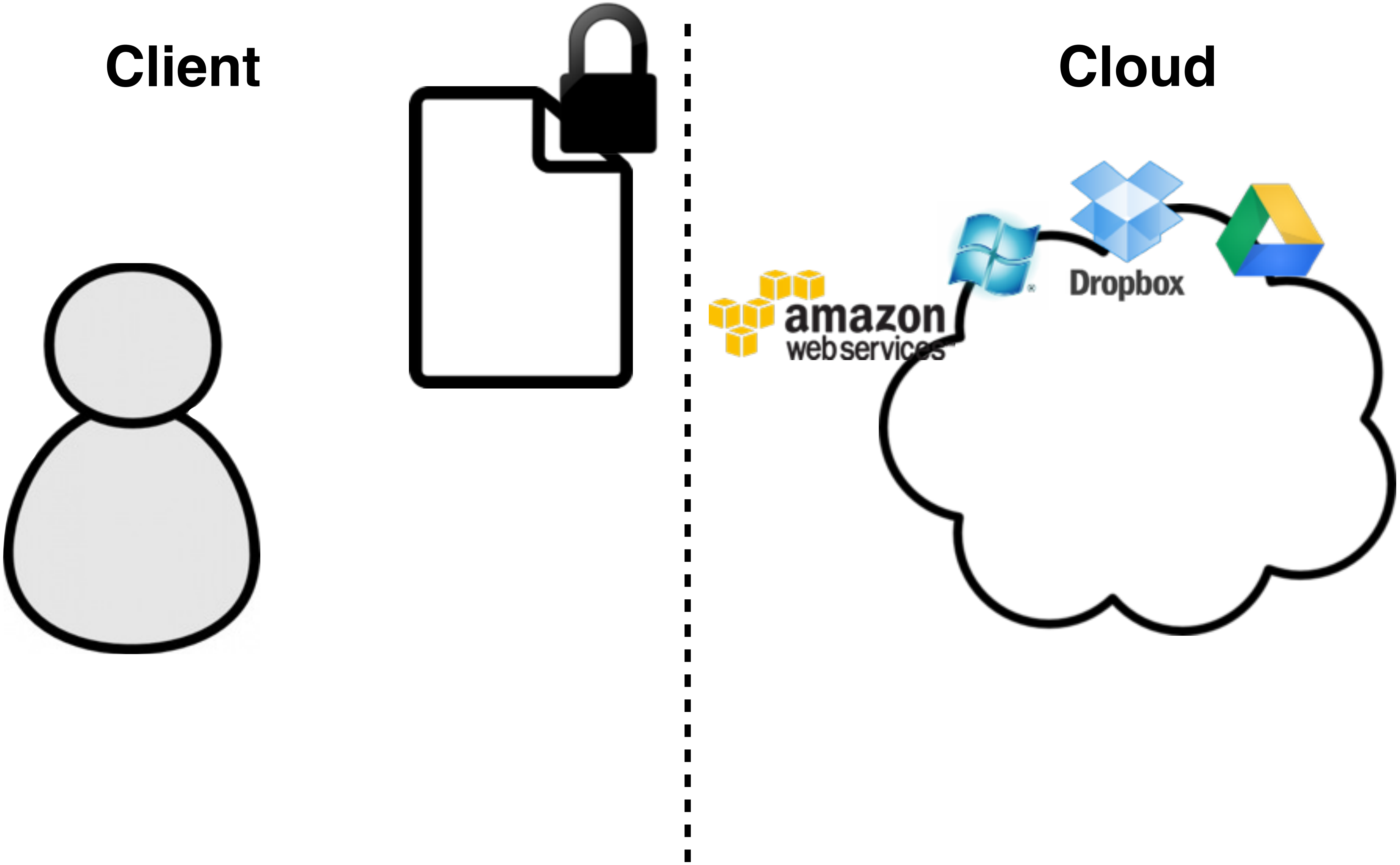
Naive Encryption



Client

Cloud

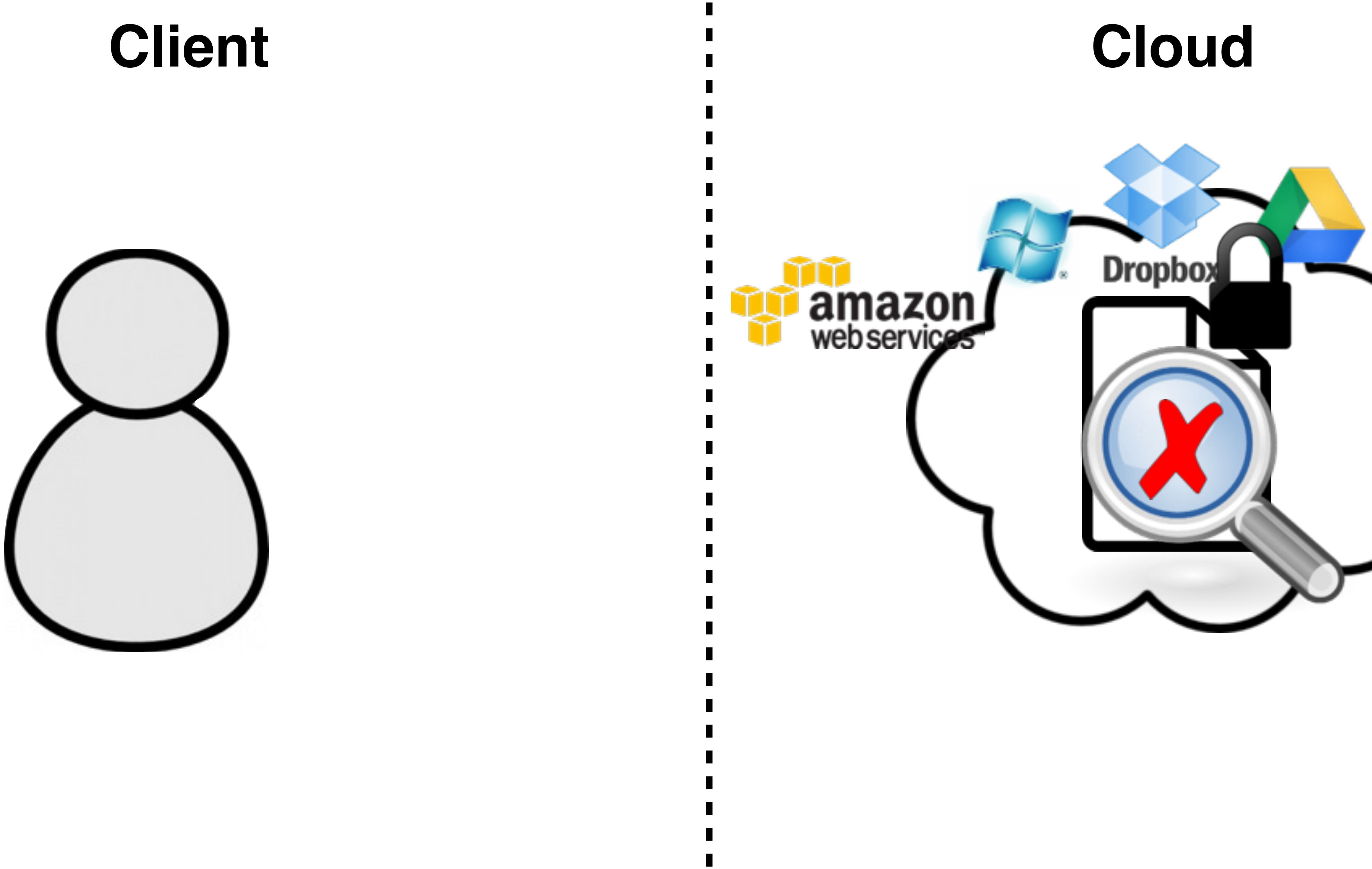
Naive Encryption



Client

Cloud

Naive Encryption

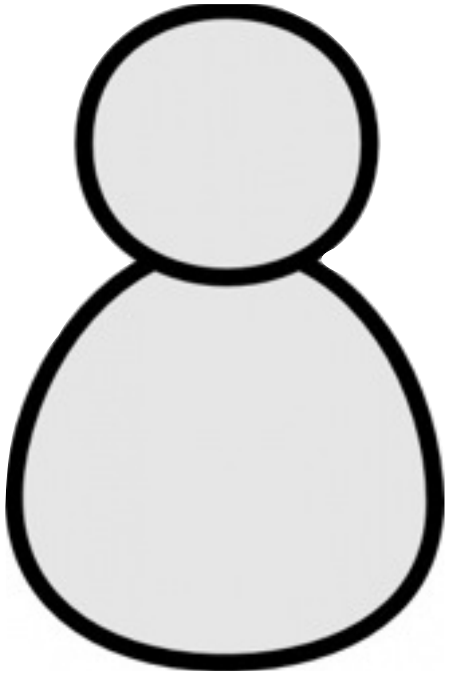


Client

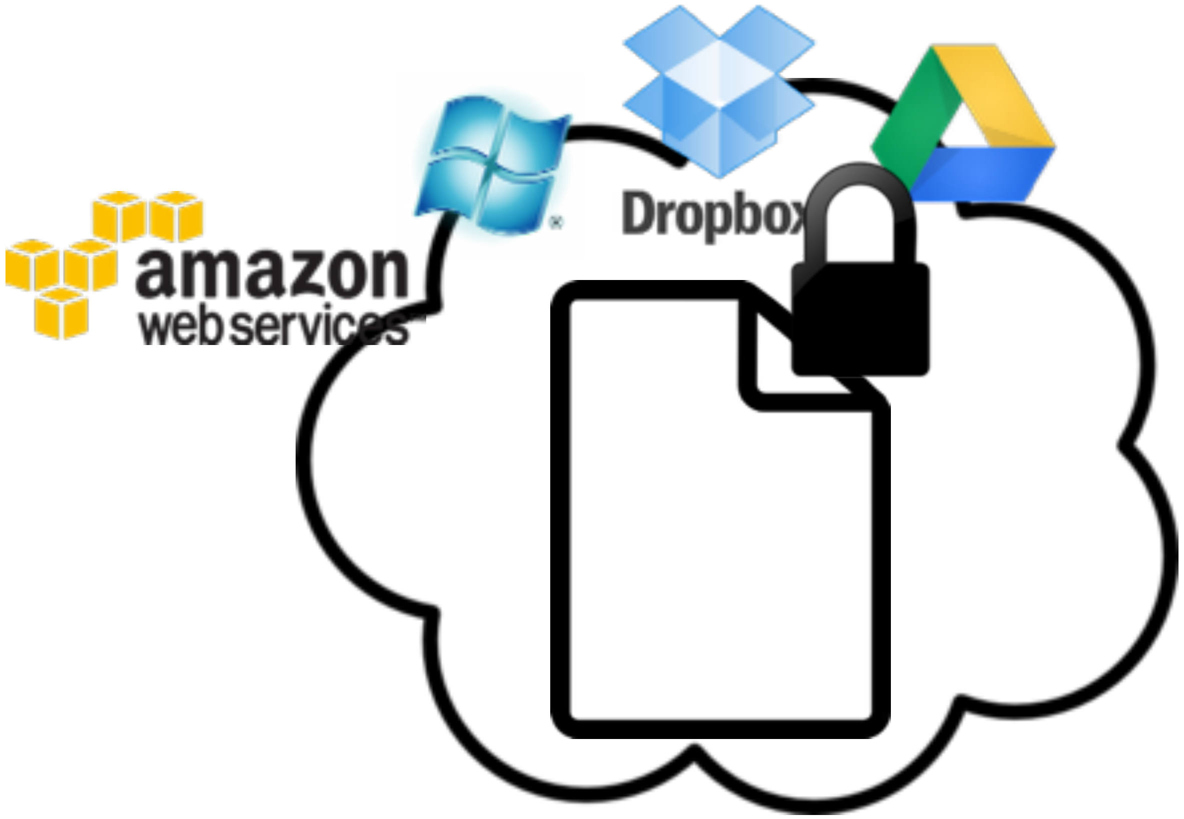
Cloud

Search with Naive Encryption?

Client

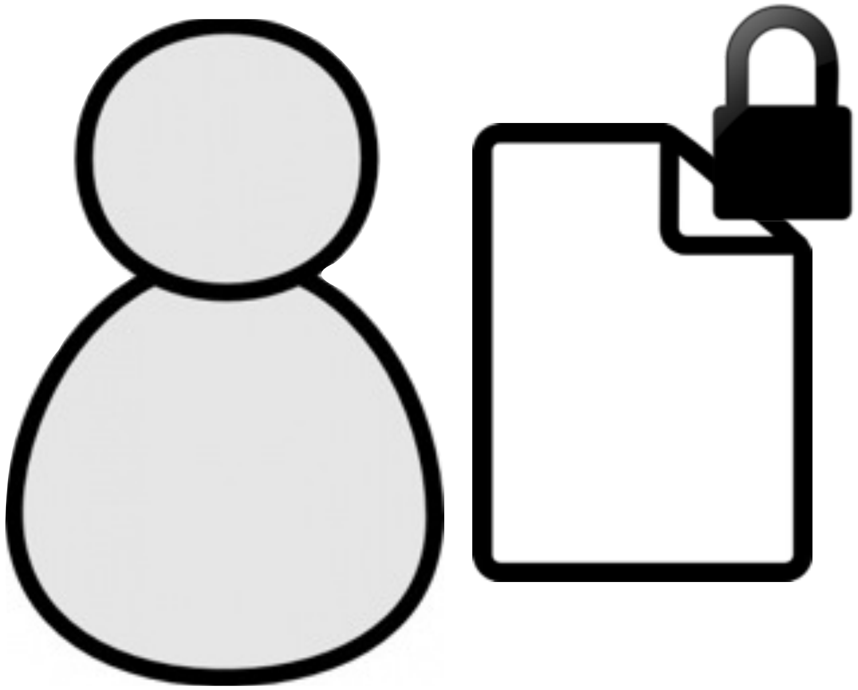


Cloud

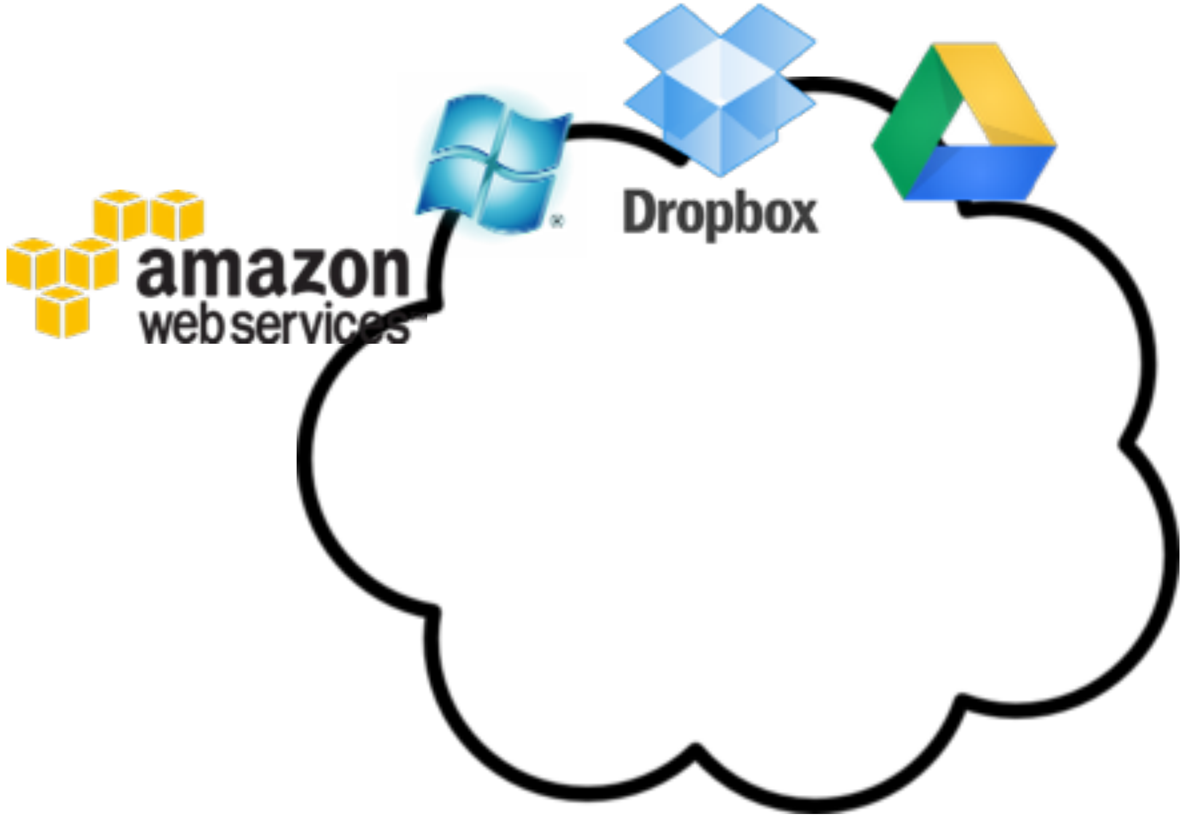


Search with Naive Encryption?

Client

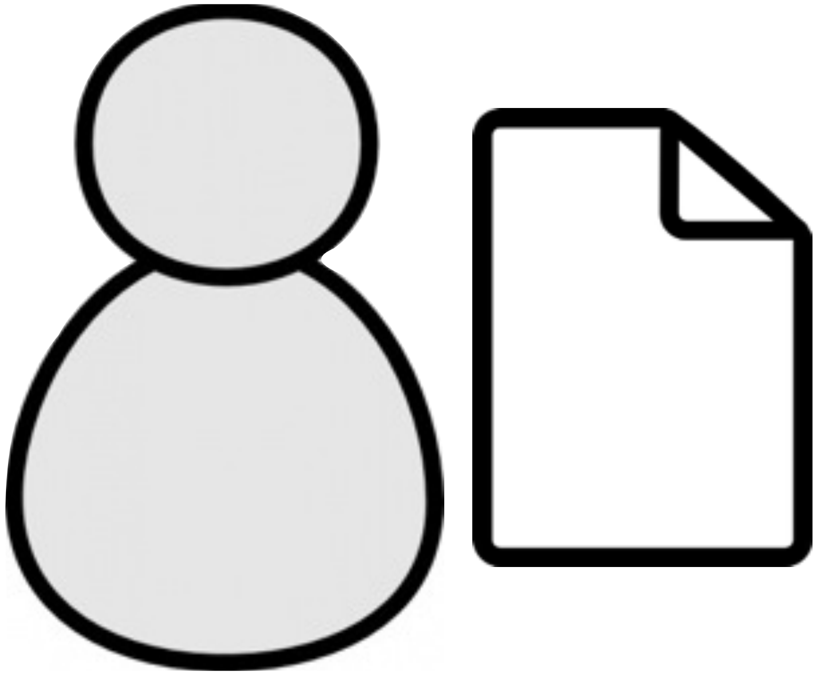


Cloud

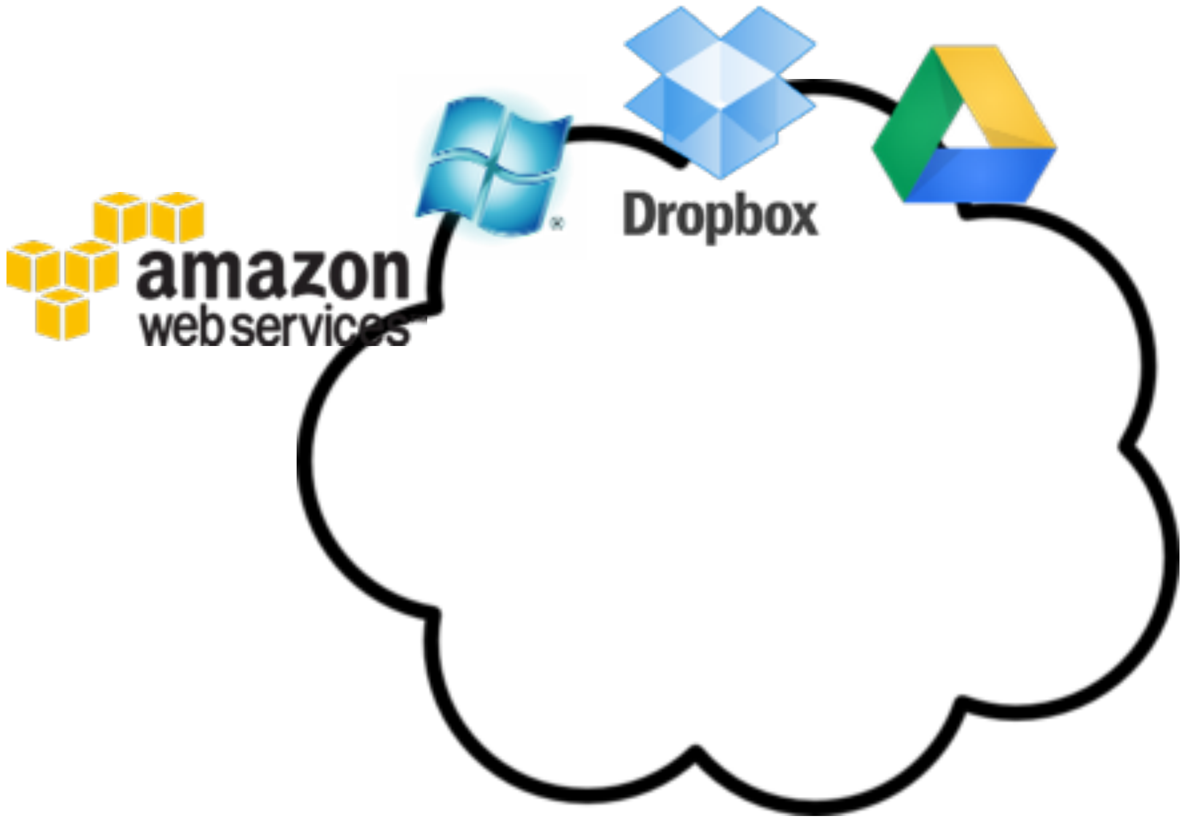


Search with Naive Encryption?

Client

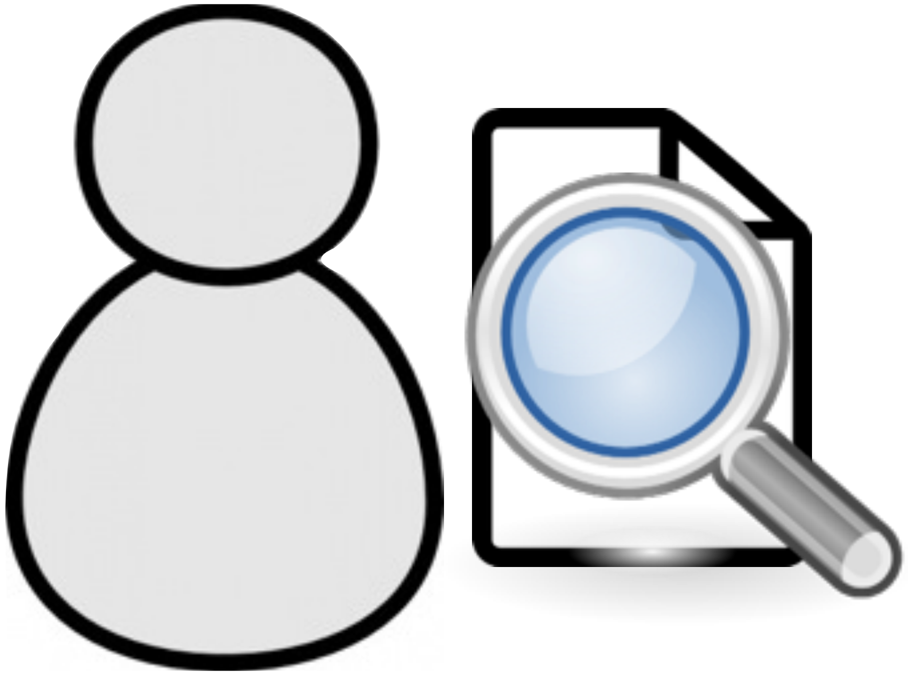


Cloud

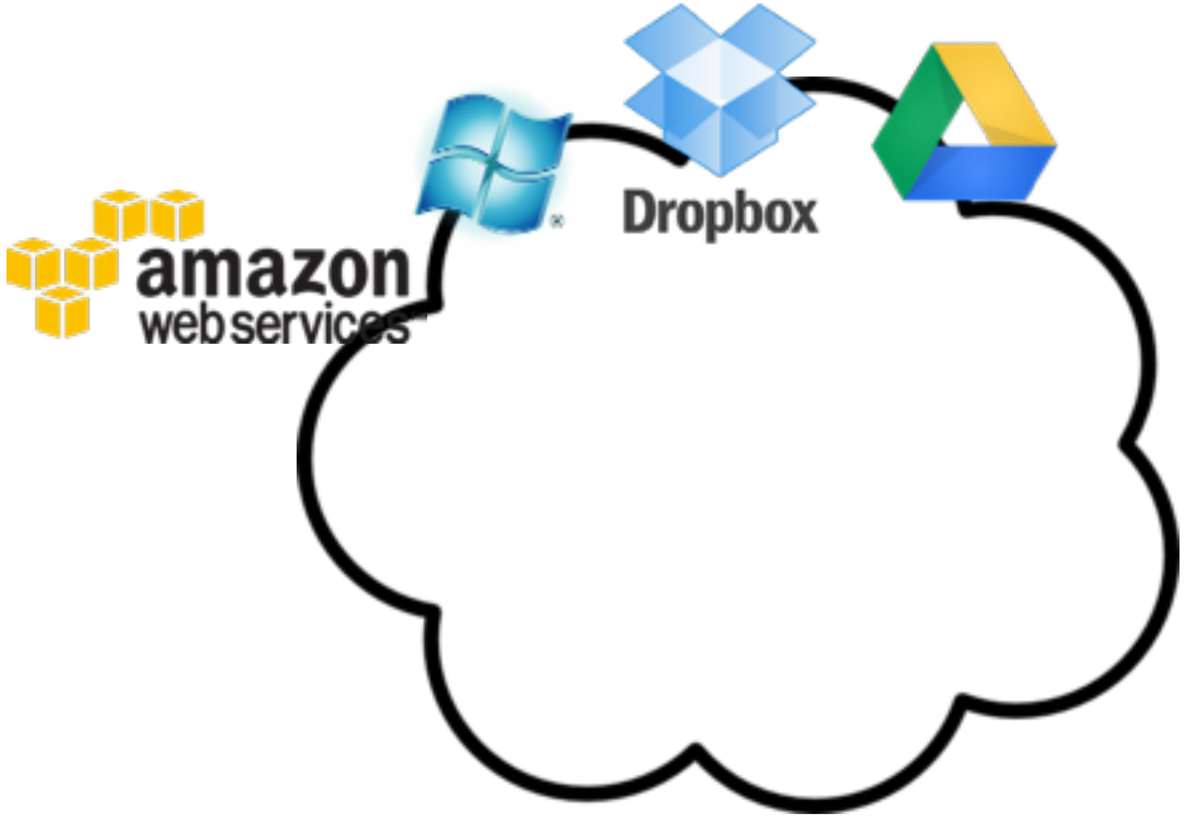


Search with Naive Encryption?

Client



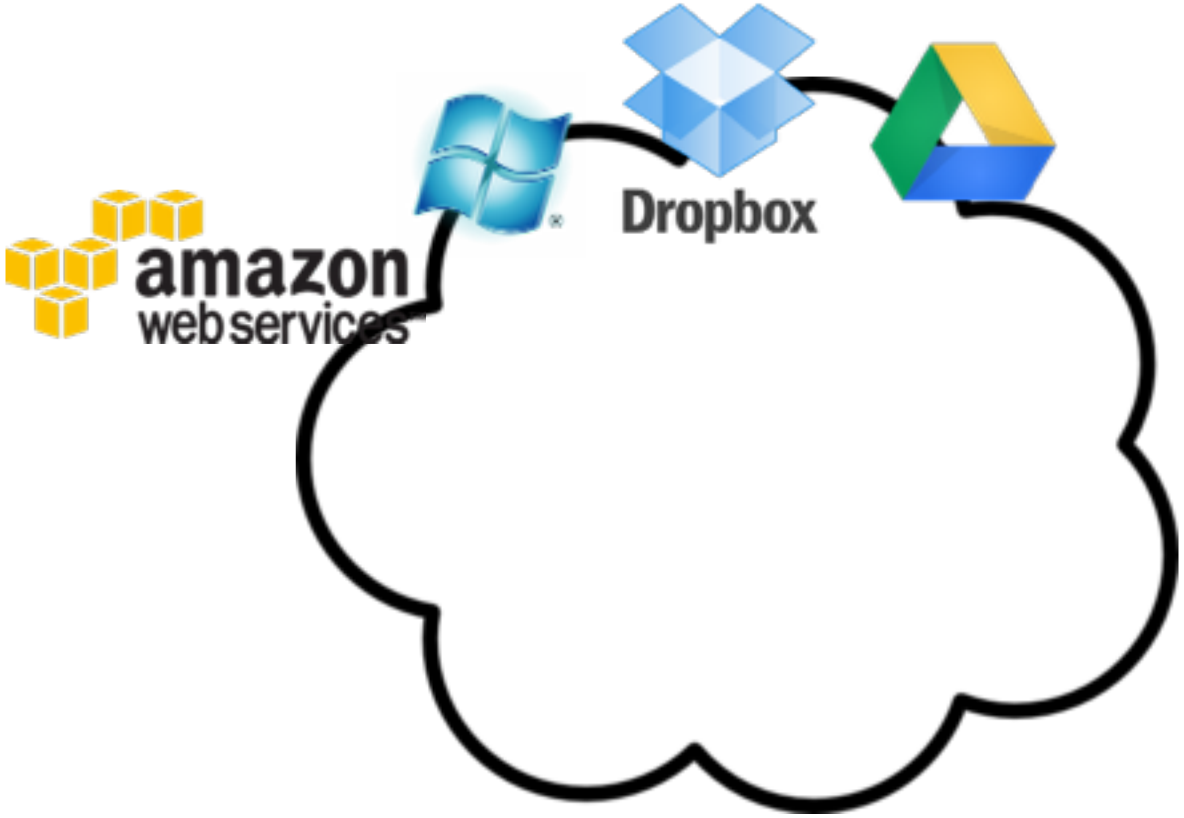
Cloud



Search with Naive Encryption?

Client

Cloud



Can we do better?

Yes!

- property-preserving encryption
- functional encryption
- fully-homomorphic encryption
- secure two-party computation
- oblivious RAMs
- searchable symmetric encryption

Taken from Seny Kamara's blog: http://outsourcedbits.org/

Searchable Encryption

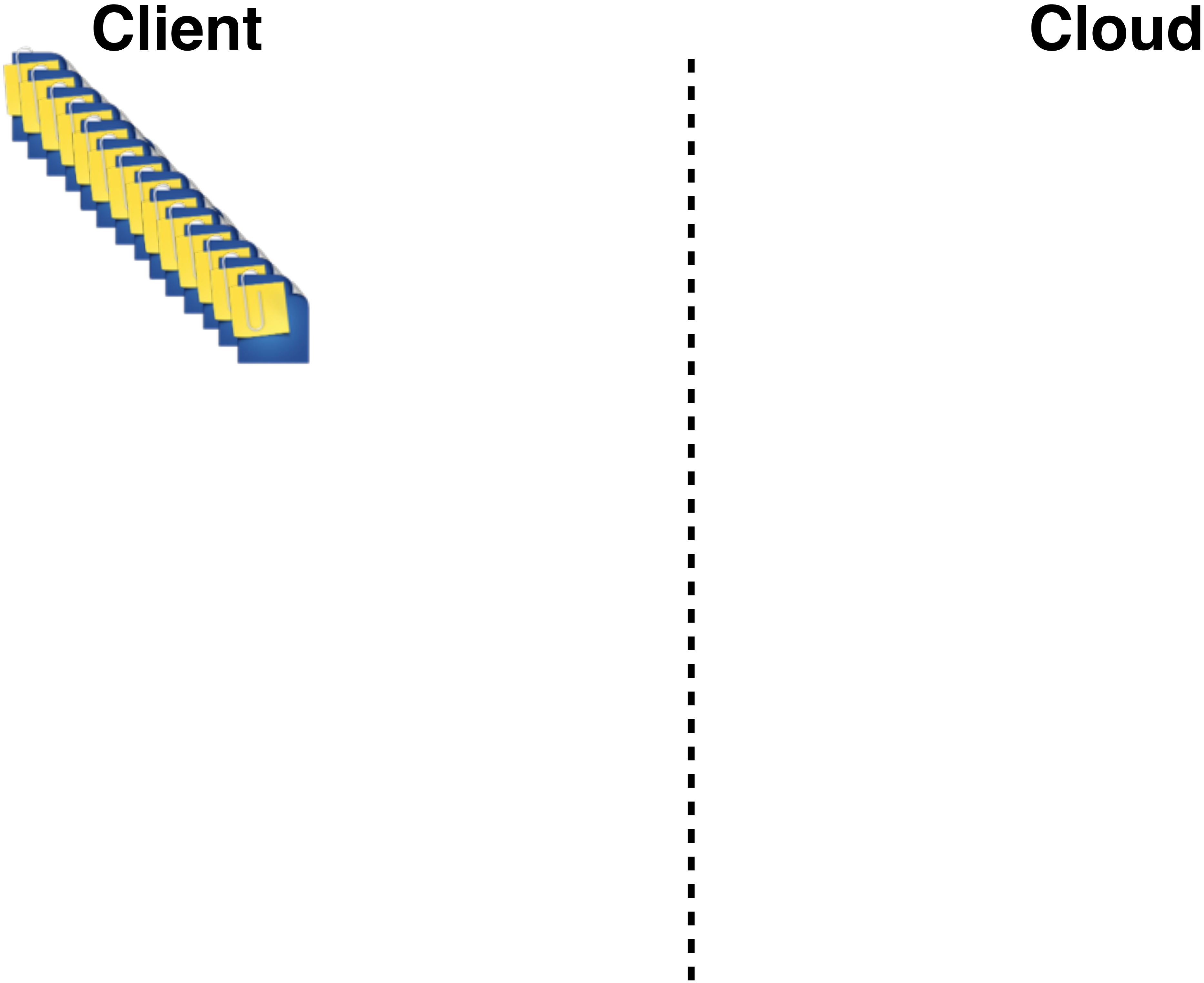
The Functionality

Setup Phase

Client

Cloud

Setup Phase

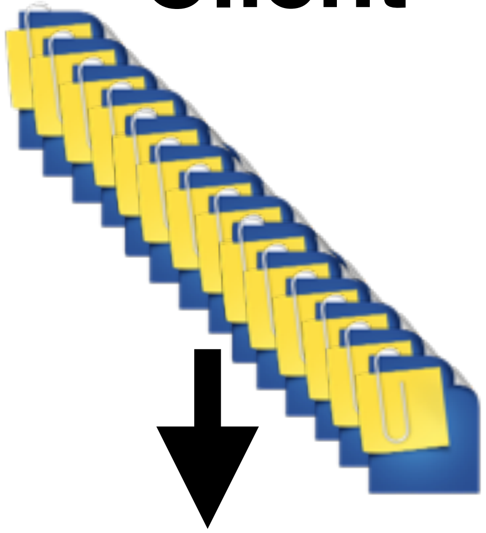


Client

Cloud

Setup Phase

Client



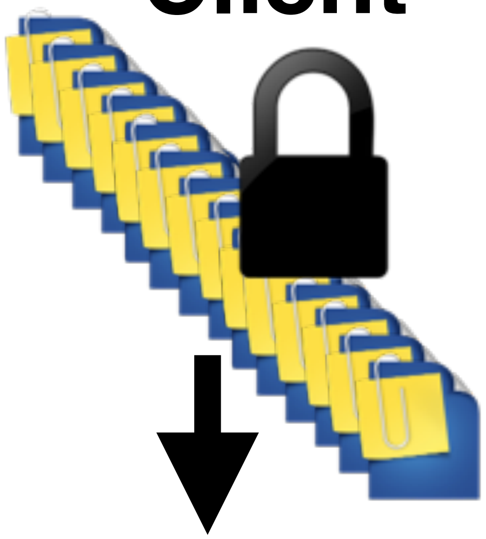
Index

word	document list
best	1, 2
illinois	3
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	3, 4
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

Cloud

Setup Phase

Client



Index

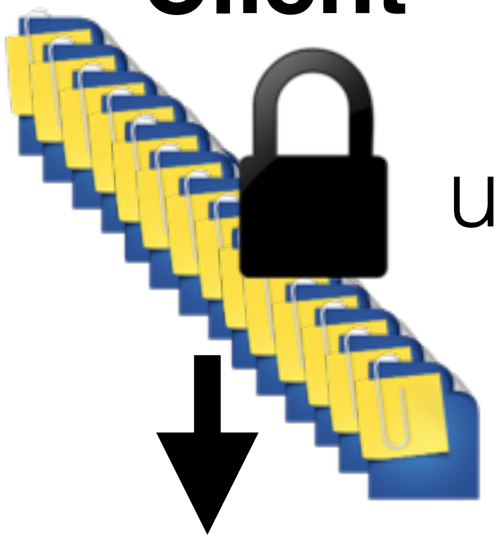
word	document list
best	1, 2
illinois	3
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	3, 4
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

Cloud

Setup Phase

Client

Cloud



using AES

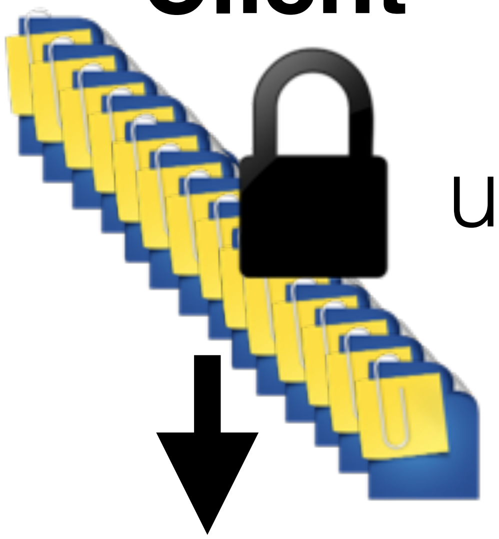
Index

word	document list
best	1, 2
illinois	3
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	3, 4
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

Setup Phase

Client

Cloud



using AES

Index

word	document list
best	1, 2
illinois	3
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	3, 4
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

using SSE

Setup Phase

Client

Index

word	document list
best	1, 2
illinois	3
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	3, 4
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

using SSE

Cloud

Setup Phase

Client

Cloud

Index

word	document lis
best	1, 2
illinois	3
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	3, 4
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

Online Phase

Client

Cloud

Index

word	document list
illinois	1, 3
best	2
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	1, 3, 4, 8
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

Online Phase

Client

Search for the keyword “illinois”

Cloud

Index

word	document list
illinois	1, 3
best	2
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	1, 3, 4, 8
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

Online Phase

Client

illinois

Search for the keyword “illinois”

Cloud

Index

word	document list
illinois	1, 3
best	2
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	1, 3, 4, 8
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

Online Phase

Client

Search for the keyword
“illinois”

Cloud

illinois

Index

word	document list
illinois	1, 3
best	2
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	1, 3, 4, 8
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

Online Phase

Client

Search for the keyword "illinois"

Cloud

Index

word	document list
illinois	1, 3
best	2
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	1, 3, 4, 8
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

Online Phase

Client

Cloud

1

3

illinois

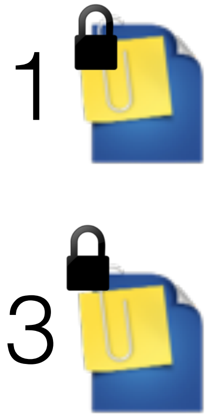
Index

word	document list
illinois	1, 3
best	2
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	1, 3, 4, 8
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

Search for the keyword “illinois”

Online Phase

Client



Search for the keyword “illinois”

Cloud

illinois

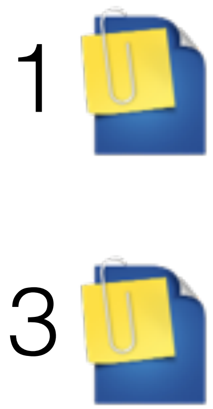
Index

word	document list
illinois	1, 3
best	2
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	1, 3, 4, 8
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

Online Phase

Client

Cloud



Index

word	document list
illinois	1, 3
best	2
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	1, 3, 4, 8
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

illinois

Search for the keyword
"illinois"

Online Phase

Client

Search for the keyword
“illinois”

Cloud

Index

word	document list
illinois	1, 3
best	2
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	1, 3, 4, 8
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

illinois

Online Phase

Client

Cloud

Index

word	document list
illinois	1, 3
best	2
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	1, 3, 4, 8
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

Online Phase

Client

Add document

100

Cloud

Index

word	document list
illinois	1, 3
best	2
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	1, 3, 4, 8
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

Online Phase

Client

Add document

100 illinois, blue

Cloud

Index

word	document list
illinois	1, 3
best	2
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	1, 3, 4, 8
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

Online Phase

Client

Add document

100

illinois, blue

Cloud

Index

word	document list
illinois	1, 3
best	2
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	1, 3, 4, 8
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

Online Phase

Client

Add document

100 illinois, blue

Cloud

Index

word	document list
illinois	1, 3
best	2
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	1, 3, 4, 8
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

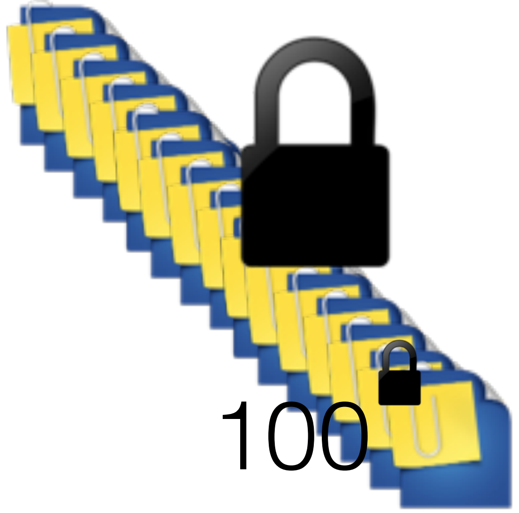
Online Phase

Client

Add document

illinois, blue

Cloud



Index

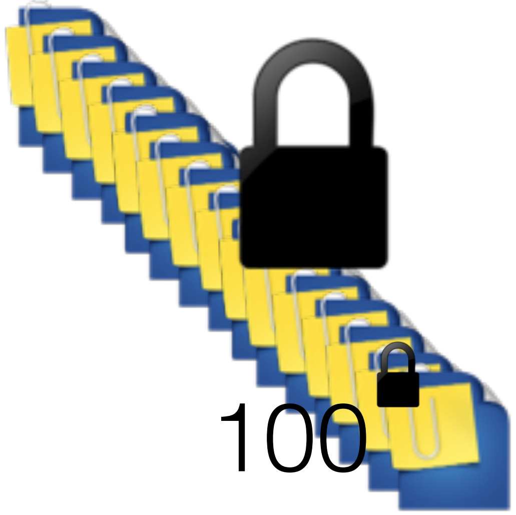
word	document list
illinois	1, 3
best	2
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	1, 3, 4, 8
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

Online Phase

Client

Add document

Cloud



Index

word	document list
illinois	1, 3
best	2
microsoft	1, 4, 5
america	6, 7, 1
	1, 3, 4, 8
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

naveed2@illinois.edu

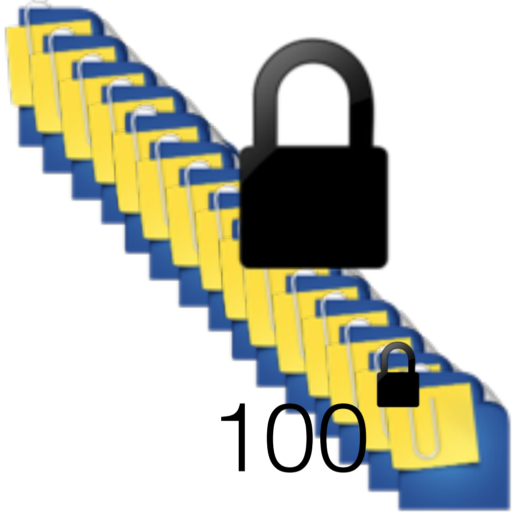
illinois, blue

Online Phase

Client

Add document

Cloud



Update Index

word	document list
illinois	1, 3, ***100***
best	2
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	1, 3, 4, 8
blue	1, ***100***
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

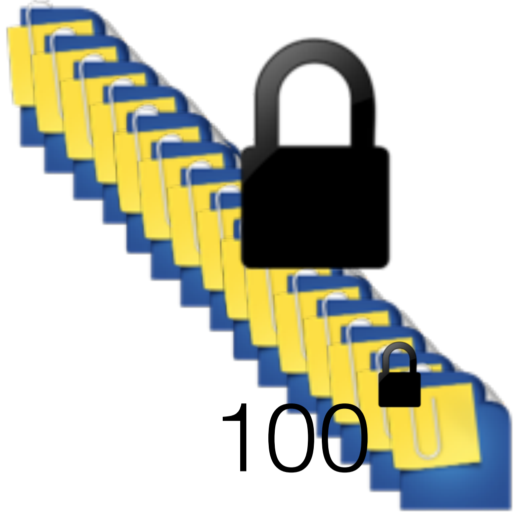
Online Phase

Client

Add document

Same procedure for delete

Cloud

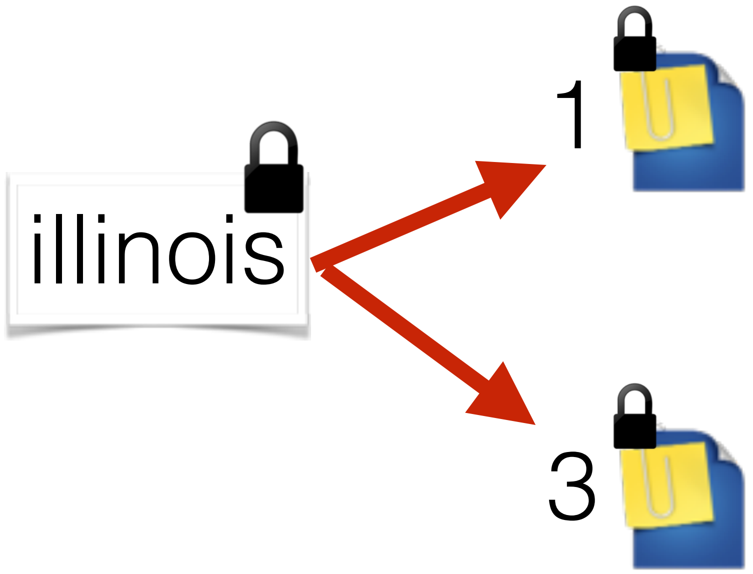


Update Index

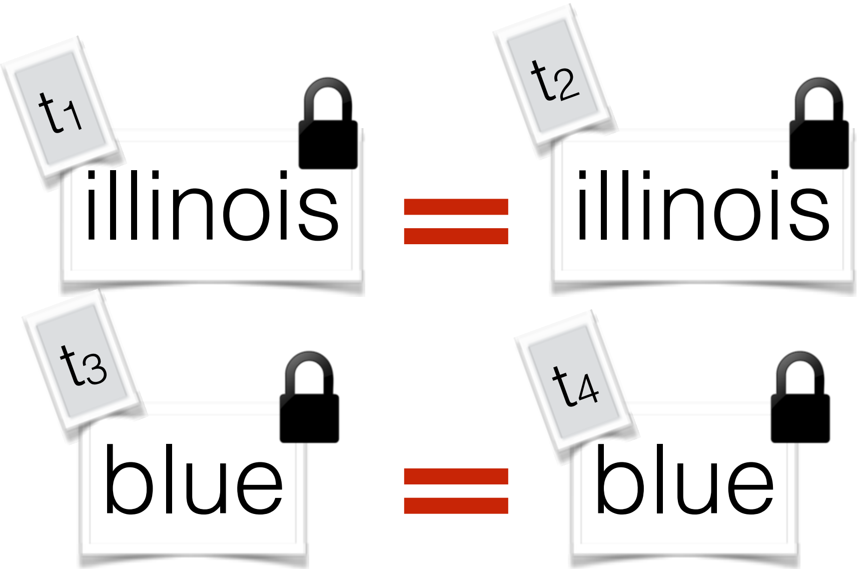
word	document list
illinois	1, 3, ***100***
best	2
microsoft	1, 4, 5
america	6, 7, 1
naveed2@illinois.edu	1, 3, 4, 8
blue	1, ***100***
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6,

Leakage

Access Pattern

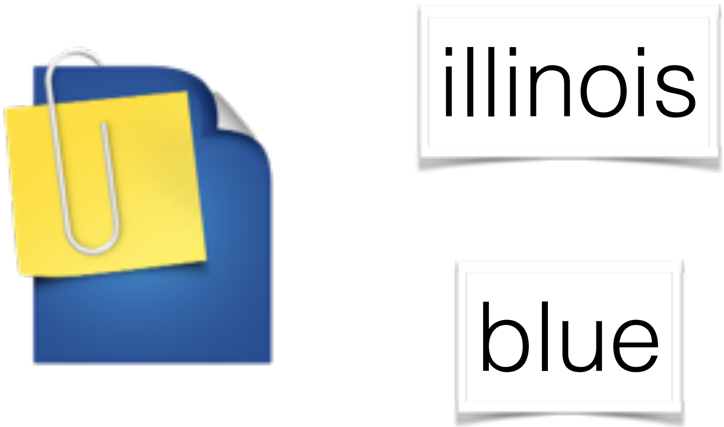


Search Pattern



Additional Add/Delete Leakage

- Hashes of all the keywords in the newly added document

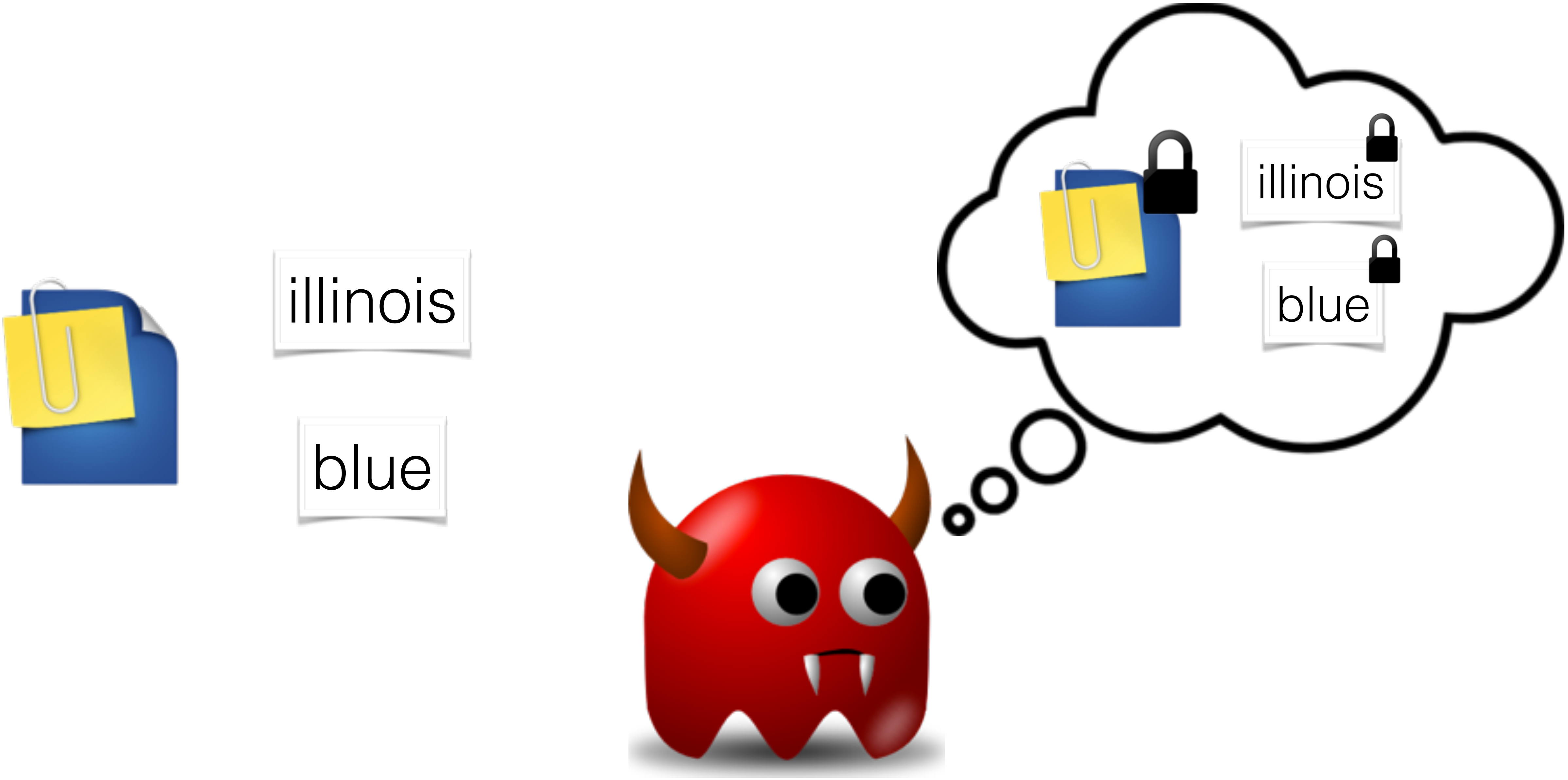


illinois

blue

Additional Add/Delete Leakage

- Hashes of all the keywords in the newly added document



illinois

blue

illinois

blue

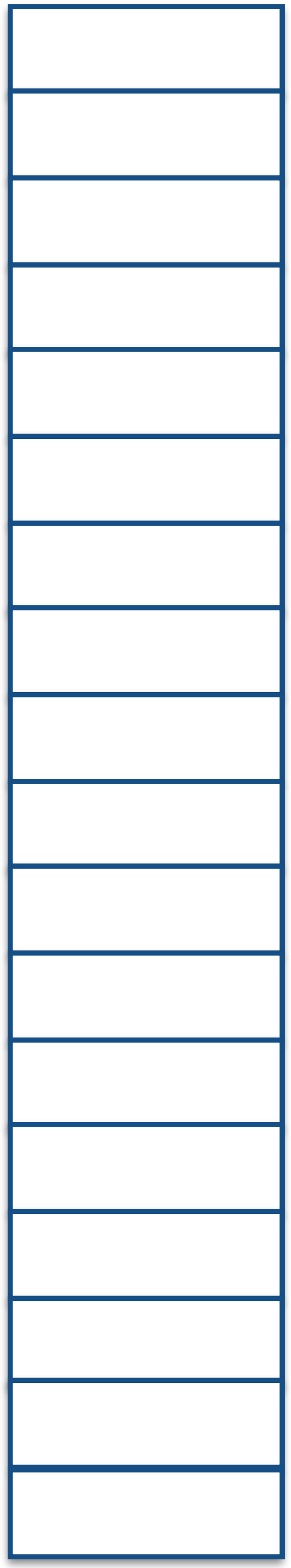
Security Definitions

- Non-adaptive Security
  - All queries are generated in a single batch
- Adaptive Security
  - Queries can be generated as a function of previous search results

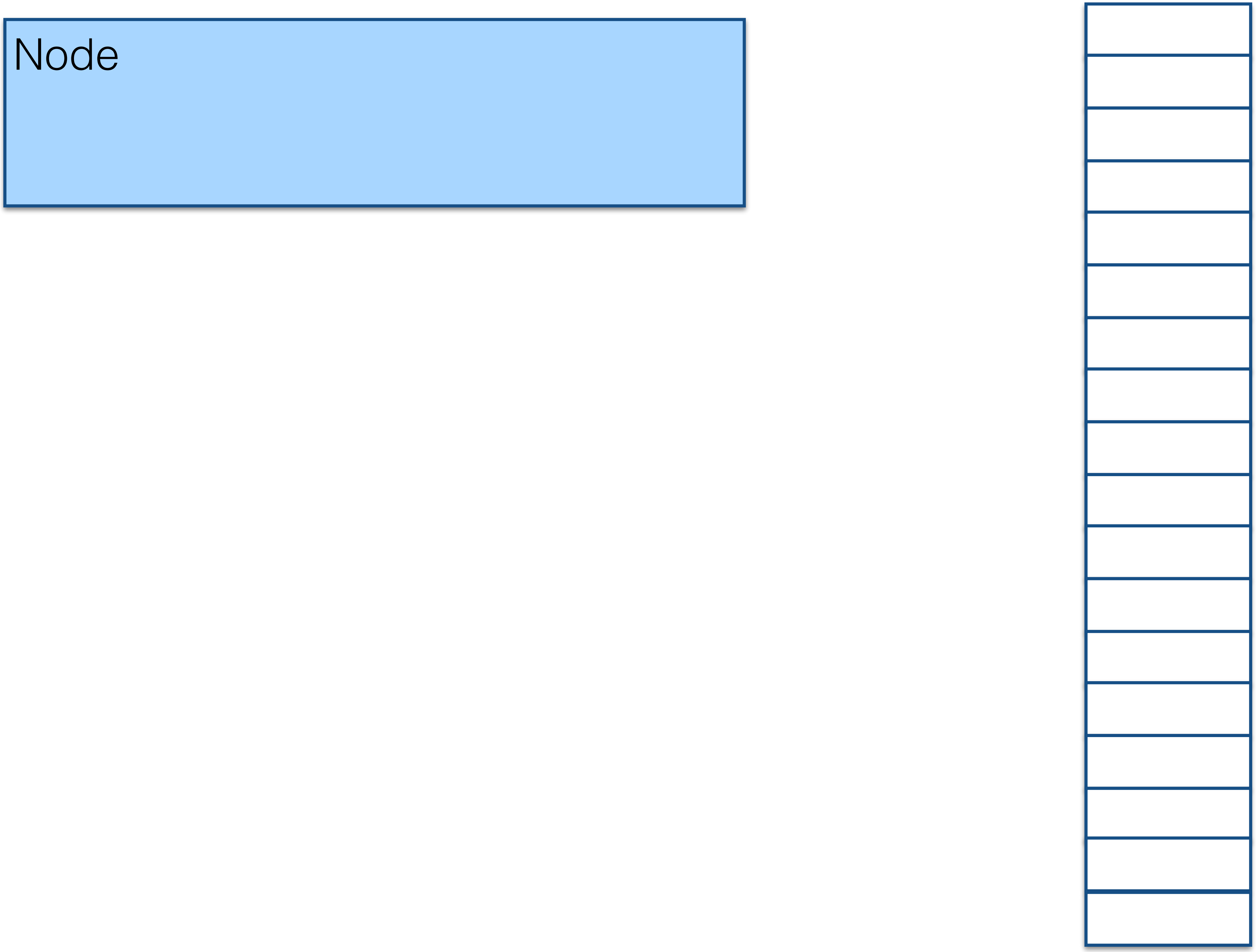
Previous Work

- Schemes supporting single-keyword queries
    - Song-Wagner-Perring00, Goh03, Chang-Mitzenmacher05, Curtmola-Garay-Kamara-Ostrovsky2006, Kurosawa-Ohtaki12, Chase-Kamara10, Liesdonk-Sedghi-Doumen-Hartel-Jonker10, Kamara-Papamanthou-Roeder12, Kamara-Papamanthou13, Stefanov-Papamanthou-Shi14, Cash-Jaeger-Jarecki-Jutla-Krawczyk-Rosu-Steiner14
- Schemes supporting conjunctive/boolean queries
    - Cash-Jarecki-Jutla-Krawczyk-Rosu-Steiner13, Jarecki-Jutla-Krawczyk-Rosu-Steiner13,
- All require computation on the server side
- Some schemes are not parallelizable
- Non-standard leakage or more leakage during updates

Linked-list based Schemes

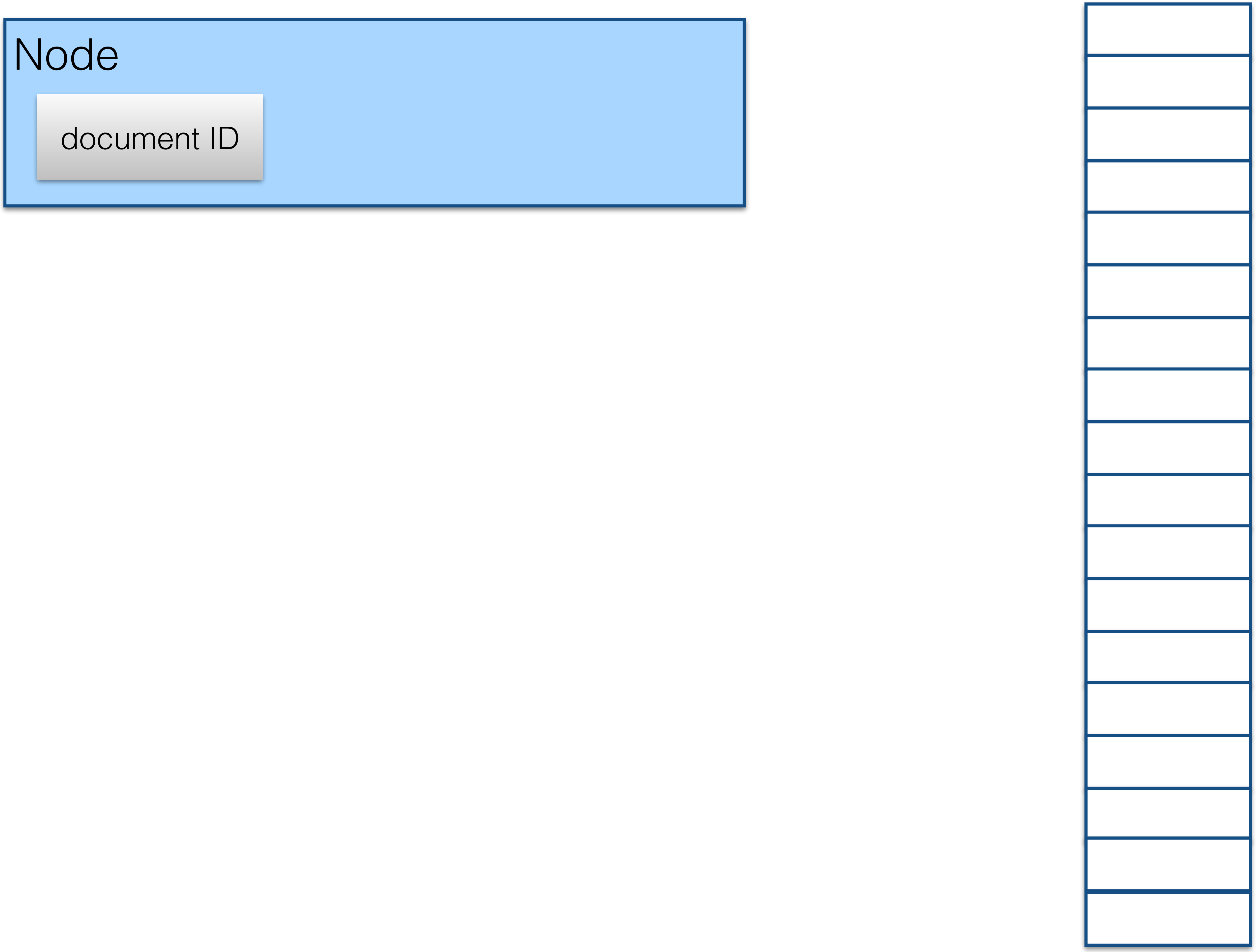


Linked-list based Schemes



Node

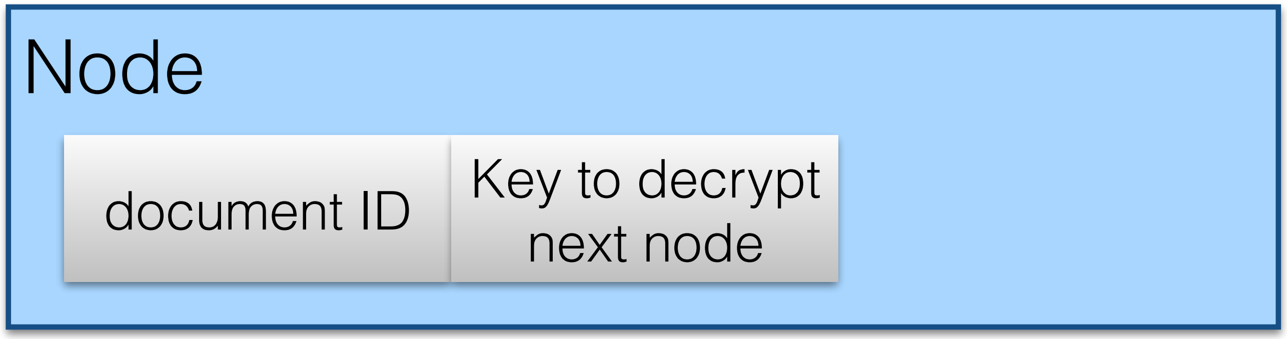
Linked-list based Schemes



Node

document ID

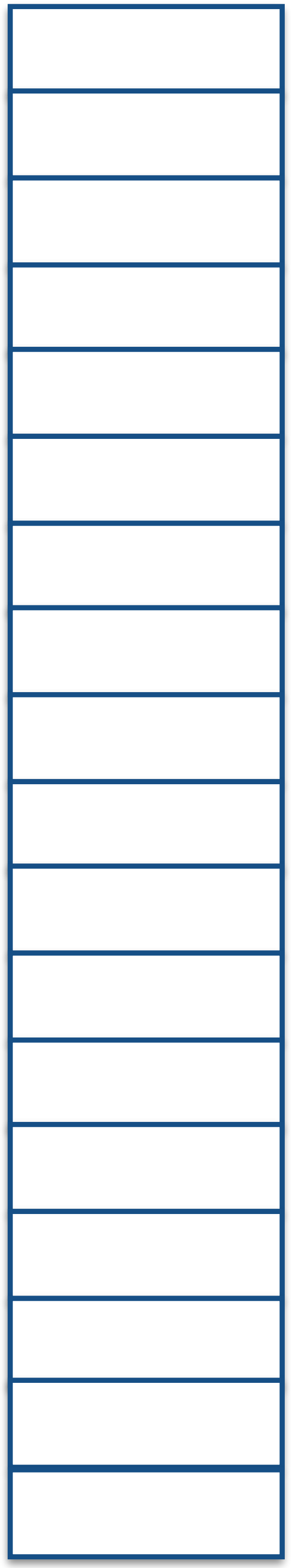
Linked-list based Schemes



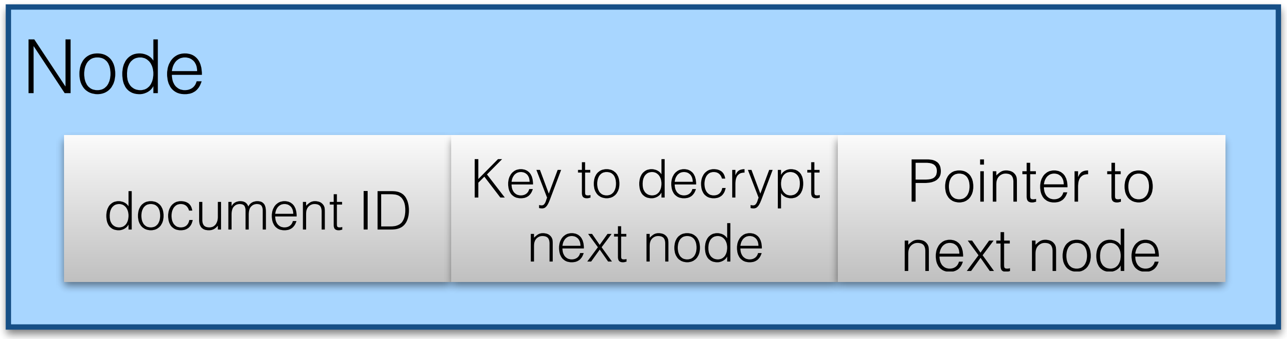
Node

document ID

Key to decrypt next node



Linked-list based Schemes

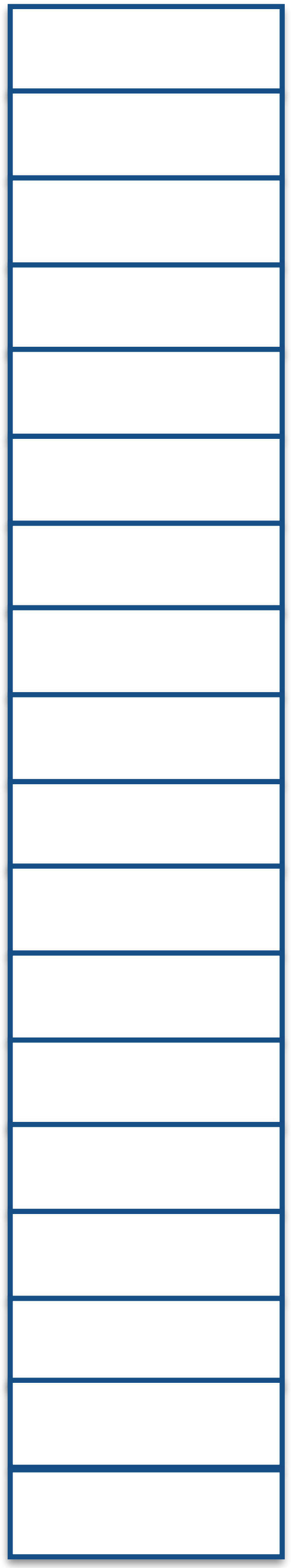


Node

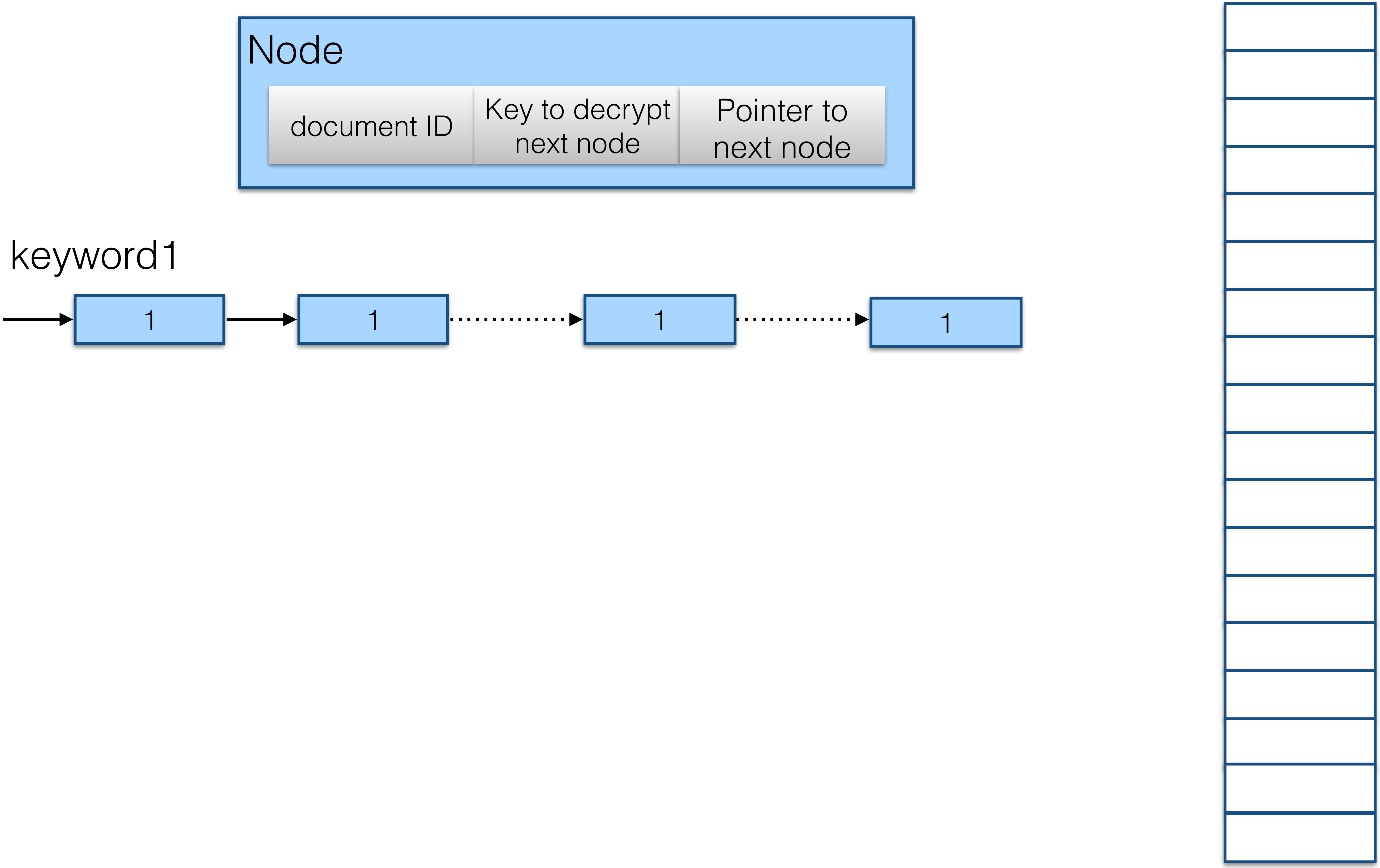
document ID

Key to decrypt next node

Pointer to next node



Linked-list based Schemes



Node

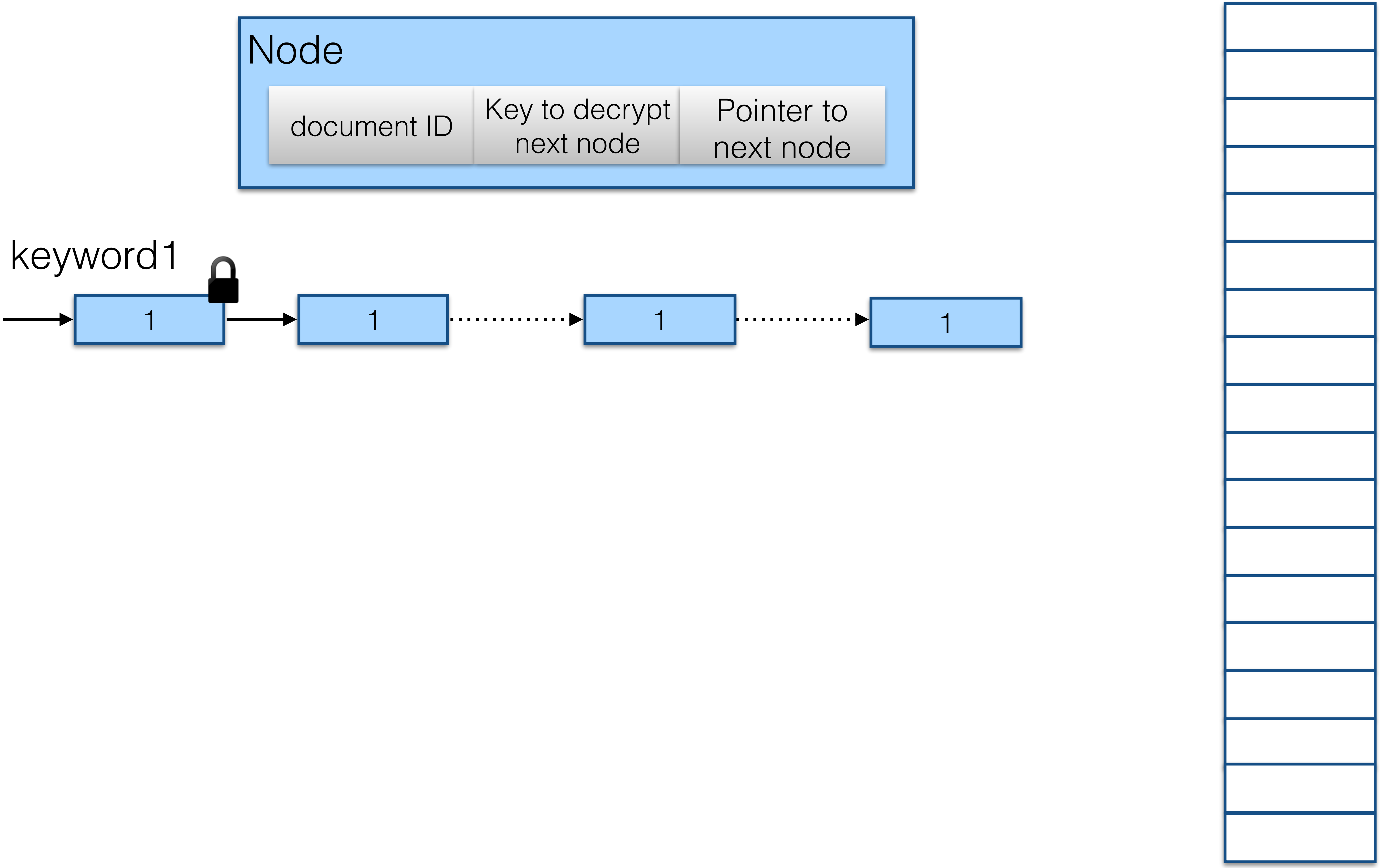
document ID

Key to decrypt next node

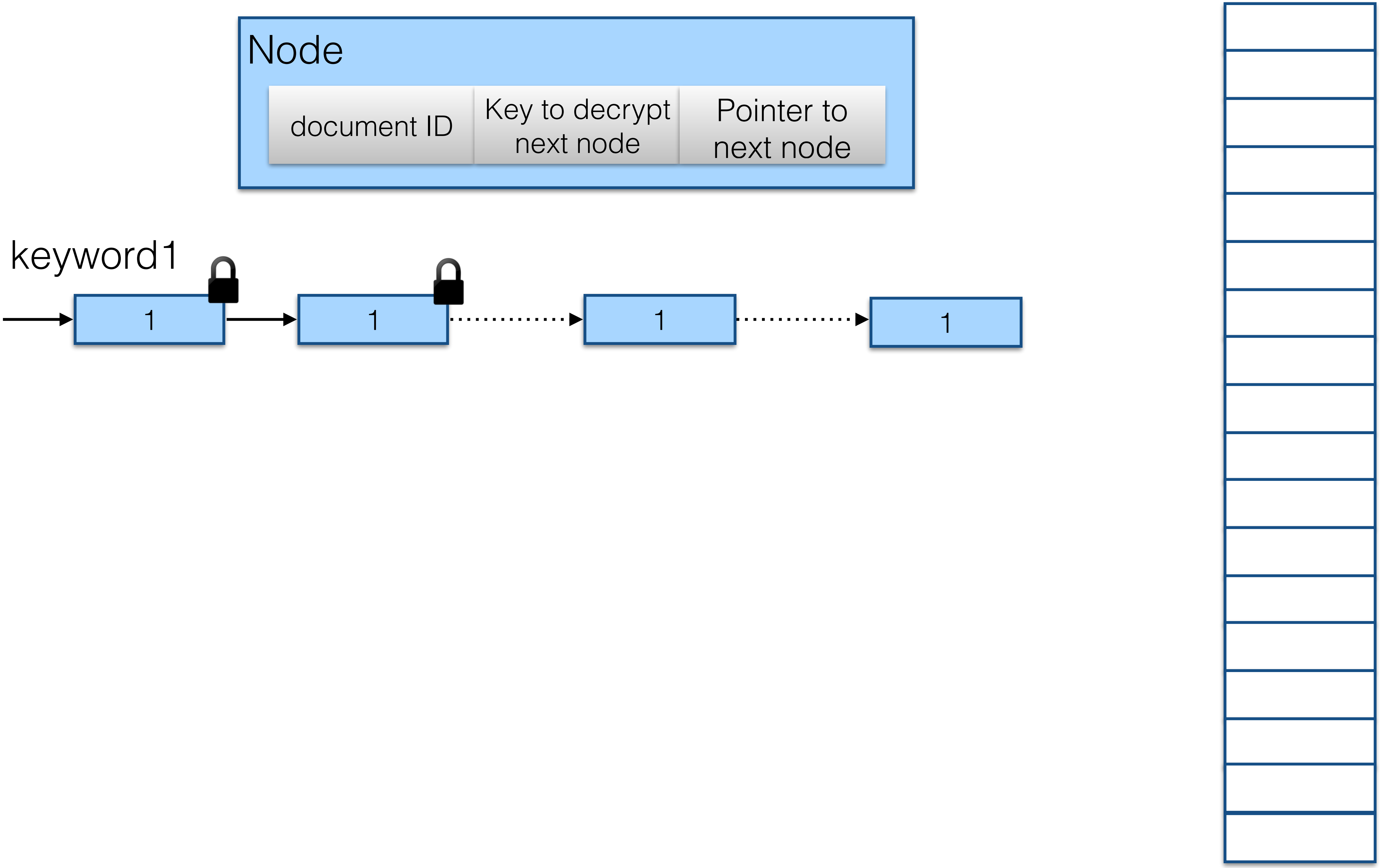
Pointer to next node

keyword1

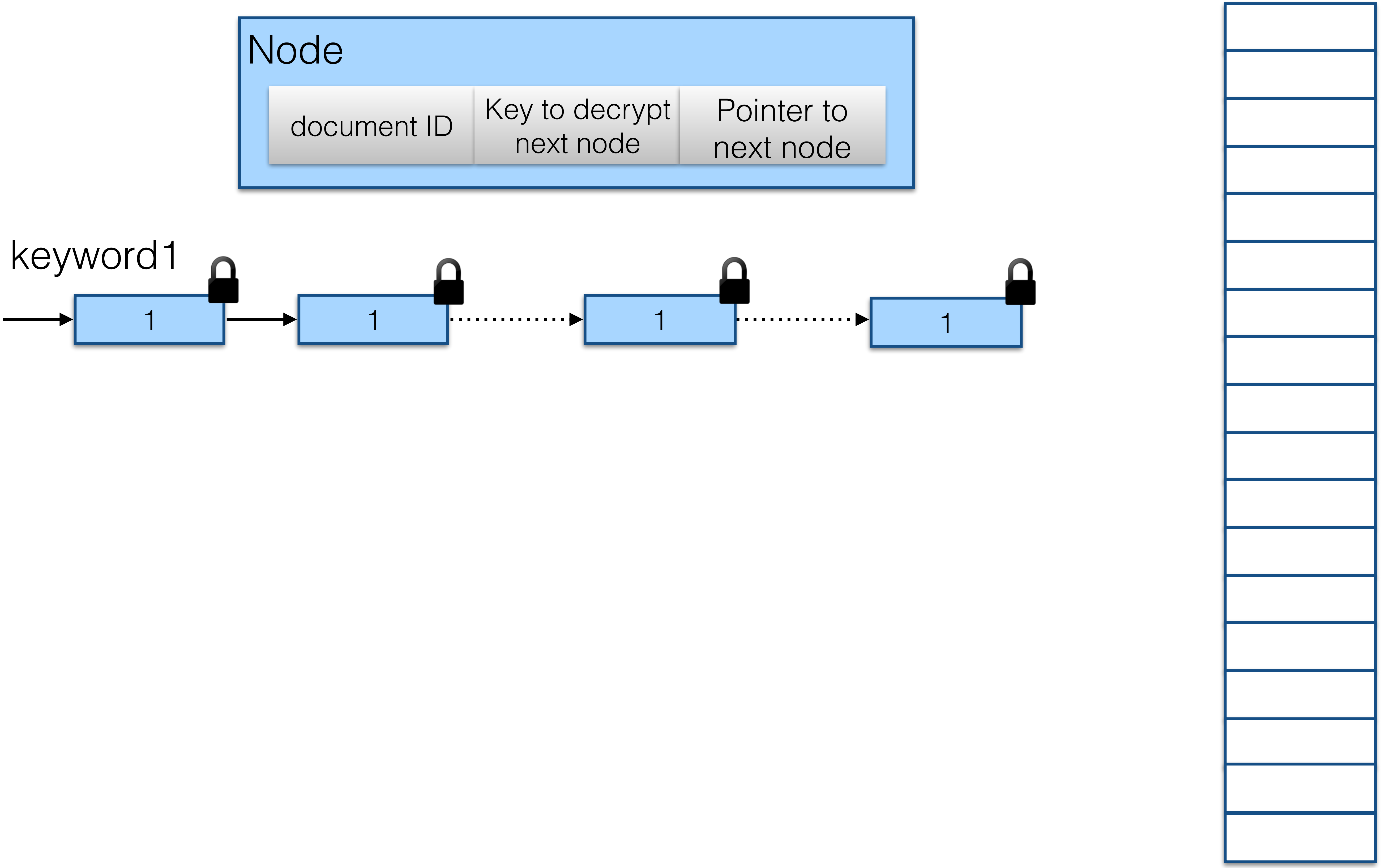
Linked-list based Schemes



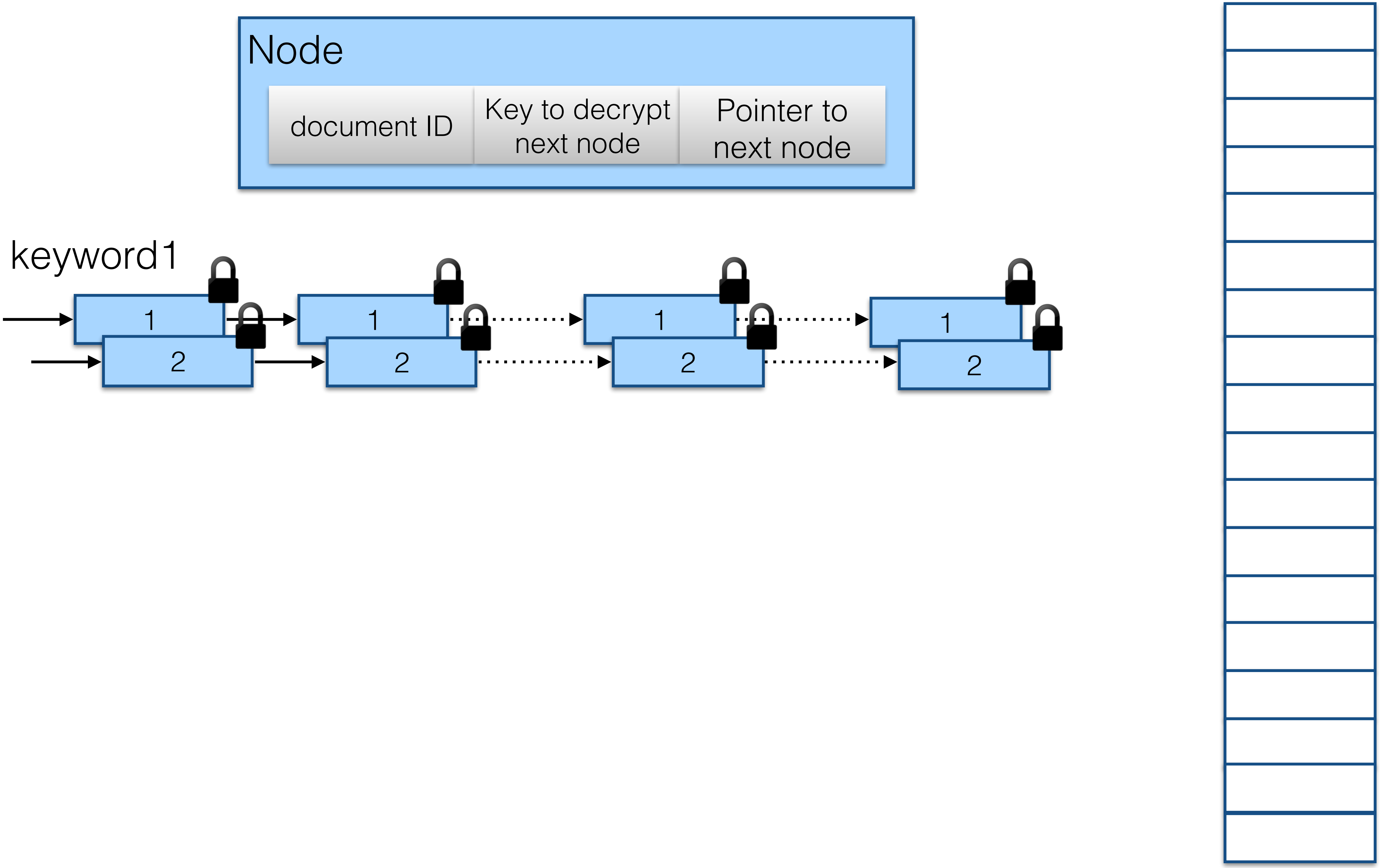
Linked-list based Schemes



Linked-list based Schemes



Linked-list based Schemes



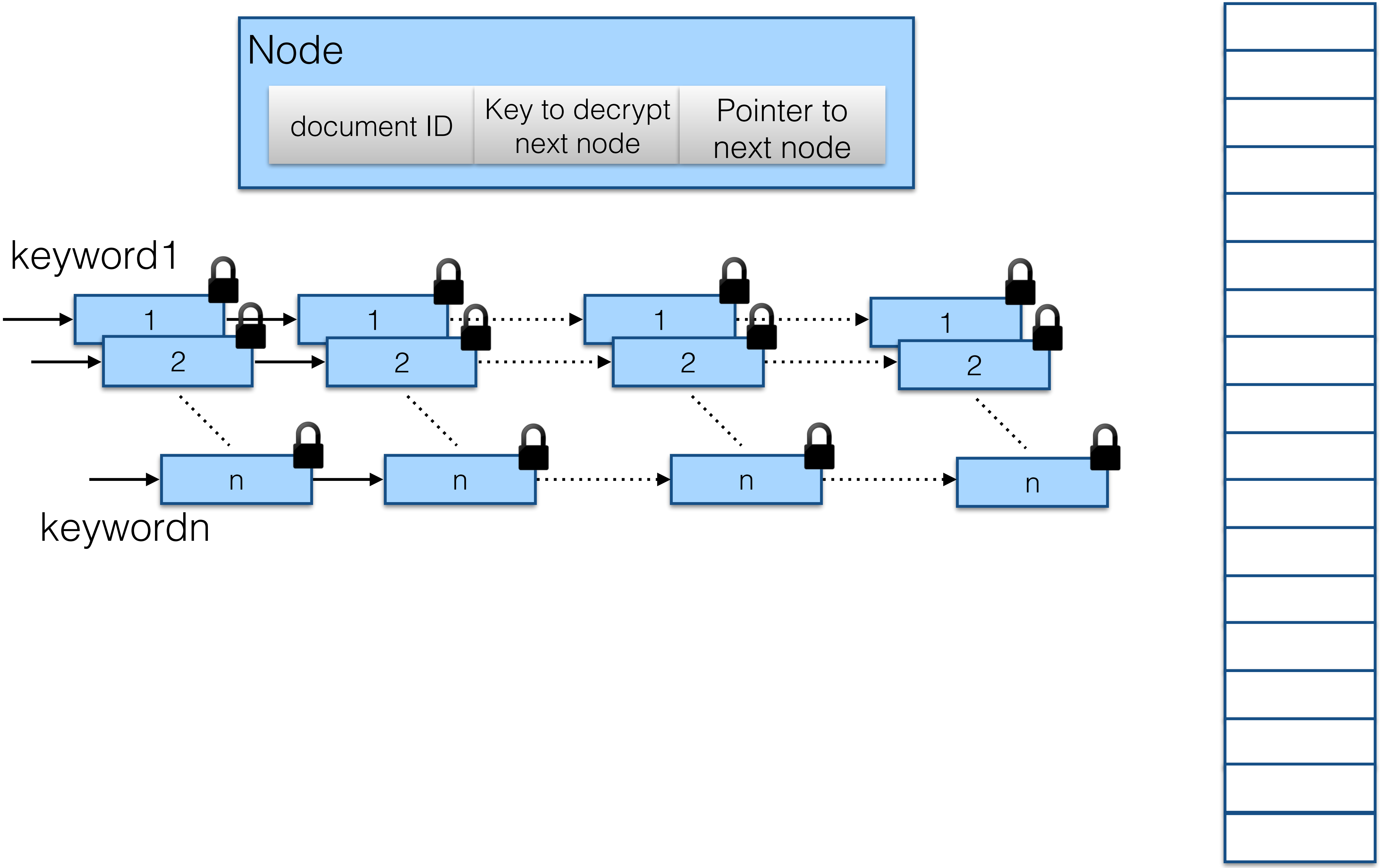
Node

document ID

Key to decrypt next node

Pointer to next node

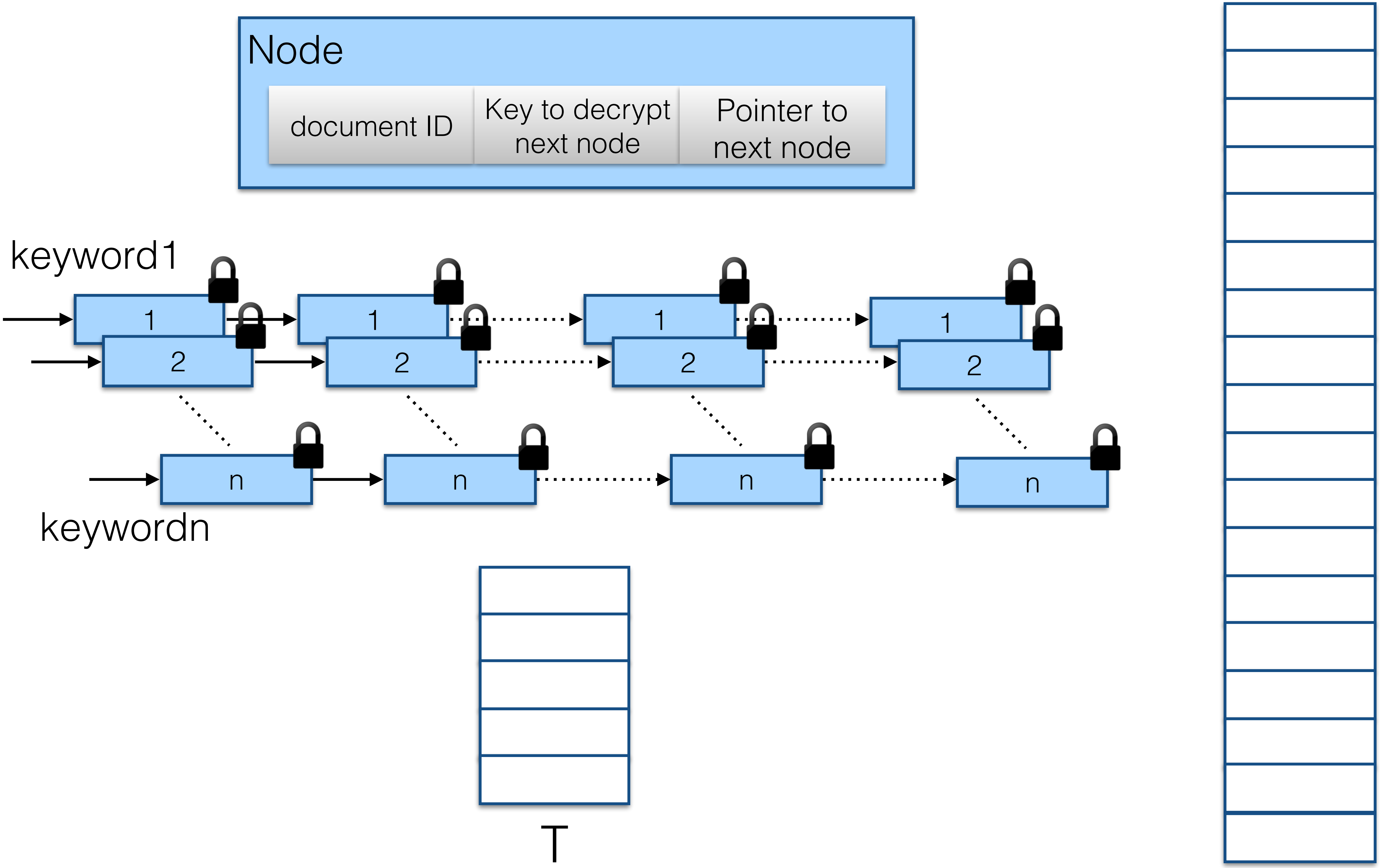
Linked-list based Schemes



Node

document ID | Key to decrypt next node | Pointer to next node

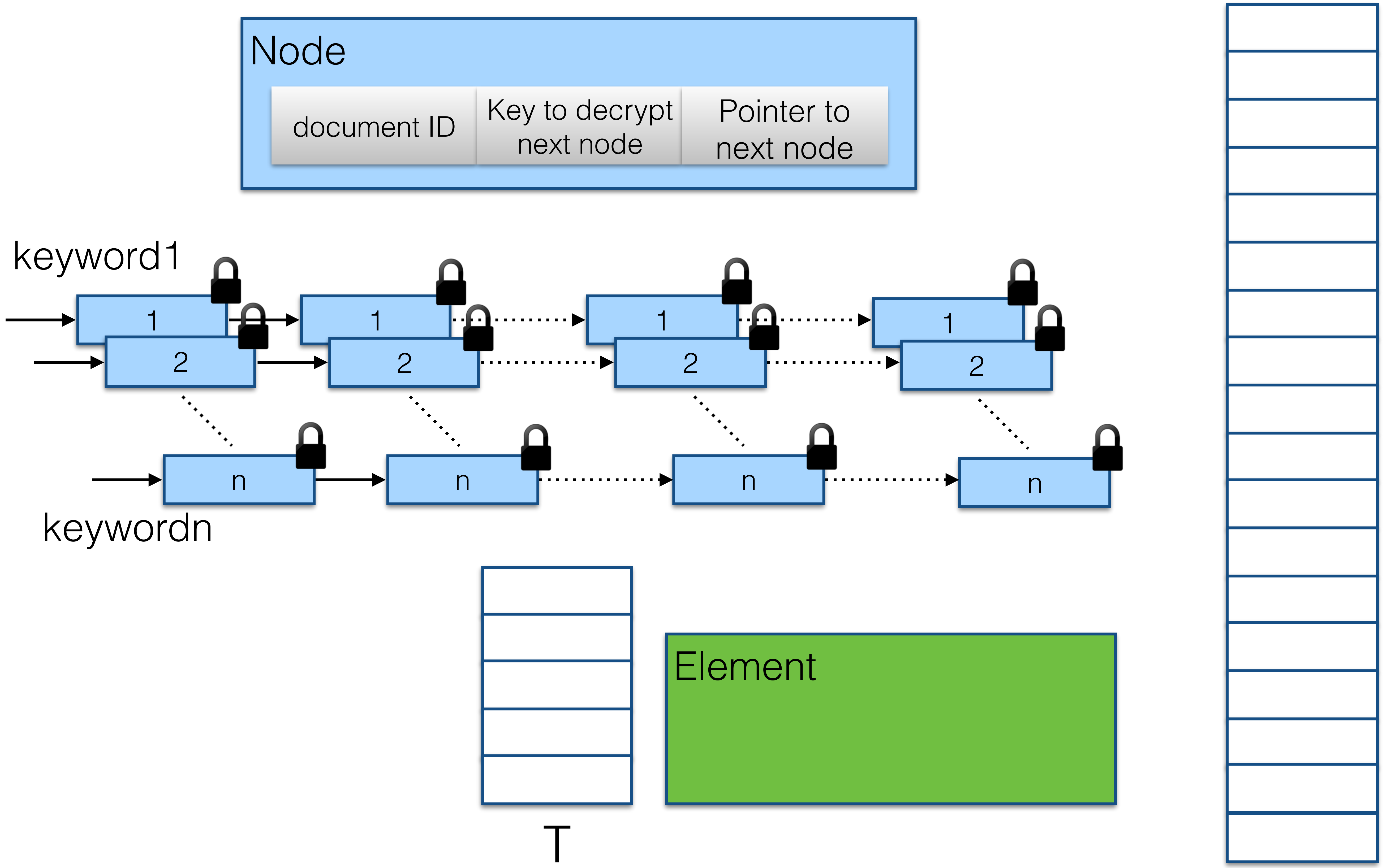
Linked-list based Schemes



Node

document ID | Key to decrypt next node | Pointer to next node

Linked-list based Schemes



Node

document ID

Key to decrypt next node

Pointer to next node

keyword1

1

2

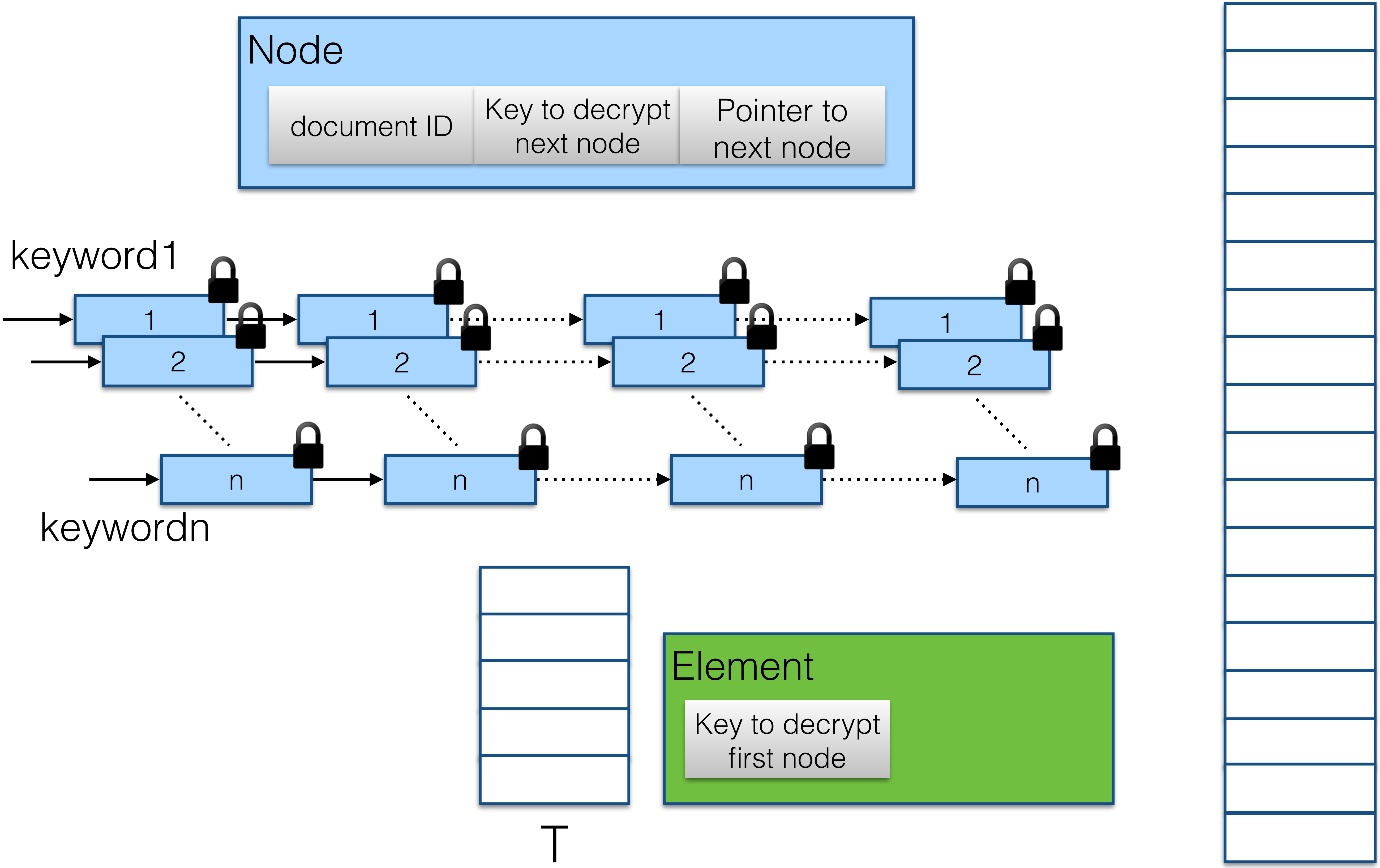
n

keywordn

T

Element

Linked-list based Schemes



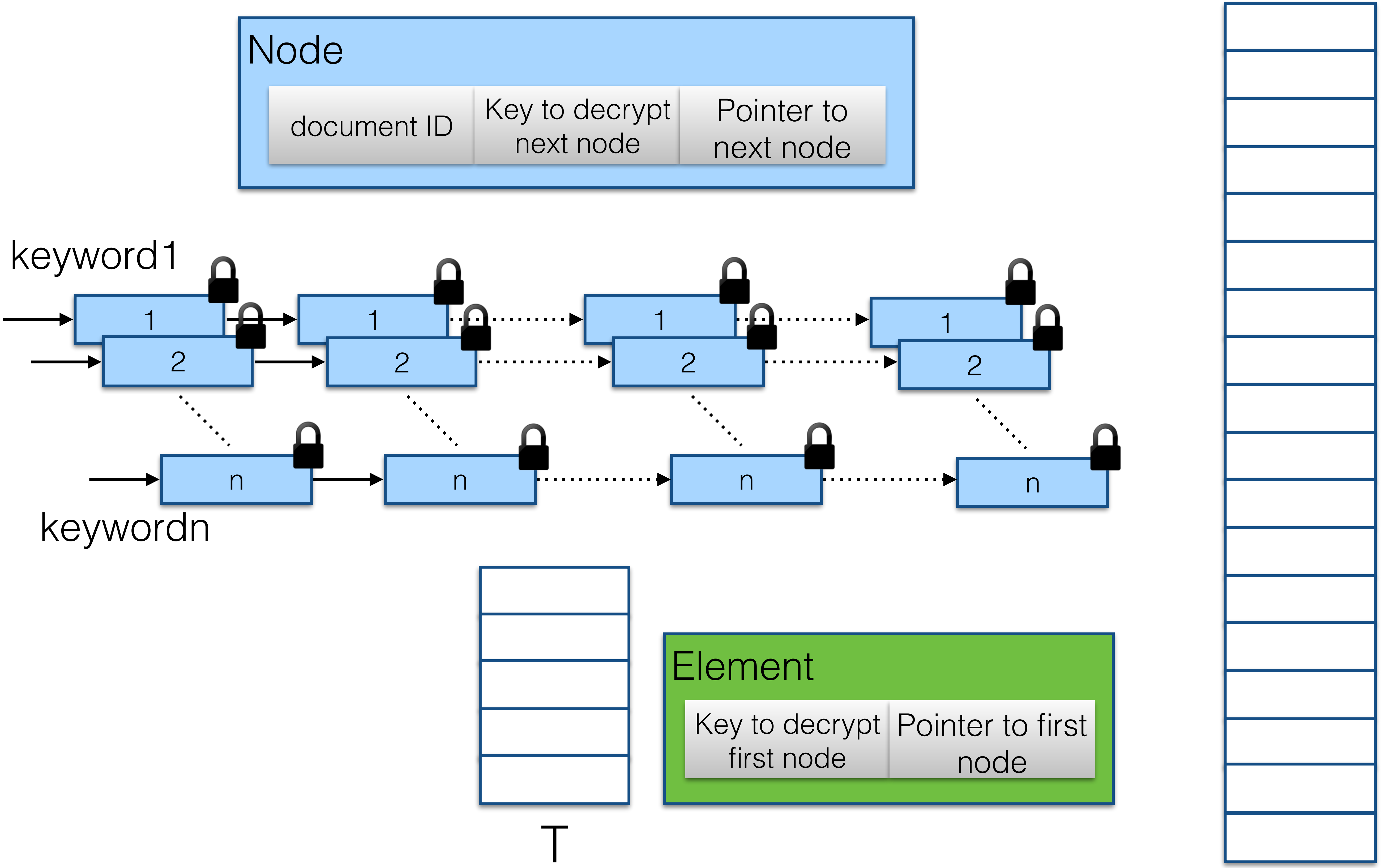
Node

document ID | Key to decrypt next node | Pointer to next node

Element

Key to decrypt first node

Linked-list based Schemes



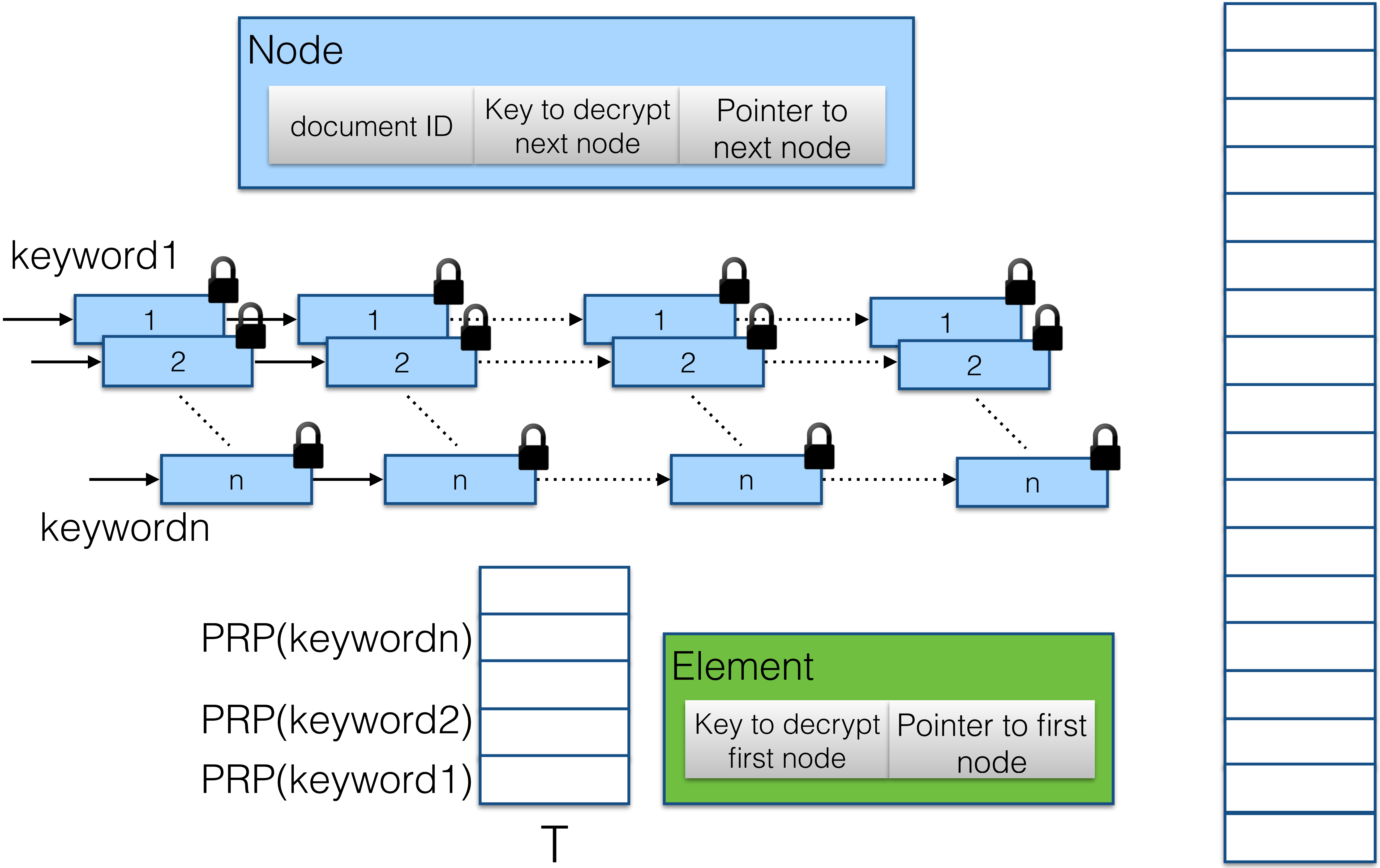
Node

document ID	Key to decrypt next node	Pointer to next node

Element

Key to decrypt first node	Pointer to first node

Linked-list based Schemes



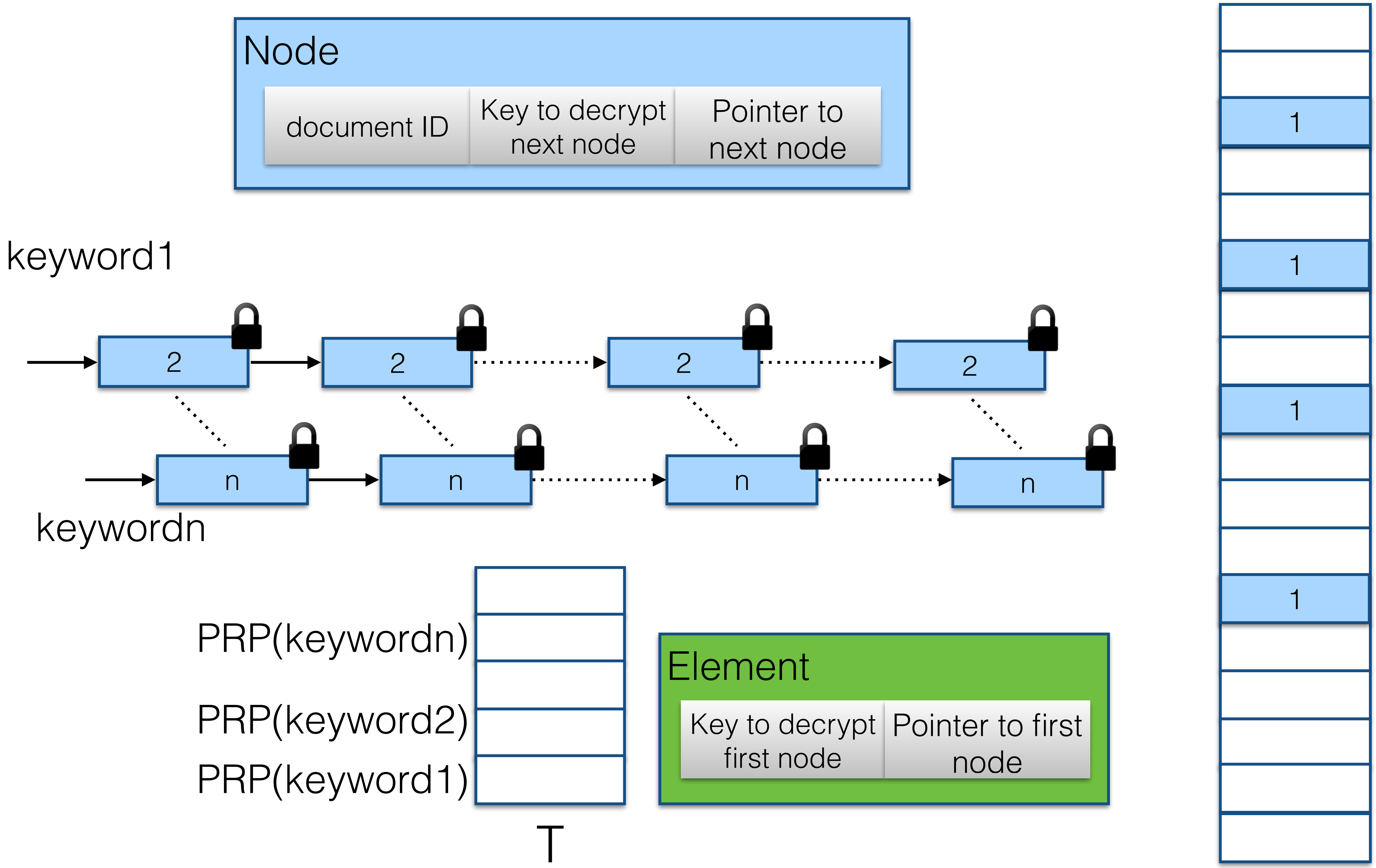
Node

document ID	Key to decrypt next node	Pointer to next node

Element

Key to decrypt first node	Pointer to first node

Linked-list based Schemes



Node

document ID

Key to decrypt next node

Pointer to next node

keyword1

keywordn

2

n

PRP(keywordn)

PRP(keyword2)

PRP(keyword1)

T

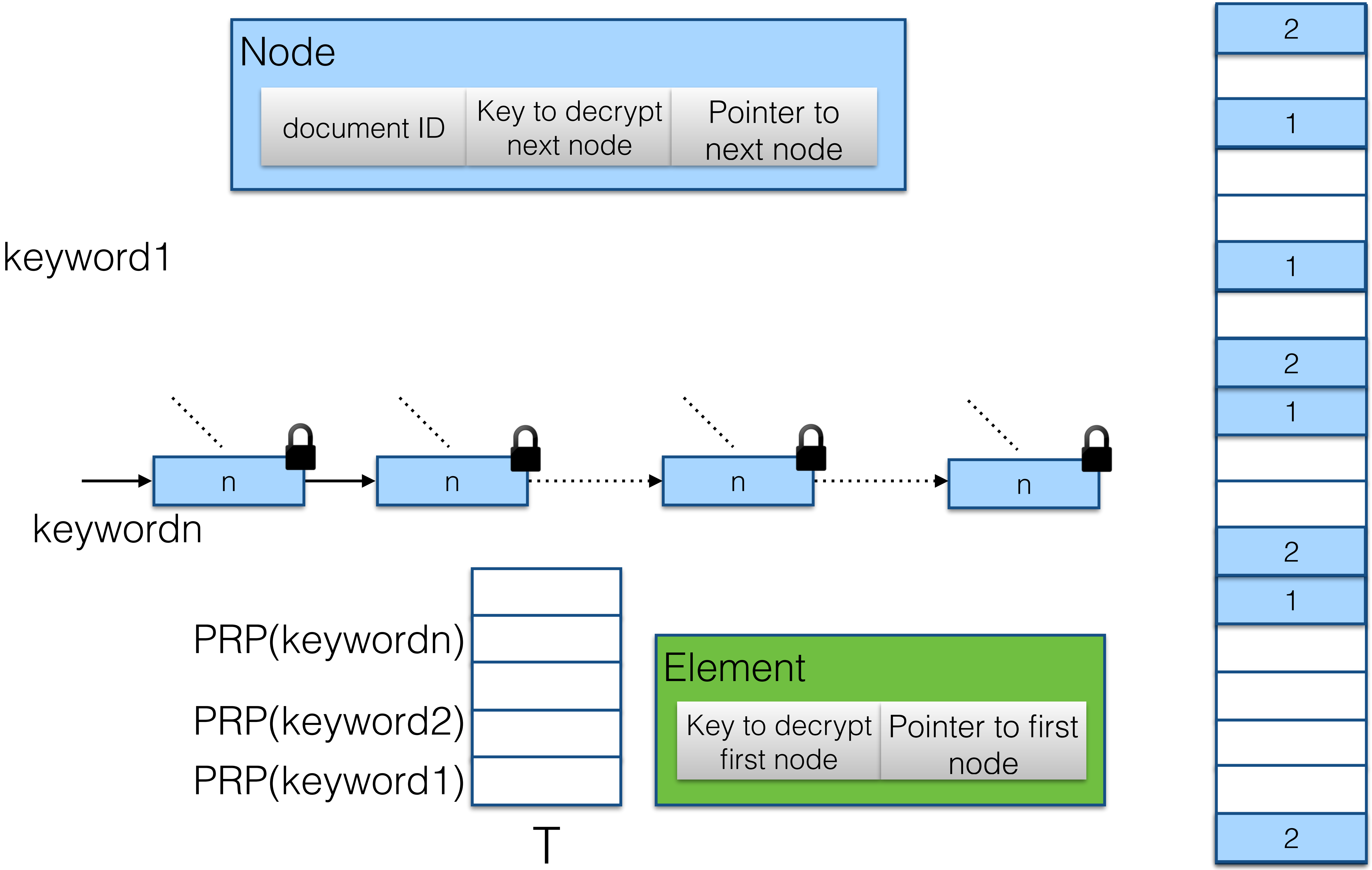
Element

Key to decrypt first node

Pointer to first node

1

Linked-list based Schemes



Node

document ID

Key to decrypt next node

Pointer to next node

keyword1

keywordn

PRP(keywordn)

PRP(keyword2)

PRP(keyword1)

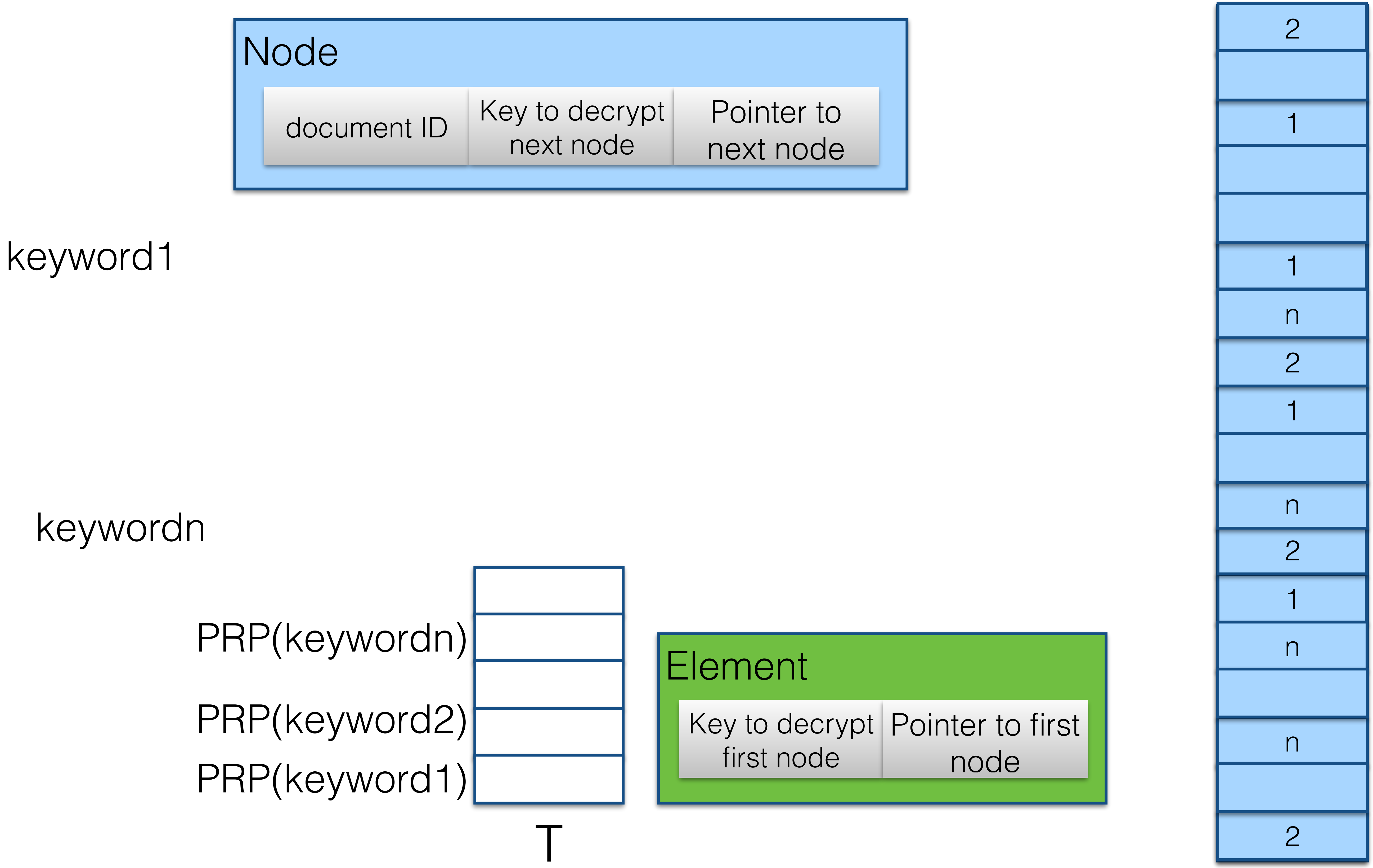
T

Element

Key to decrypt first node

Pointer to first node

Linked-list based Schemes



Node

document ID	Key to decrypt next node	Pointer to next node

keyword1

keywordn

PRP(keywordn)

PRP(keyword2)

PRP(keyword1)

T

Element

Key to decrypt first node	Pointer to first node

2

1

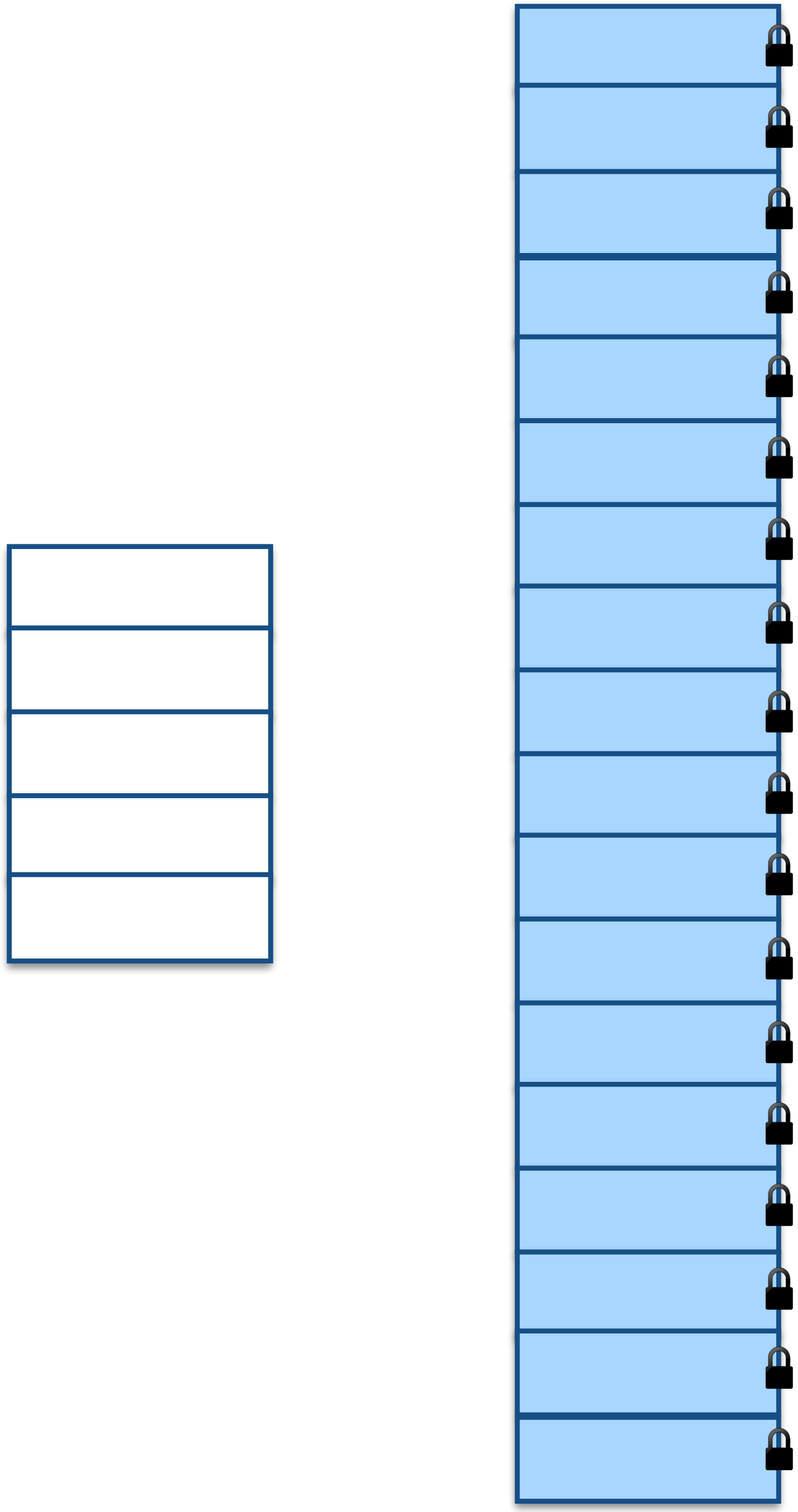
1
n
2
1

n
2
1
n

n

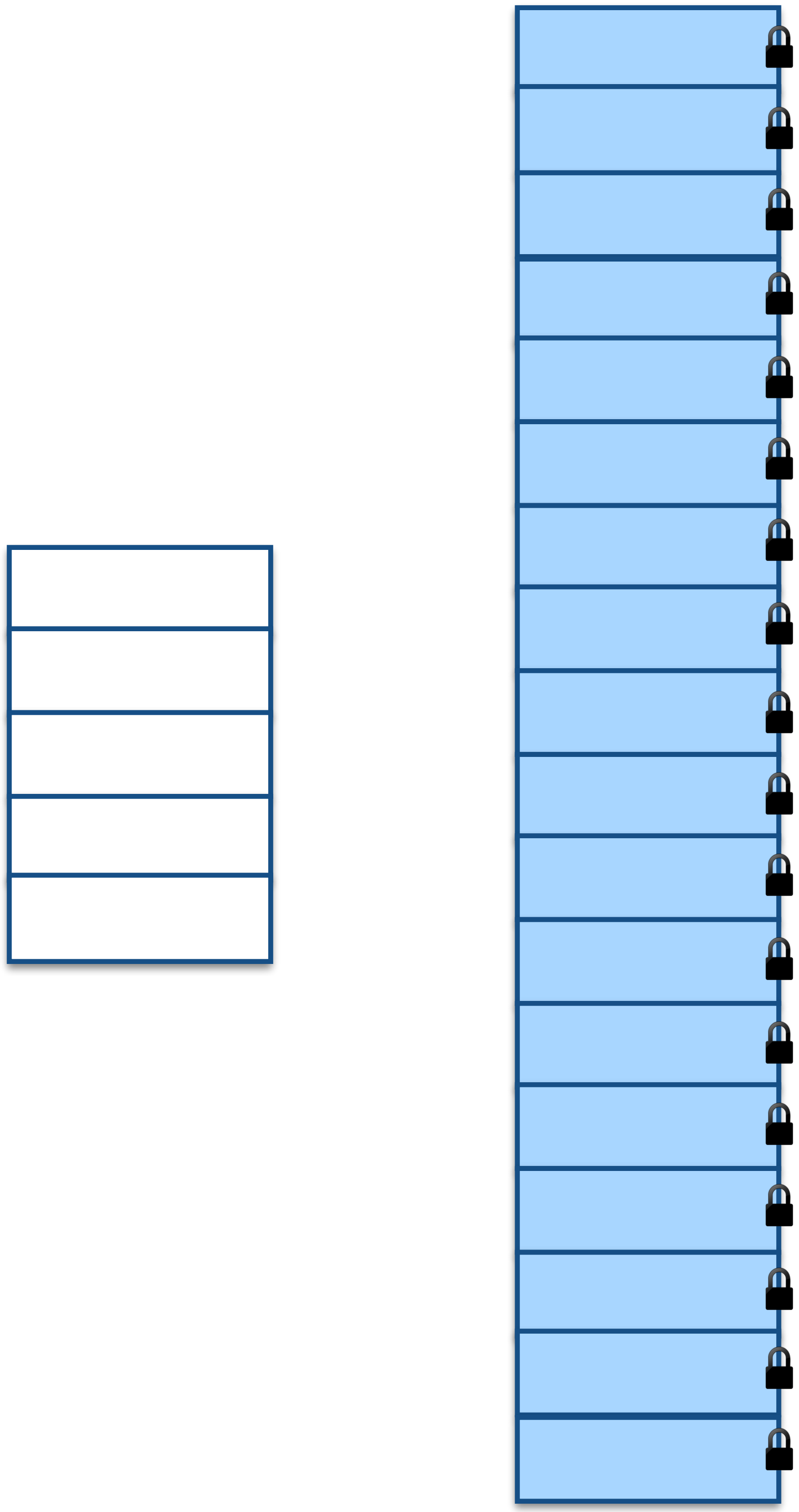
2

Search in Linked-list based Schemes



Search in Linked-list based Schemes

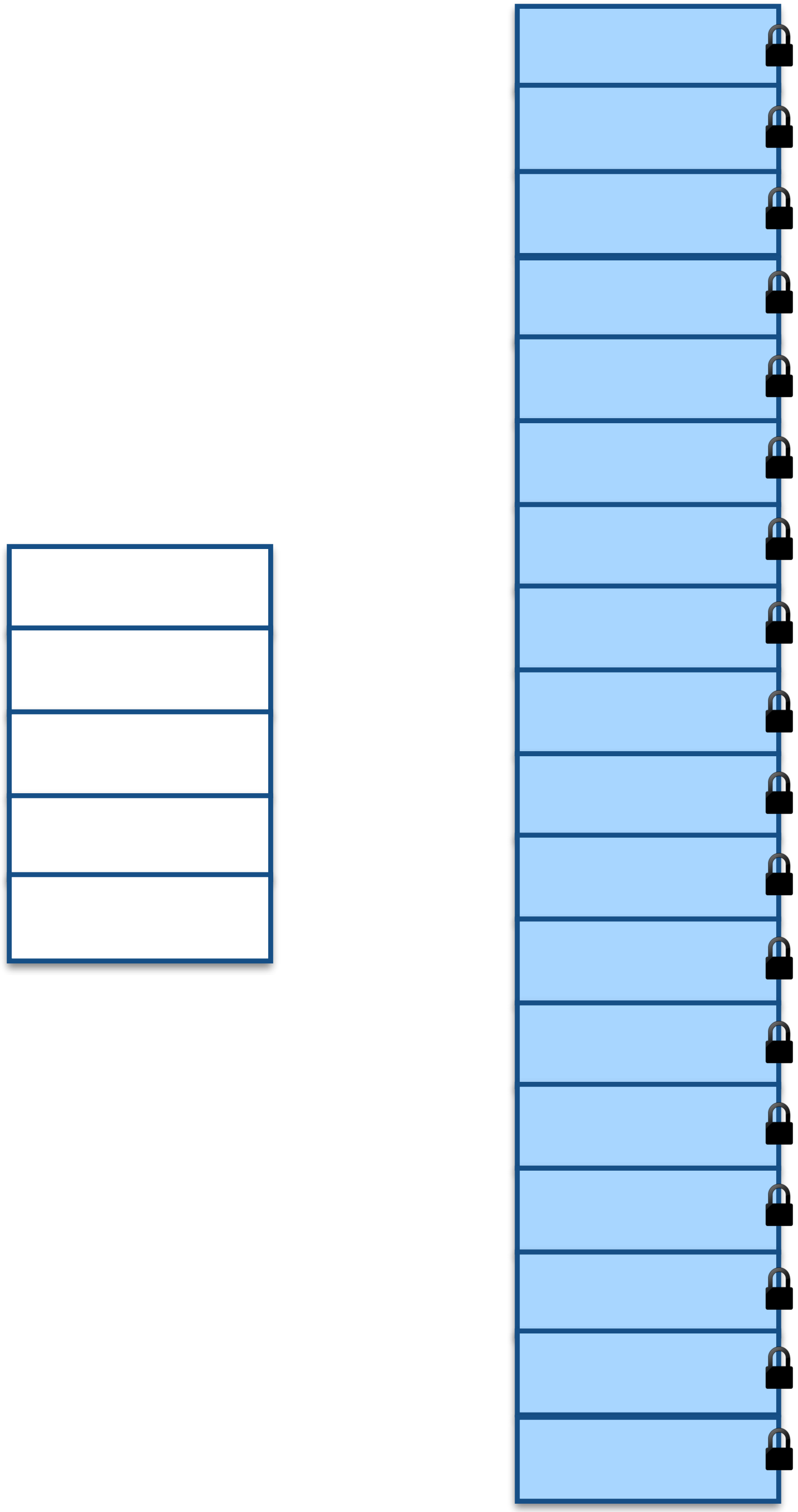
Search for keyword2



Search in Linked-list based Schemes

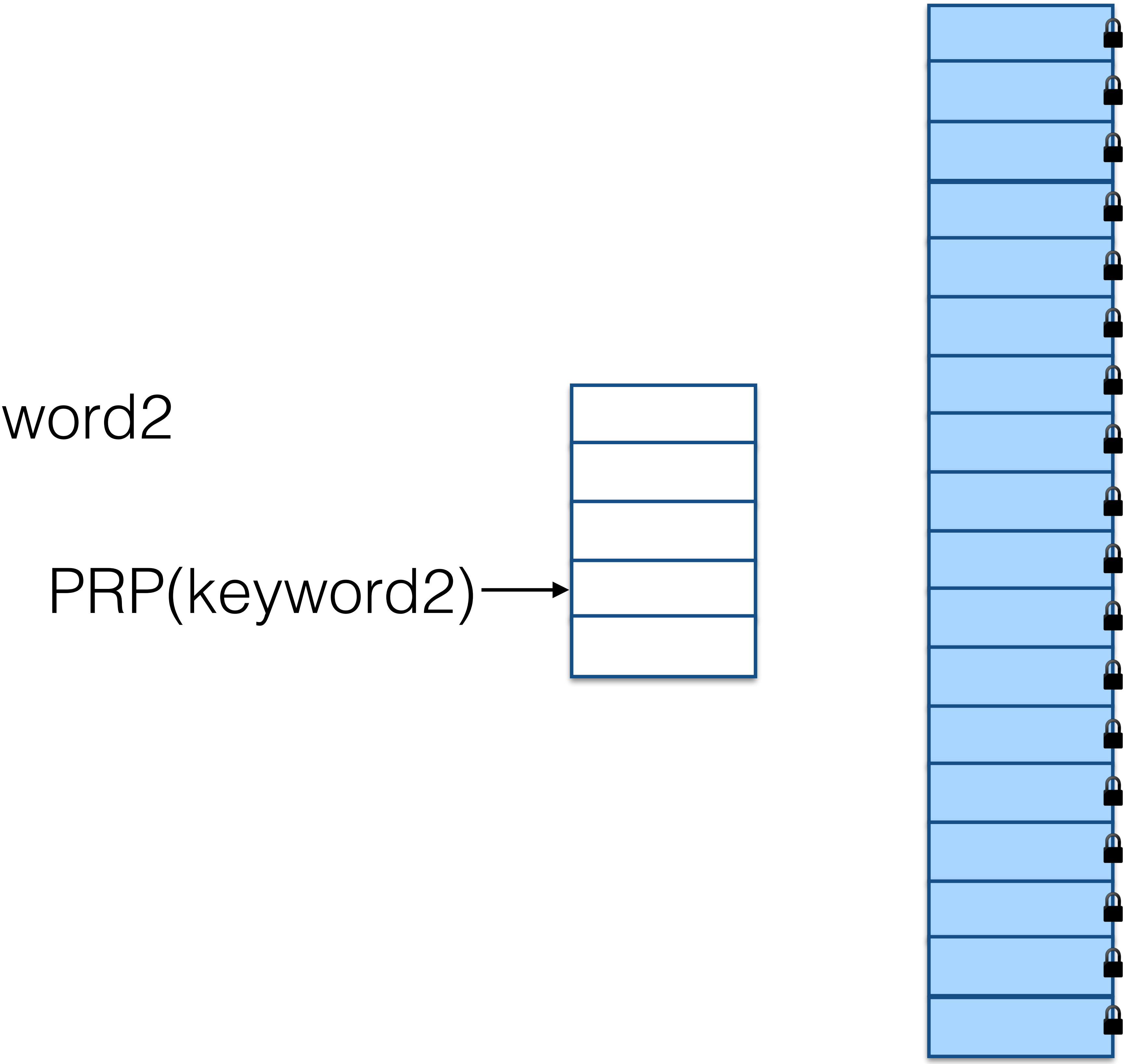
Search for keyword2

PRP(keyword2)



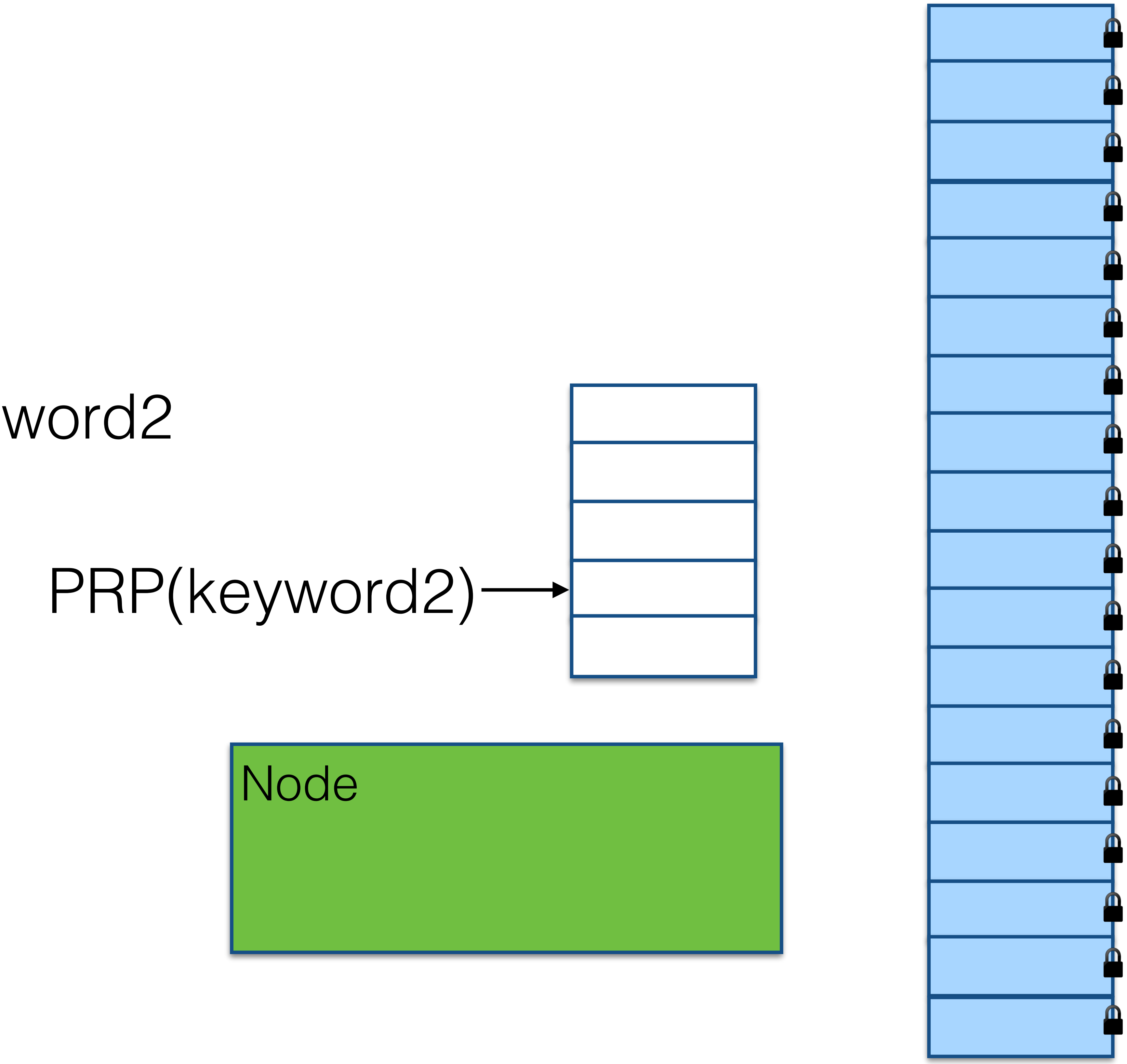
Search in Linked-list based Schemes

Search for keyword2



Search in Linked-list based Schemes

Search for keyword2

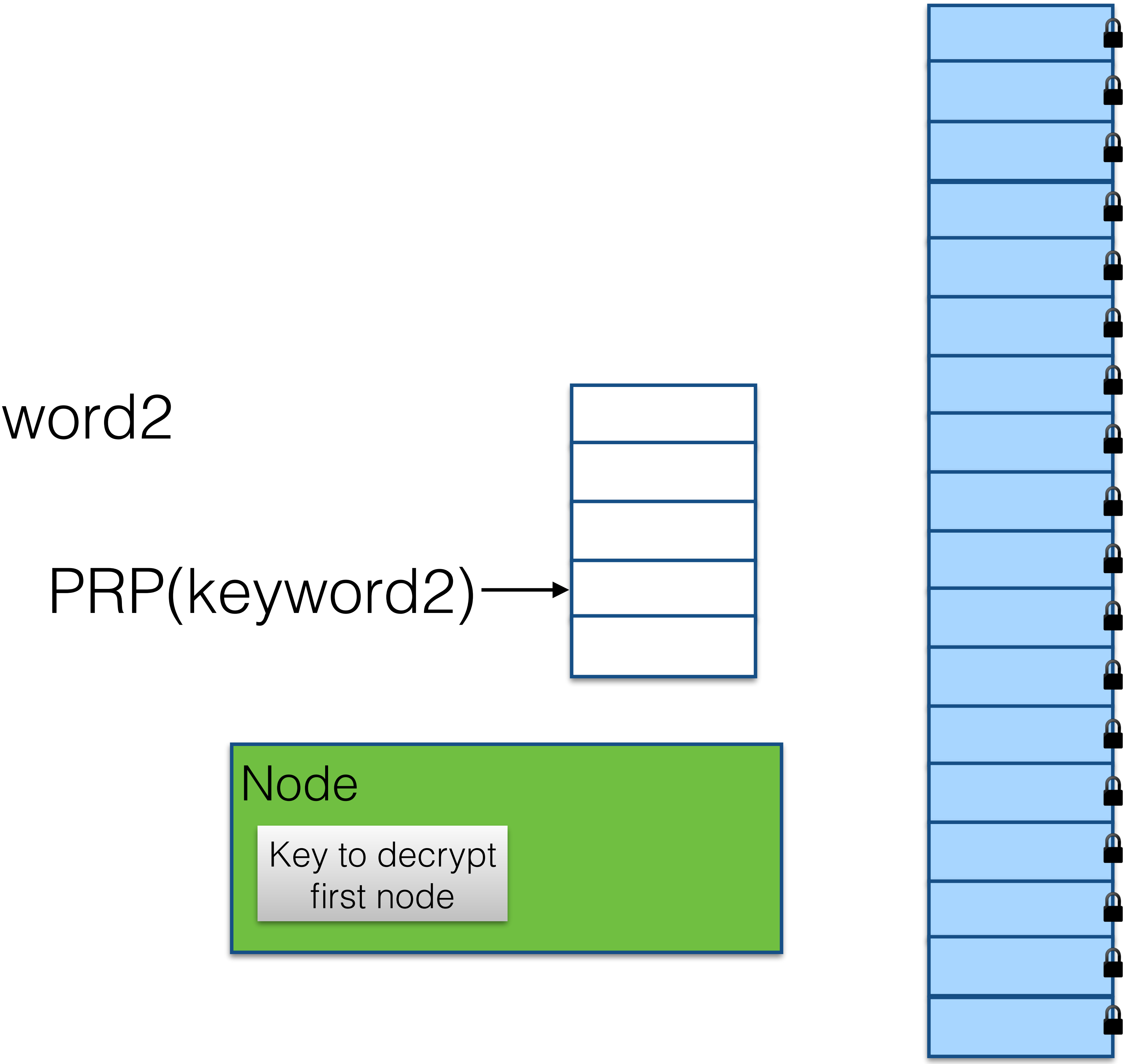


PRP(keyword2)

Node

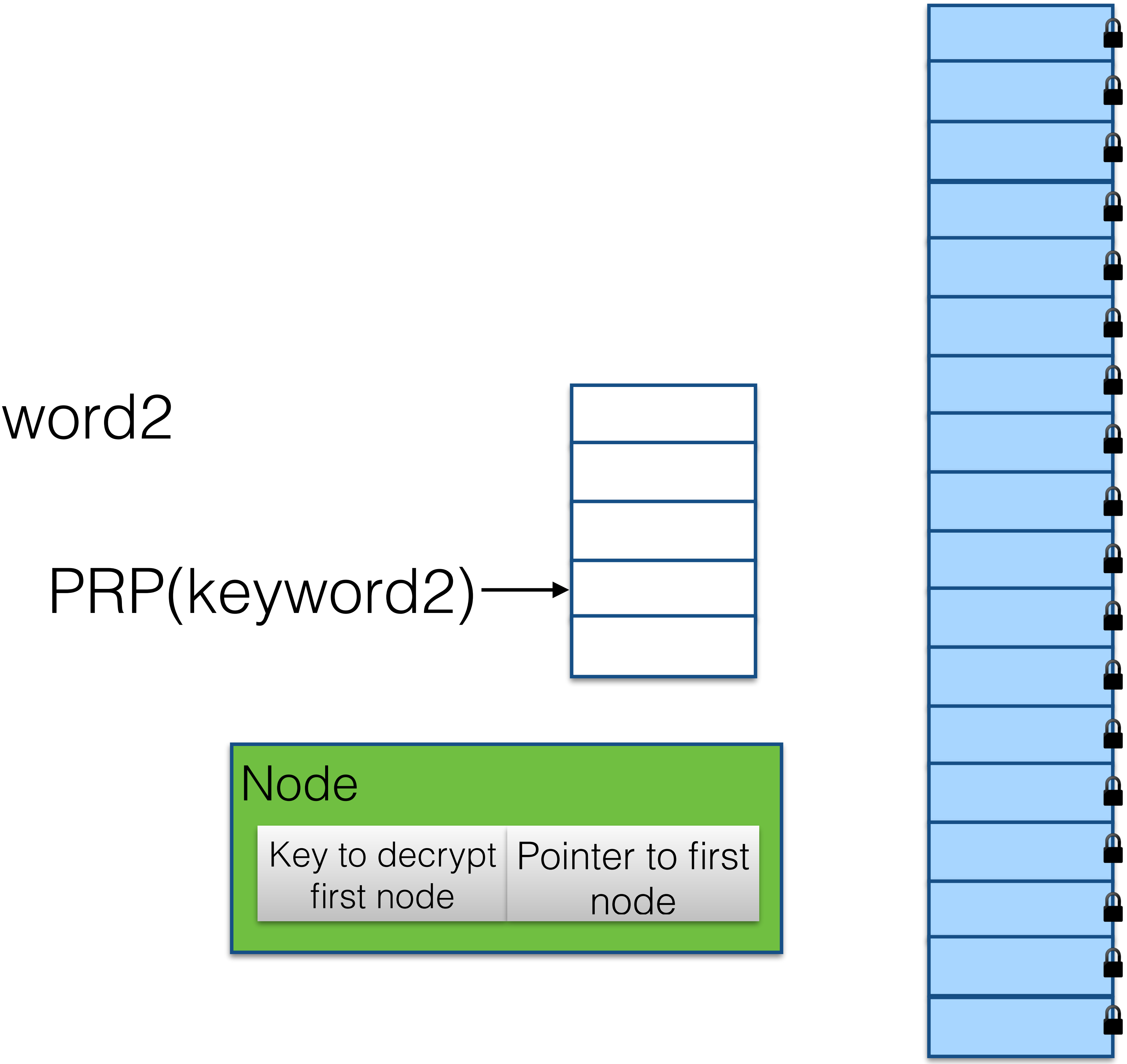
Search in Linked-list based Schemes

Search for keyword2



Search in Linked-list based Schemes

Search for keyword2



PRP(keyword2)

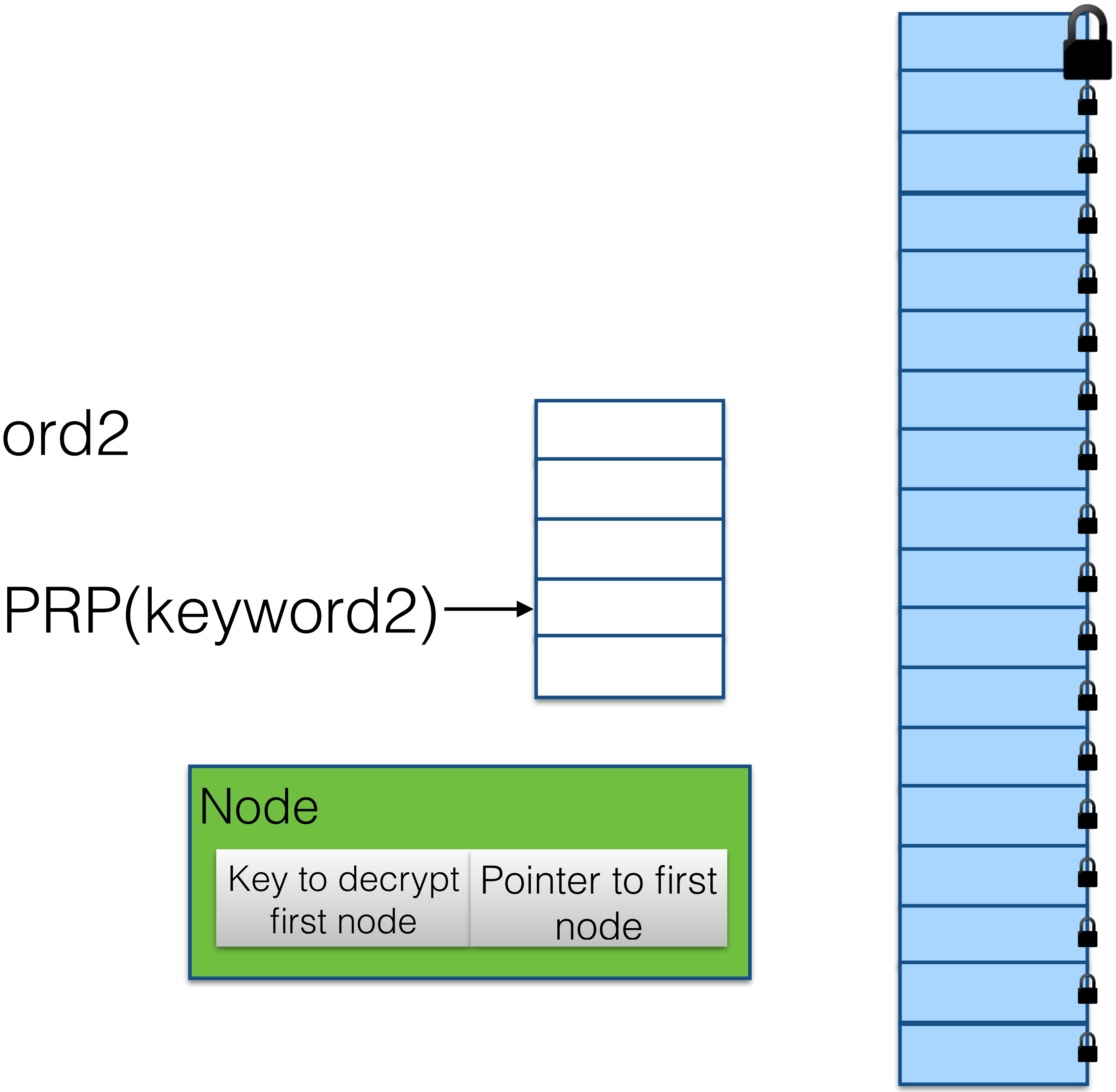
Node

Key to decrypt first node

Pointer to first node

Search in Linked-list based Schemes

Search for keyword2



PRP(keyword2)

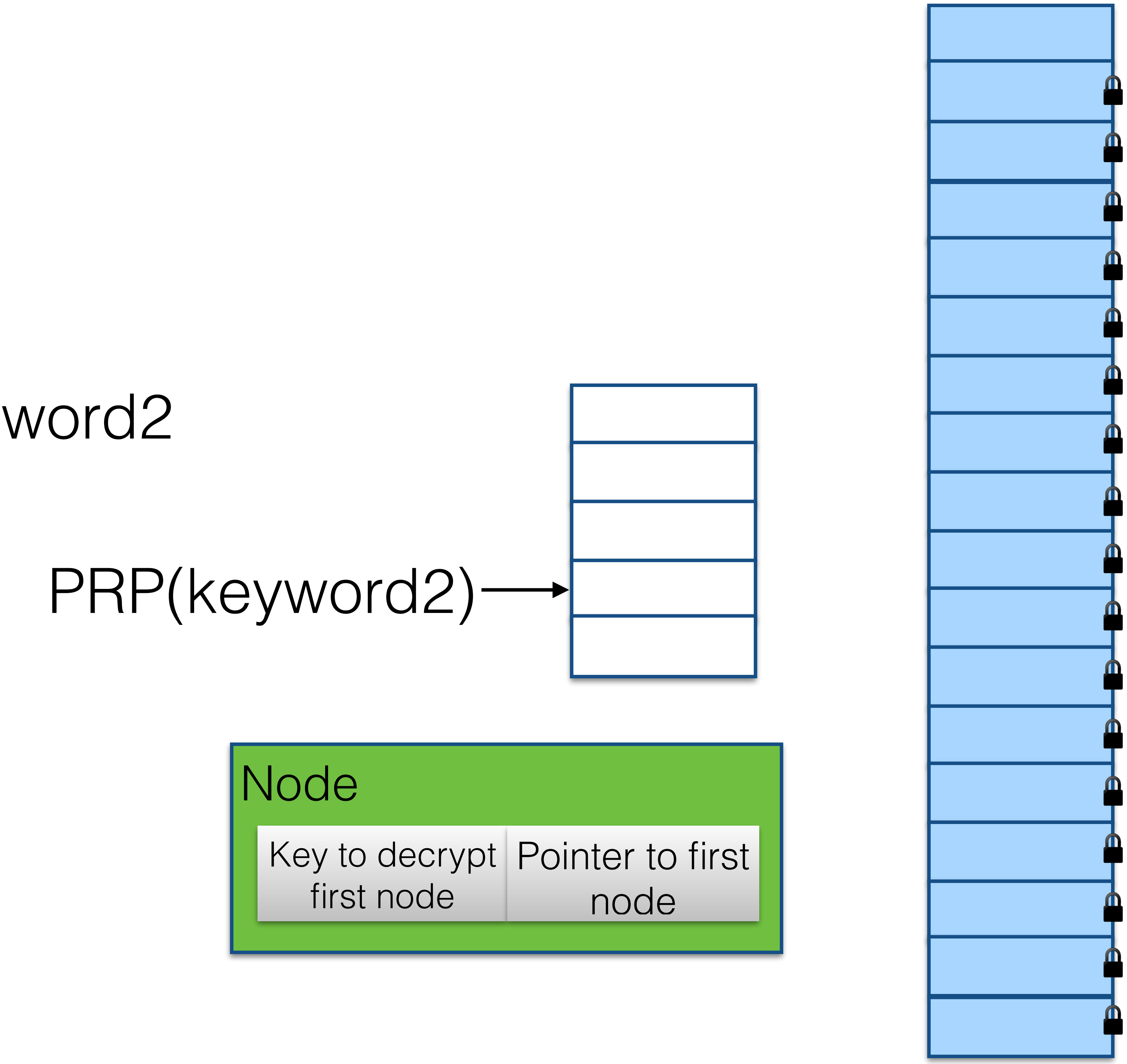
Node

Key to decrypt first node

Pointer to first node

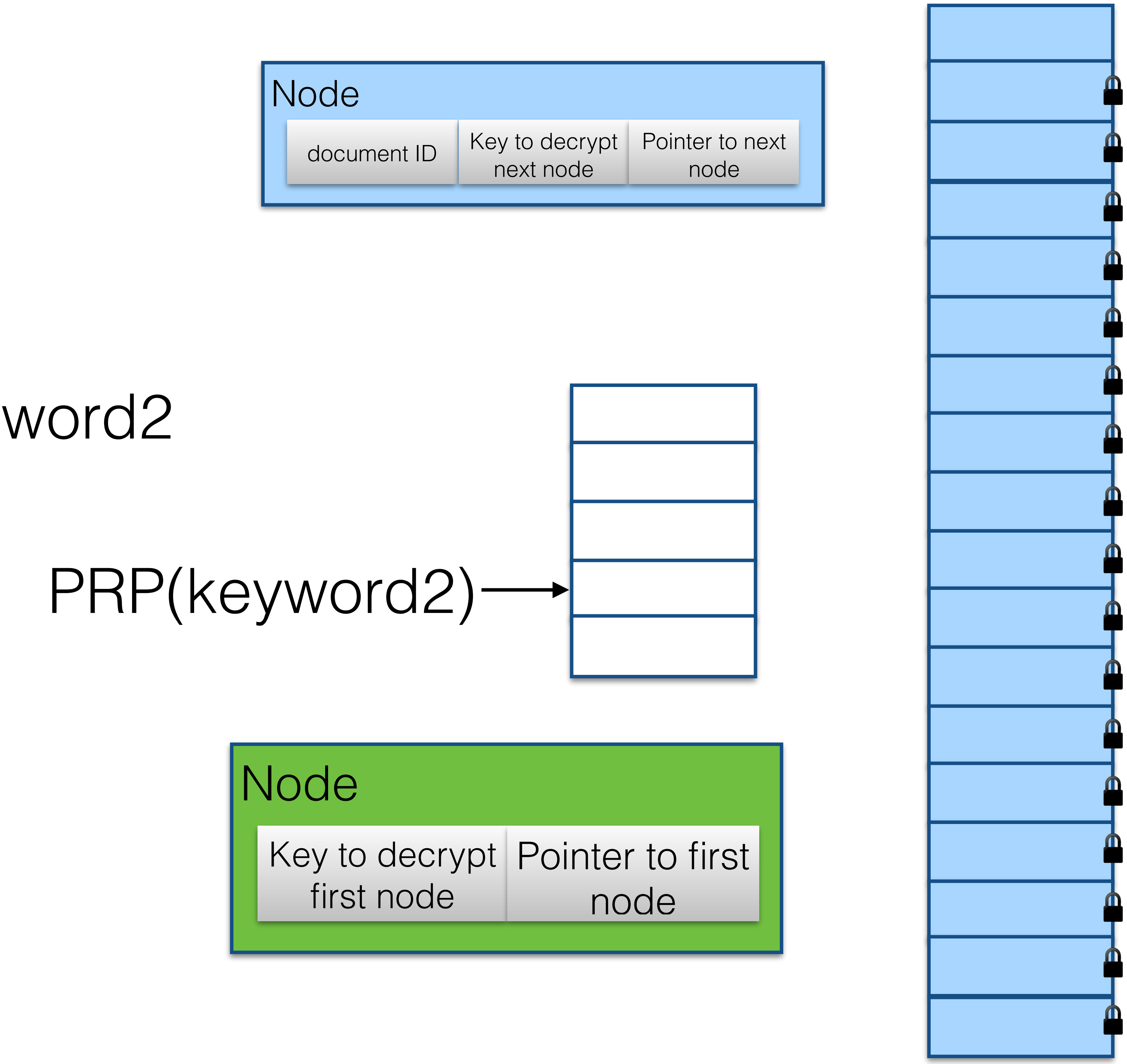
Search in Linked-list based Schemes

Search for keyword2



Search in Linked-list based Schemes

Search for keyword2



Node

document ID	Key to decrypt next node	Pointer to next node

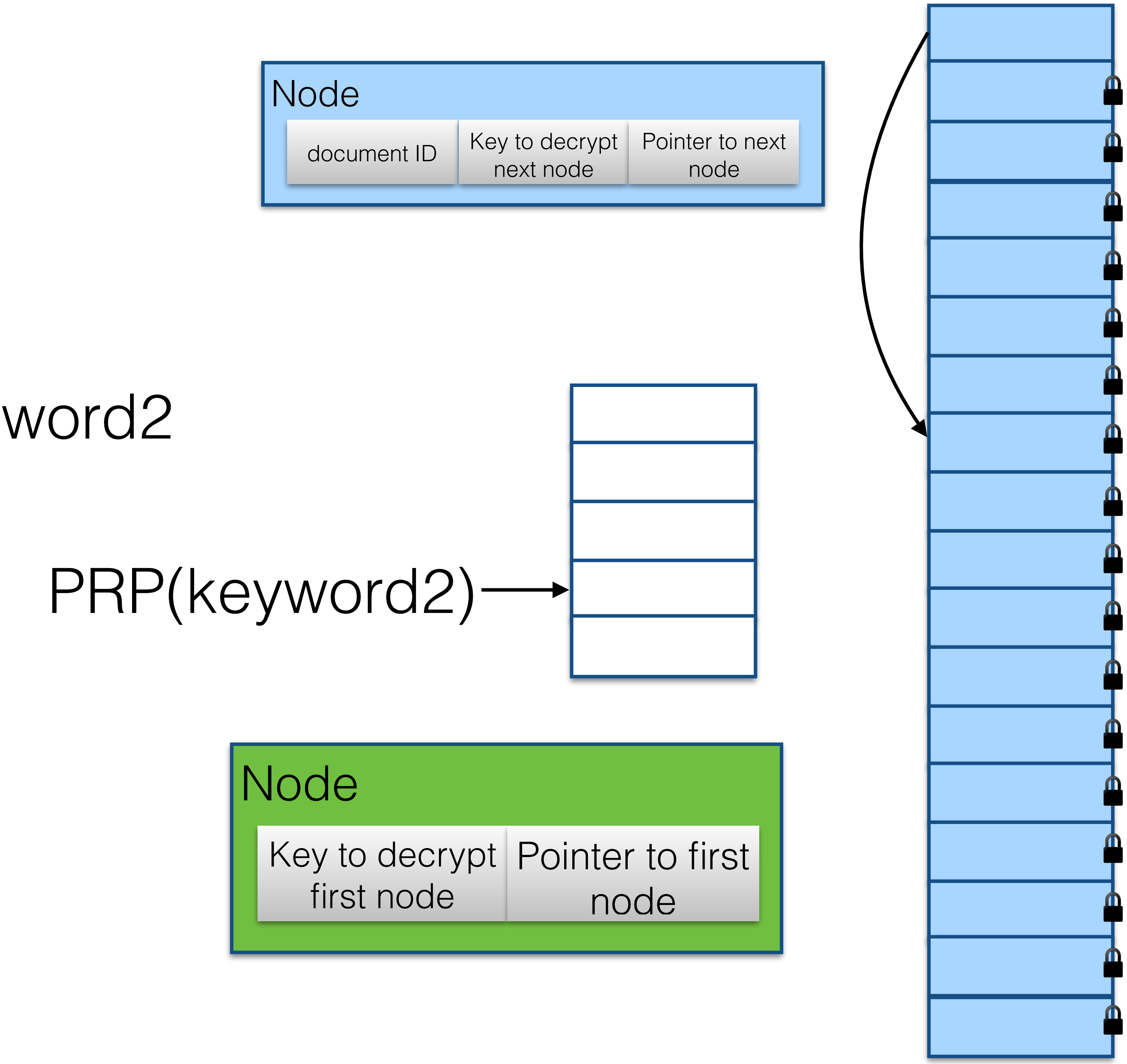
PRP(keyword2)

Node

Key to decrypt first node	Pointer to first node

Search in Linked-list based Schemes

Search for keyword2



Node

document ID

Key to decrypt next node

Pointer to next node

PRP(keyword2)

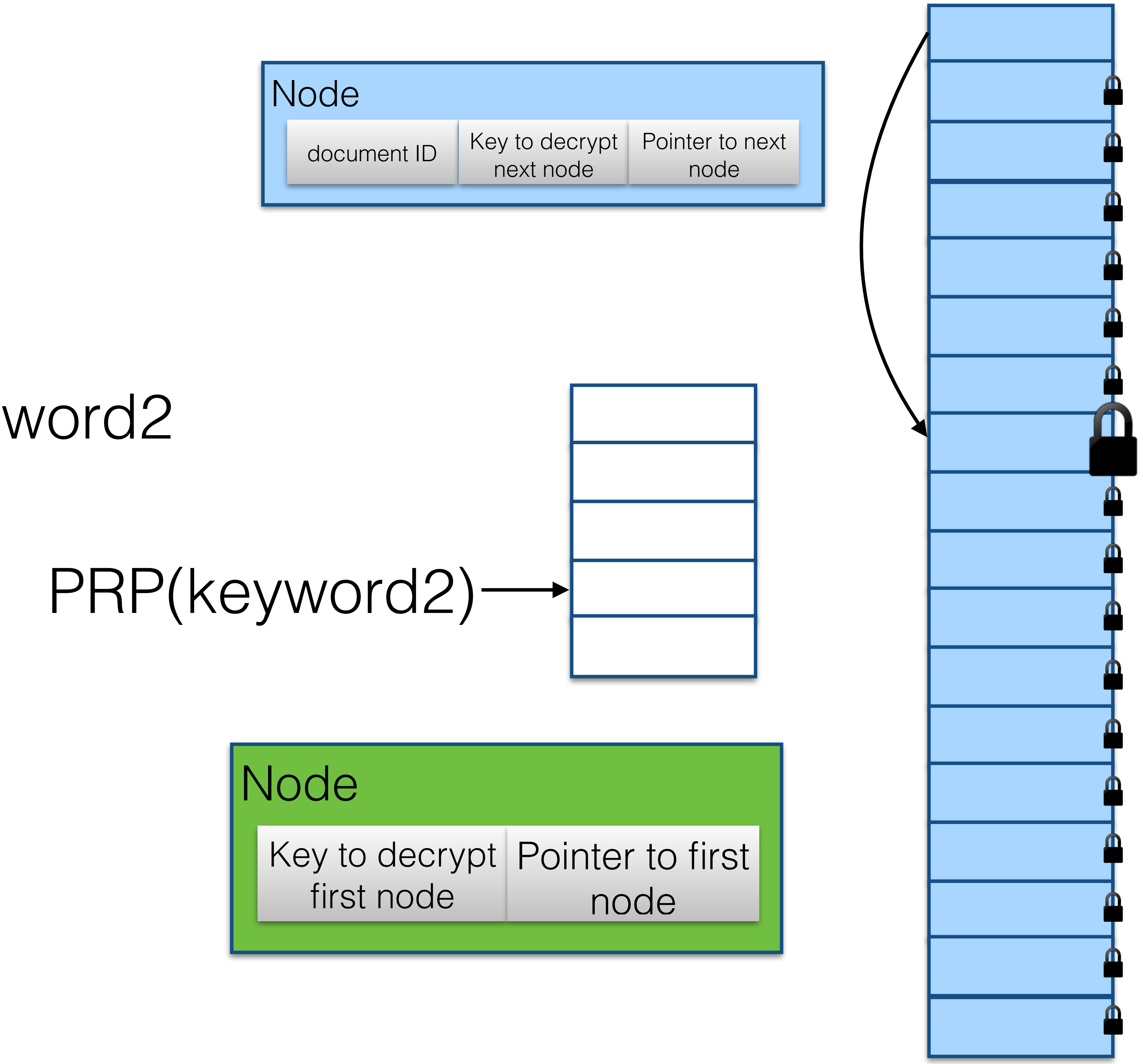
Node

Key to decrypt first node

Pointer to first node

Search in Linked-list based Schemes

Search for keyword2



Node

document ID

Key to decrypt next node

Pointer to next node

PRP(keyword2)

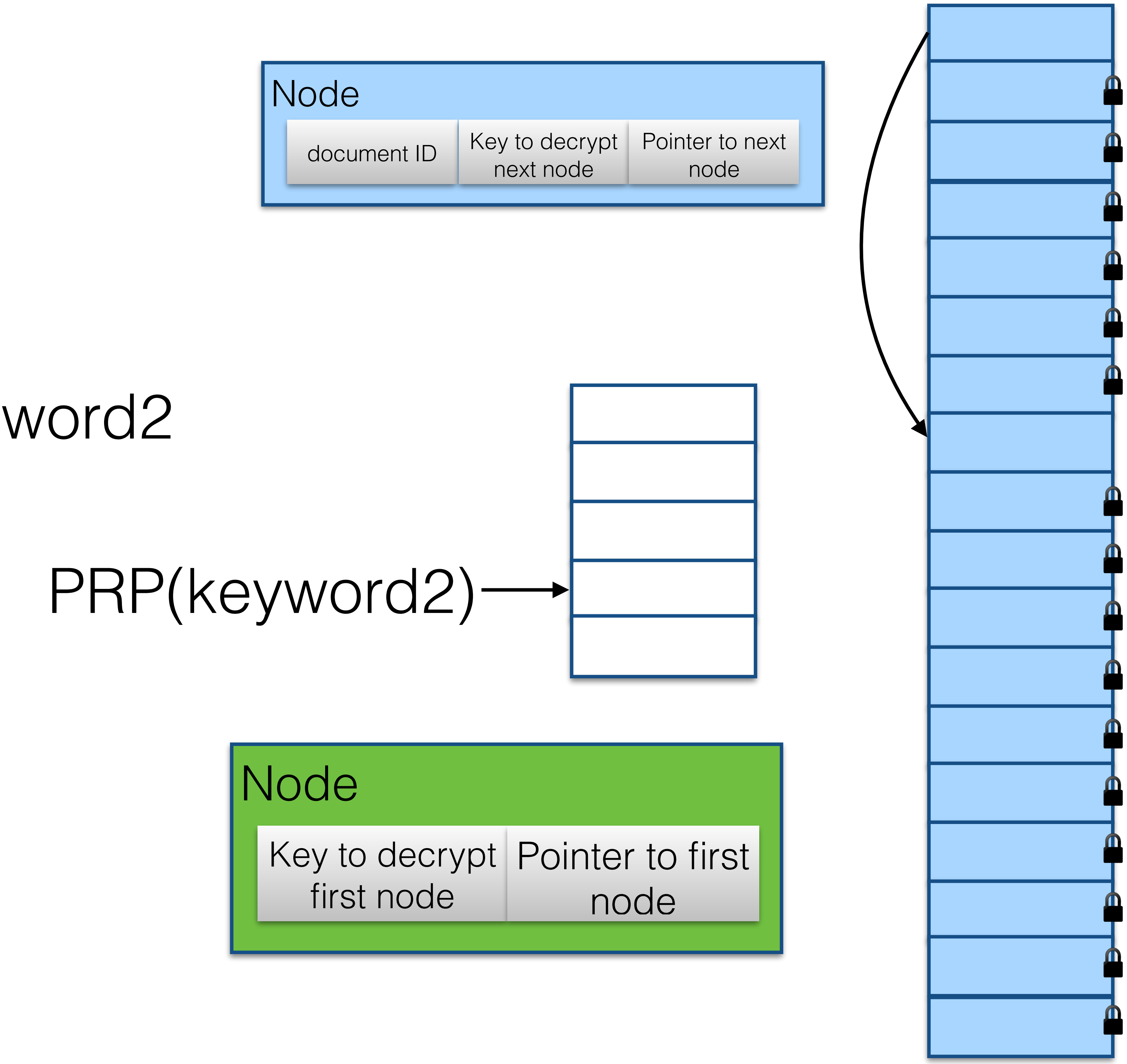
Node

Key to decrypt first node

Pointer to first node

Search in Linked-list based Schemes

Search for keyword2



Node

document ID

Key to decrypt next node

Pointer to next node

PRP(keyword2)

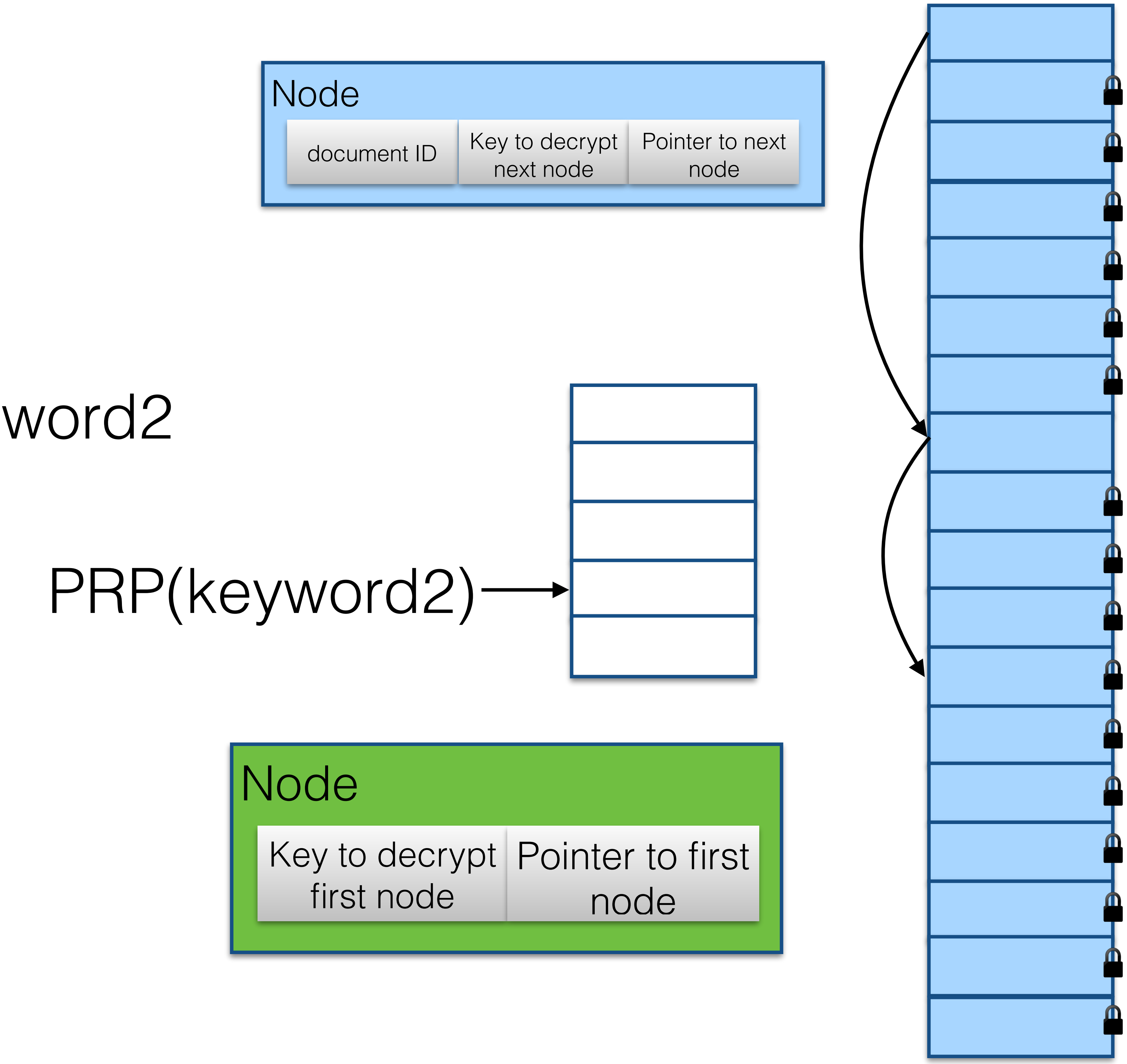
Node

Key to decrypt first node

Pointer to first node

Search in Linked-list based Schemes

Search for keyword2



Node

document ID

Key to decrypt next node

Pointer to next node

PRP(keyword2)

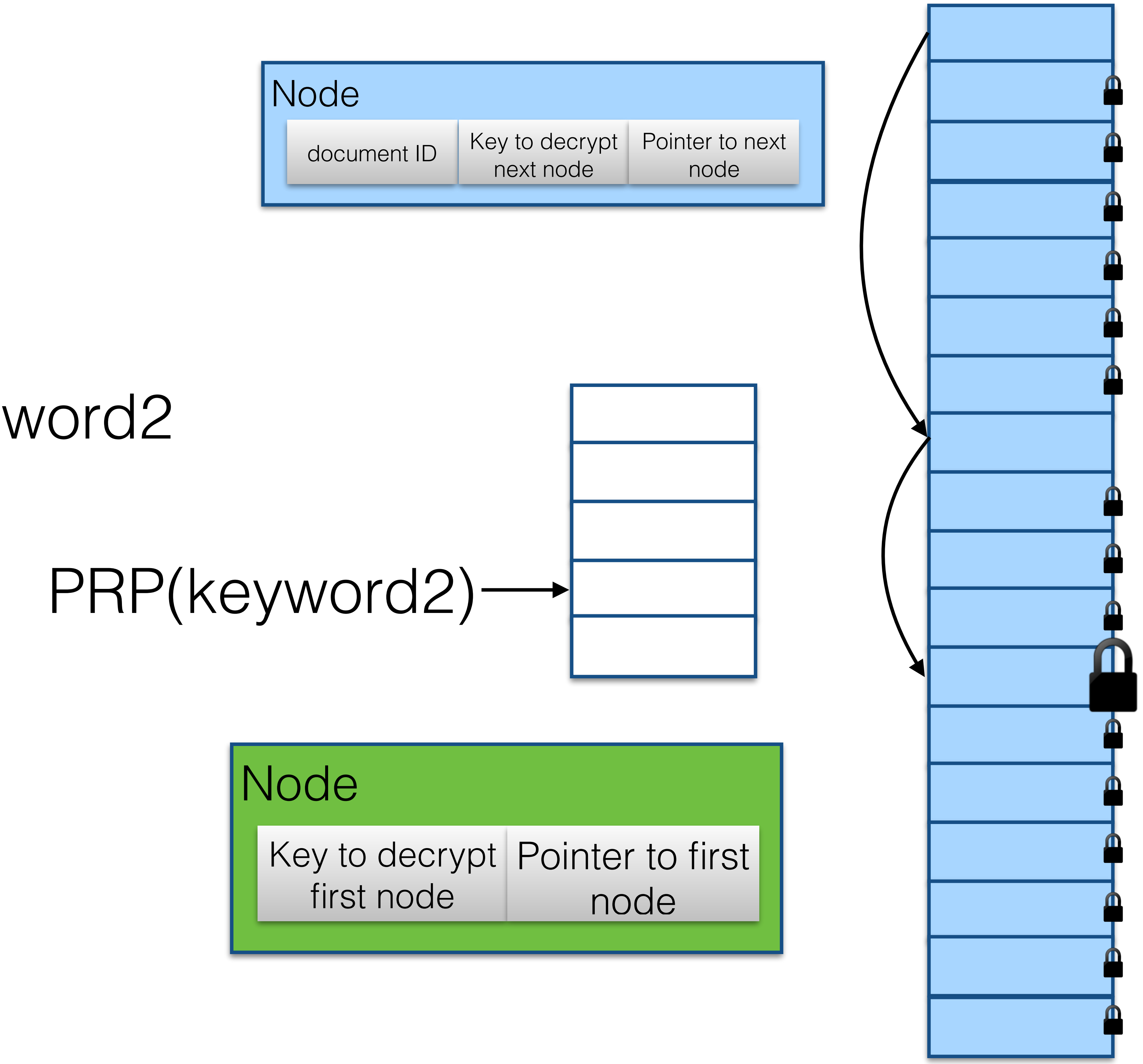
Node

Key to decrypt first node

Pointer to first node

Search in Linked-list based Schemes

Search for keyword2



Node

document ID

Key to decrypt next node

Pointer to next node

PRP(keyword2)

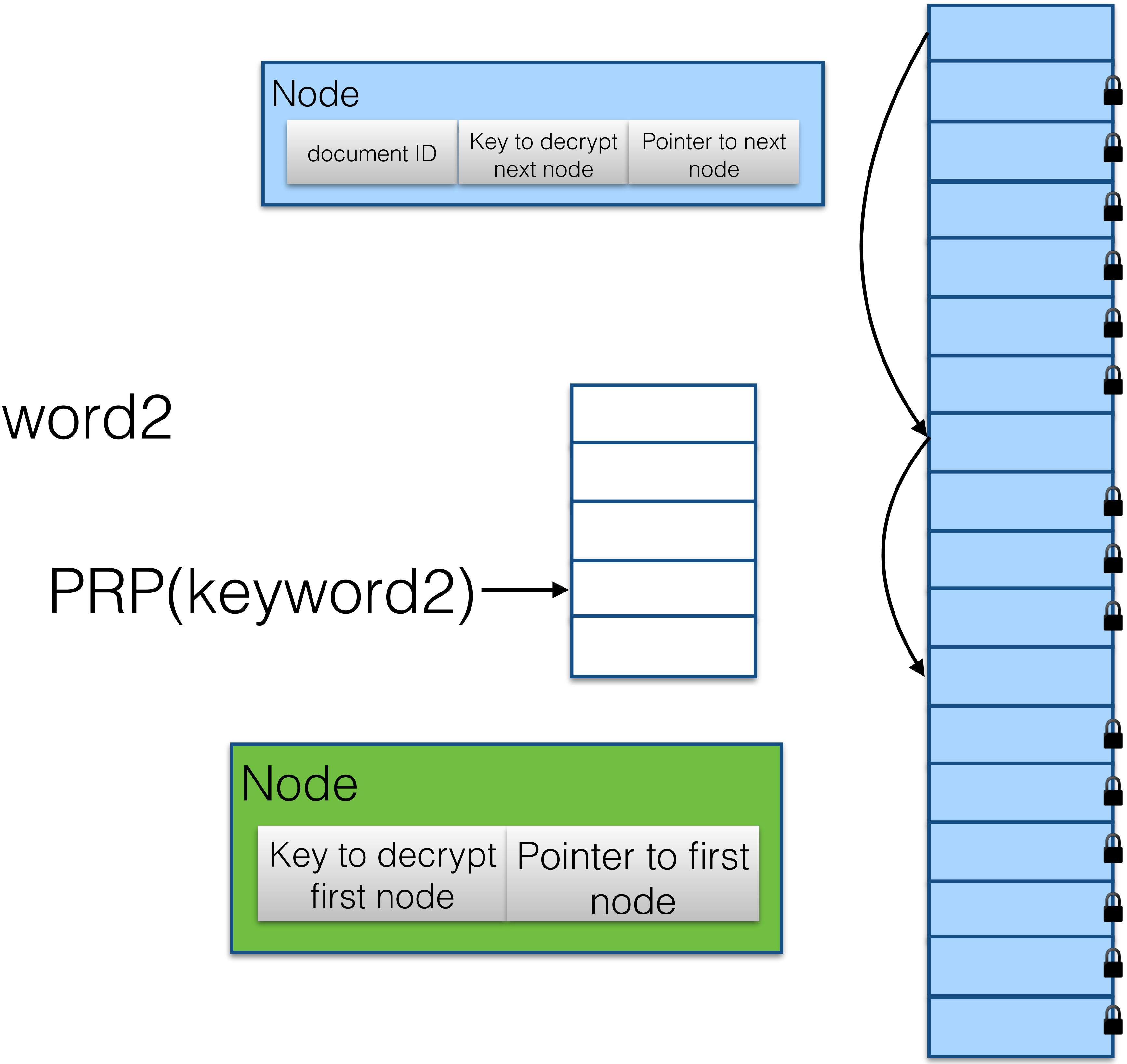
Node

Key to decrypt first node

Pointer to first node

Search in Linked-list based Schemes

Search for keyword2



Node

document ID

Key to decrypt next node

Pointer to next node

PRP(keyword2)

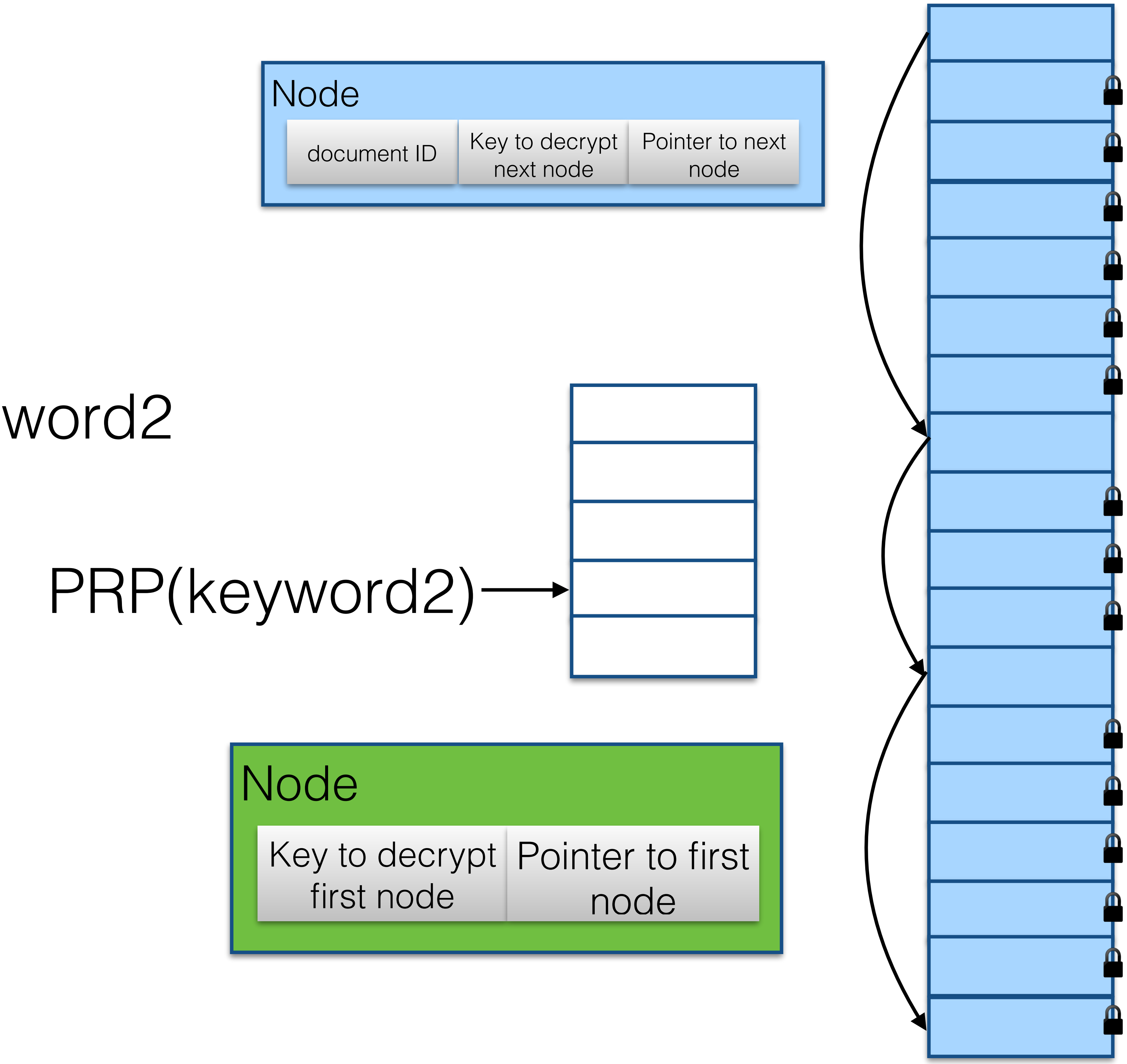
Node

Key to decrypt first node

Pointer to first node

Search in Linked-list based Schemes

Search for keyword2



Node

document ID

Key to decrypt next node

Pointer to next node

PRP(keyword2)

Node

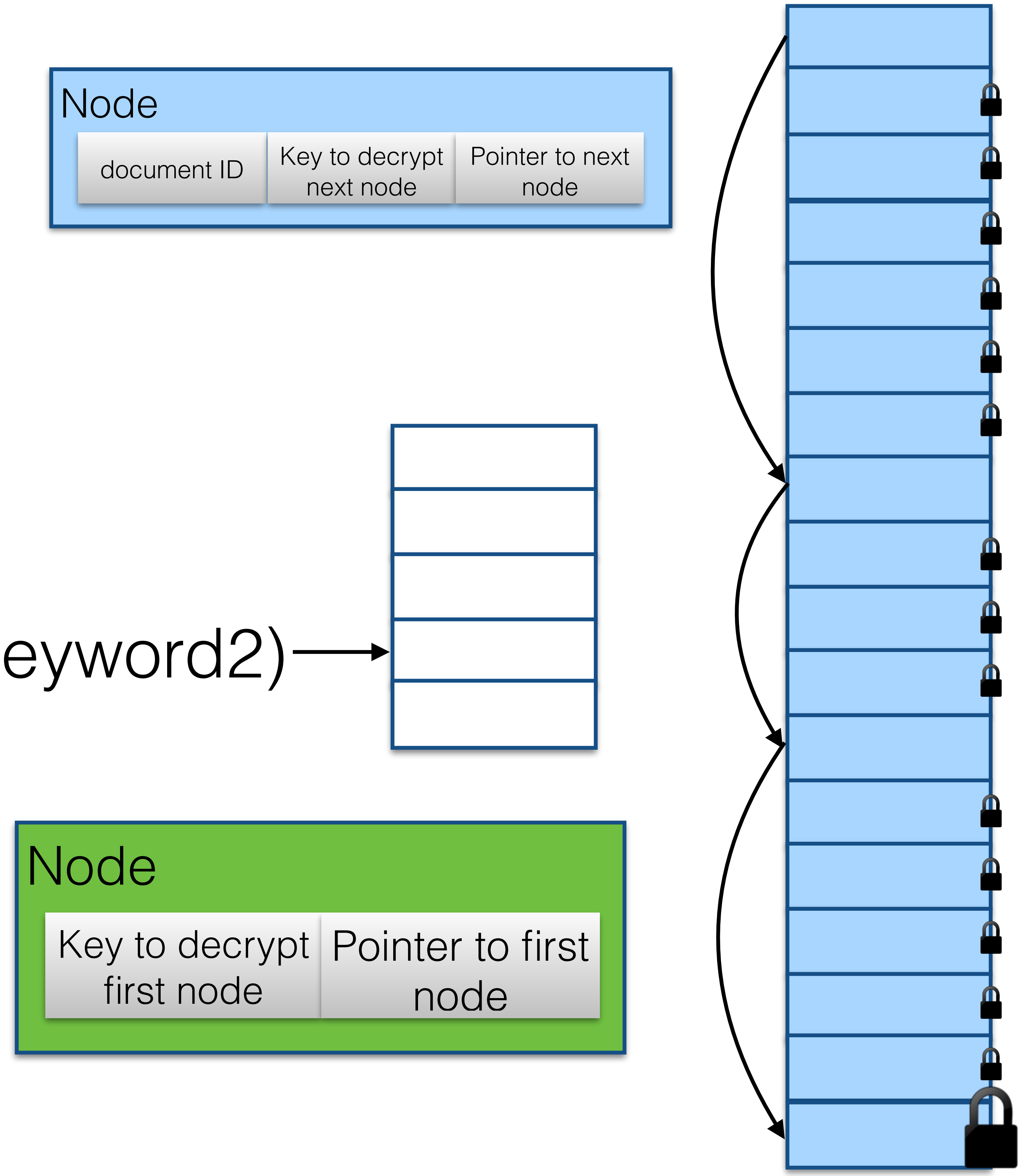
Key to decrypt first node

Pointer to first node

Search in Linked-list based Schemes

Search for keyword2

PRP(keyword2)



Node

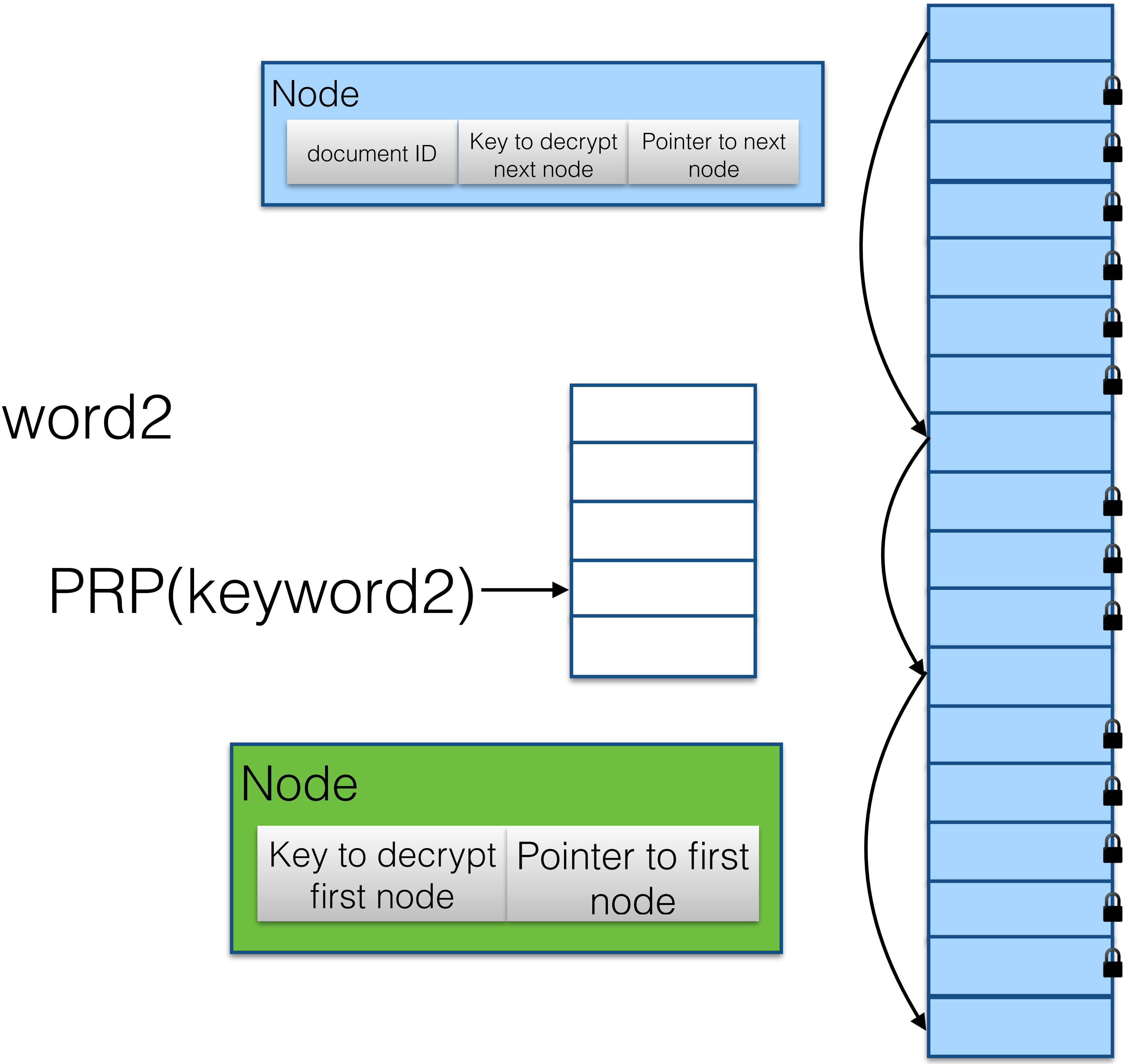
document ID	Key to decrypt next node	Pointer to next node

Node

Key to decrypt first node	Pointer to first node

Search in Linked-list based Schemes

Search for keyword2



Node

document ID

Key to decrypt next node

Pointer to next node

PRP(keyword2)

Node

Key to decrypt first node

Pointer to first node

Dictionary Based Schemes

- Use dictionary data-structure
- Each (keyword, document) pair is stored in the dictionary
- Optimizations to reduce disk reads
- Highly scalable

Dictionary Based Schemes

- Non-standard leakage
- Complicated delete operation using revocation identifiers
    - Deletion require more storage
    - Complicates later addition of deleted keywords

This Work

Supports only
Single-Keyword Search

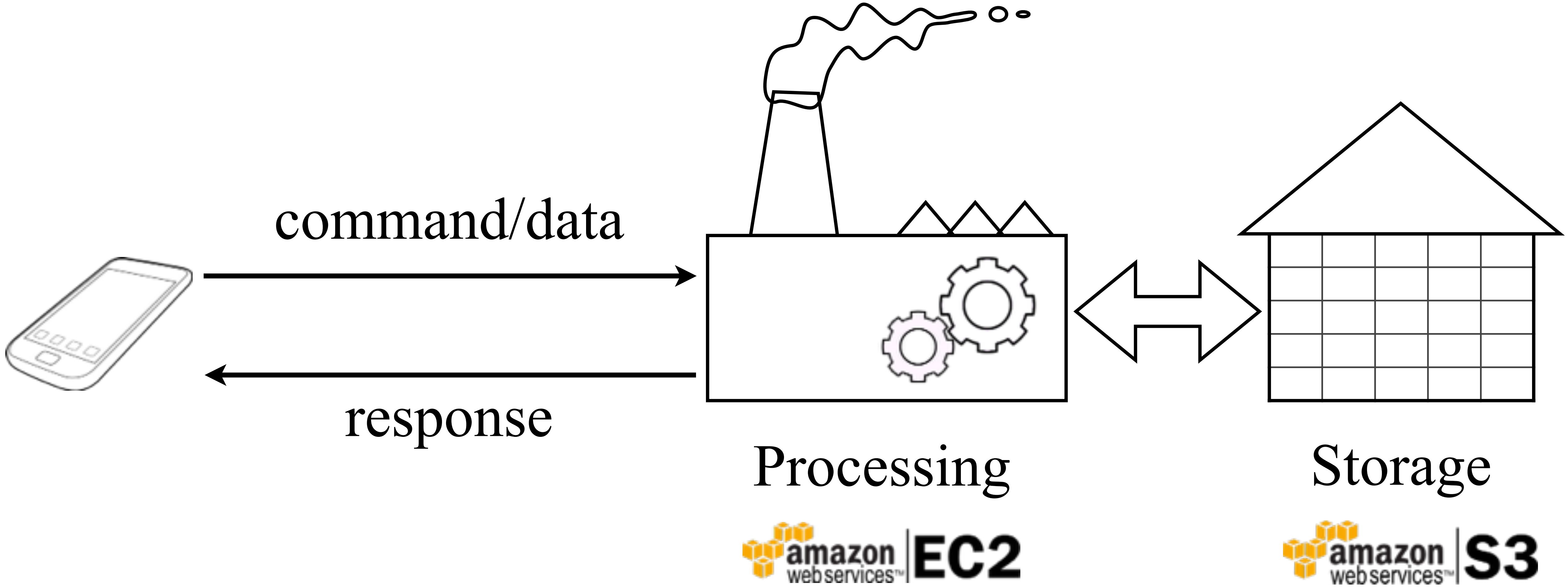
More basic primitive:
Blind Storage

Simple and efficient scheme

Computation-free server

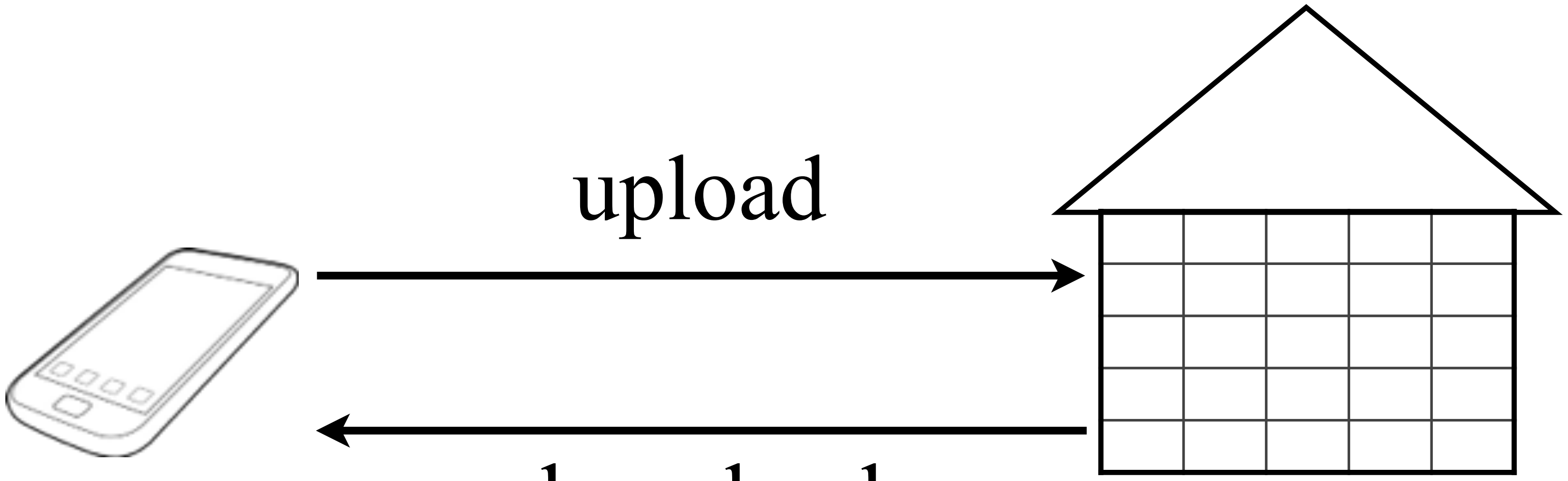
Computation-free server

All other SSE schemes require computation to be done on the server.



Computation-free server

Our scheme works with computation-free server

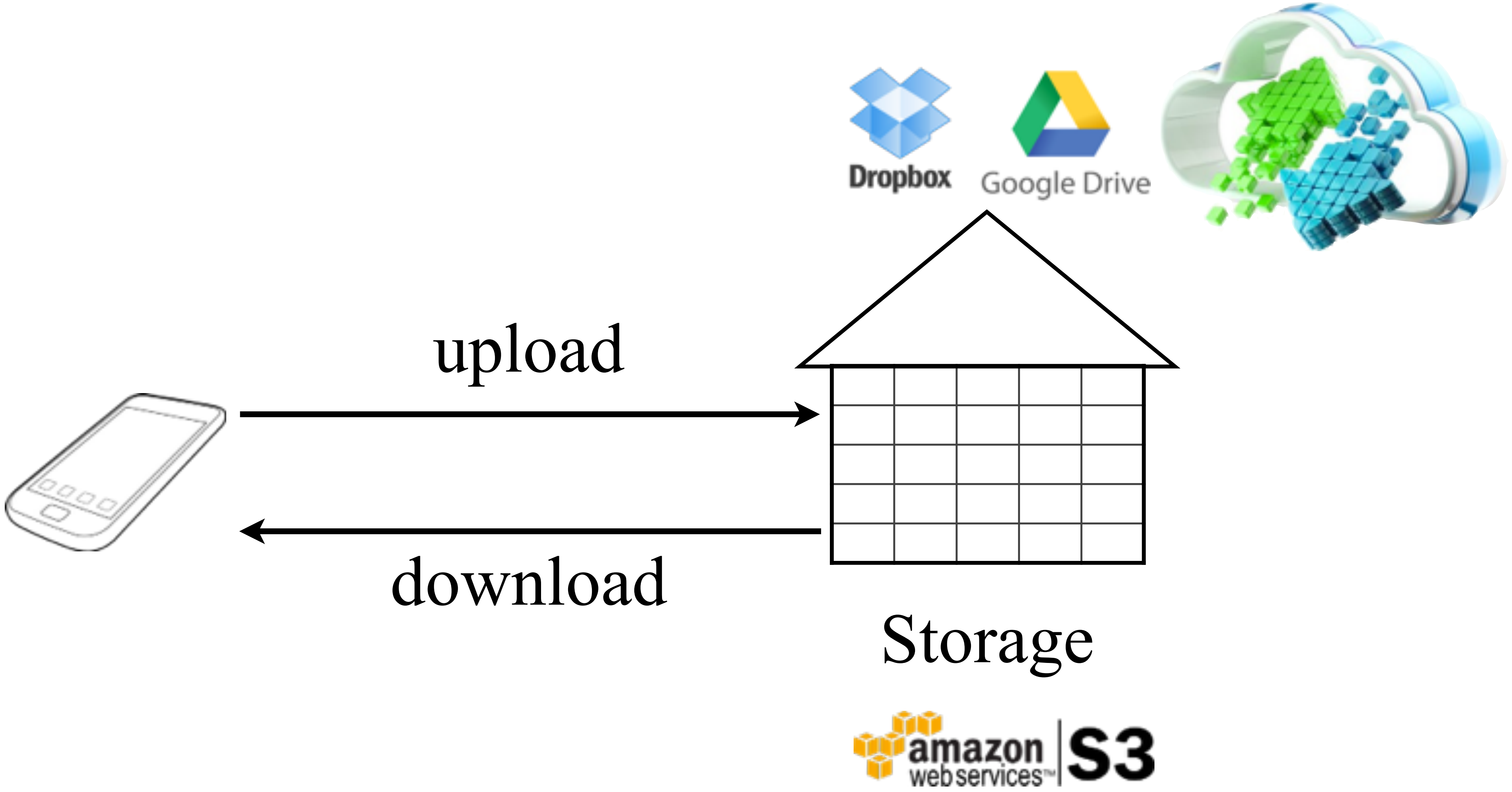


Storage

amazon web services™ | S3

Computation-free server

Our scheme works with computation-free server



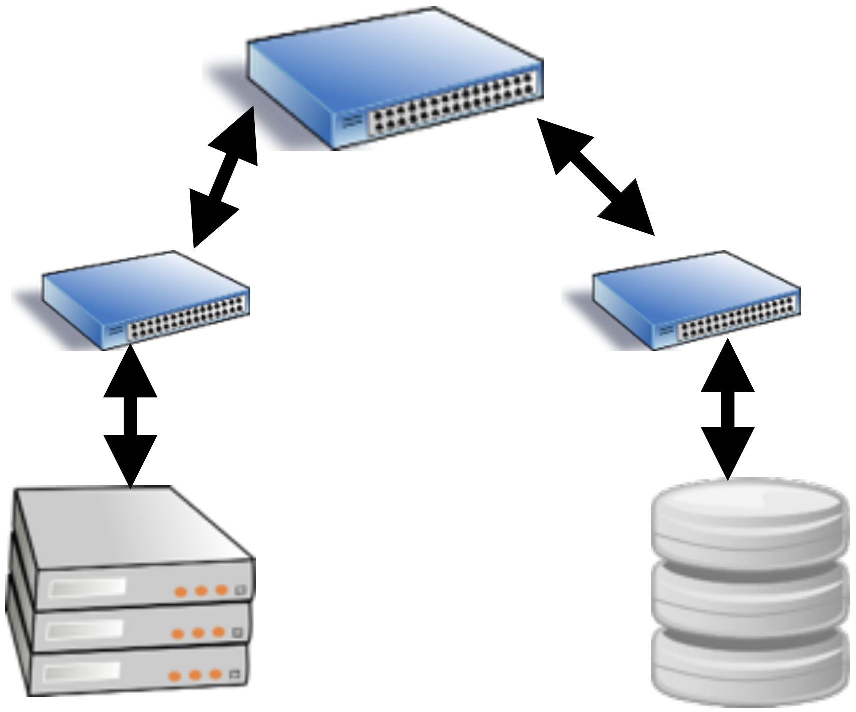
upload

download

Storage

Why is it important?

- Bandwidth costs: It is expensive to use computing and storage from two different cloud providers.
- Latency issues even using same cloud service
  - e.g., Amazon EC2 and Amazon S3
  - cloud services have well-known latency issues
  - Data from storage nodes need to be transmitted over the datacenter network



Other features

- Supports compression
- Document privacy
- Inherently parallel
- Leaks less. Leakage specified using "ideal functionality”
- Satisfies a fully adaptive security definition
- Security in the standard model
- Zero delete cost

Blind Storage

The Functionality

Setup

Client

Cloud

Setup

Client **Cloud**

Setup

Client

Cloud

BlindStore

Setup

Client

Cloud

BlindStore

Setup

Client

Cloud

BlindStore

Setup

Client

Cloud

BlindStore

Setup

Client

Cloud

BlindStore

Does **not** leak
total number of files and
size of individual files

Setup

Client

Cloud

BlindStore

Does **not** leak **total number of files** and **size of individual files**

Leaks pre-determined upper bound on the total amount of data

Access

Client

Cloud

BlindStore

Access

Client

Cloud

Read

filename

BlindStore

Access

Client

Cloud

Read

filename

BlindStore

Access

Client

Cloud

Read

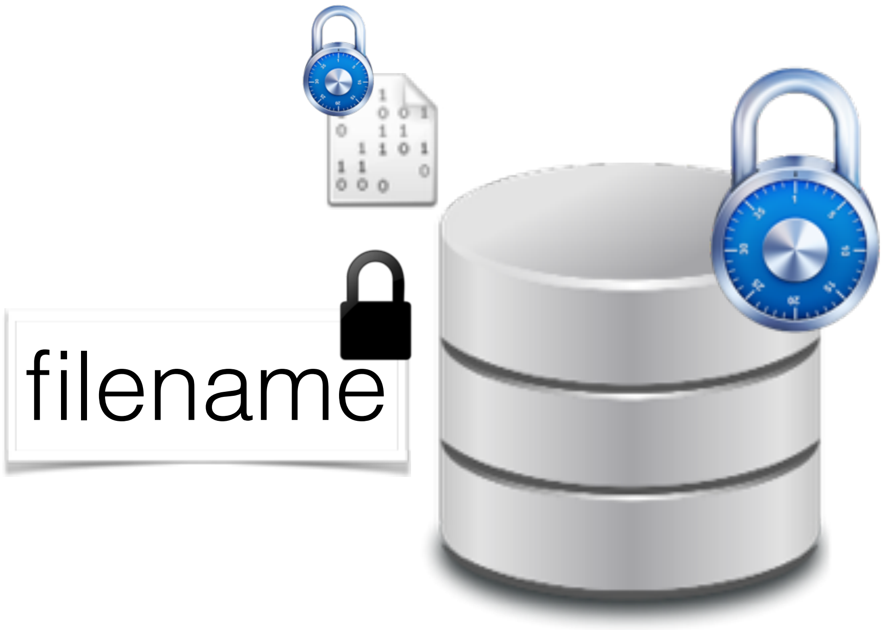
BlindStore

Access

Client

Cloud

Read



filename

BlindStore

Access

Client

Read

Cloud

Leakage

- ⋆ Access Pattern
- ⋆ File size

BlindStore

Access

Client

Cloud

Leakage

- ⋆ Access Pattern
- ⋆ File size

Read

BlindStore

Access

Client

Cloud

Leakage

- ⋆ Access Pattern
- ⋆ File size

Read

filename

BlindStore

Access

Client

Cloud

Leakage

- ⋆ Access Pattern
- ⋆ File size

Read

Write

filename 🔒

BlindStore

Access

Client

Read

Write

Cloud

Leakage

- ⋆ Access Pattern
- ⋆ File size

BlindStore

Access

Client

Cloud

Leakage

★ Access Pattern

★ File size

Read

filename

BlindStore

Write

ScatterStore

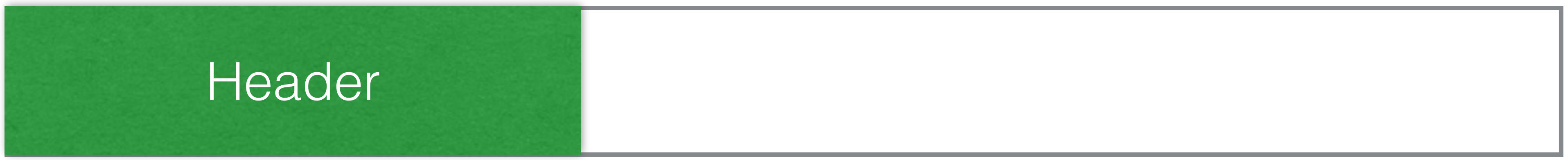
Requirements

- Should not leak the total number of files initially indexed
- Should not leak the file sizes of the files initially indexed

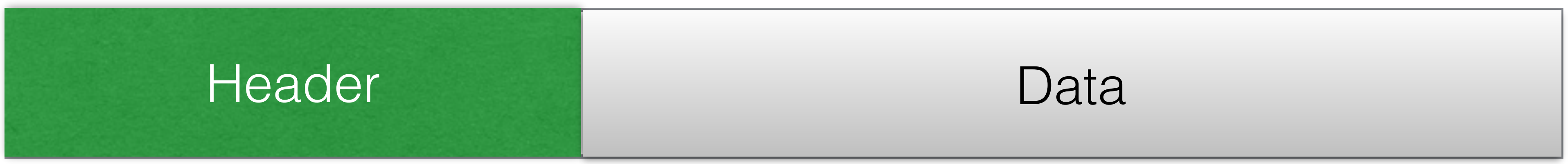
Block format

Block format

Block format



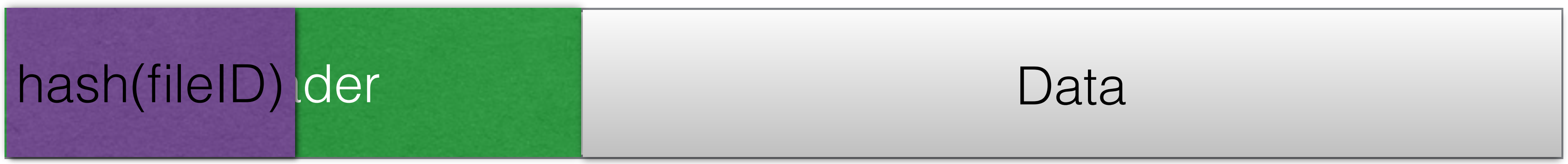
Block format



Header

Data

Block format

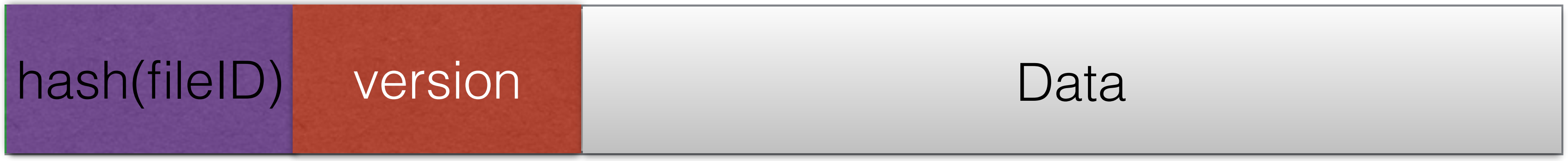


hash(fileID)

der

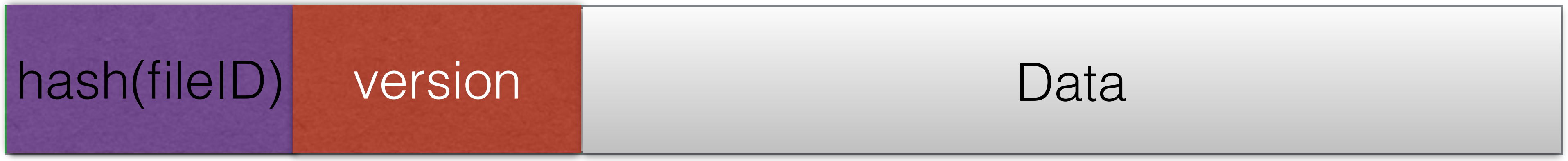
Data

Block format



hash(fileID) version Data

Block format



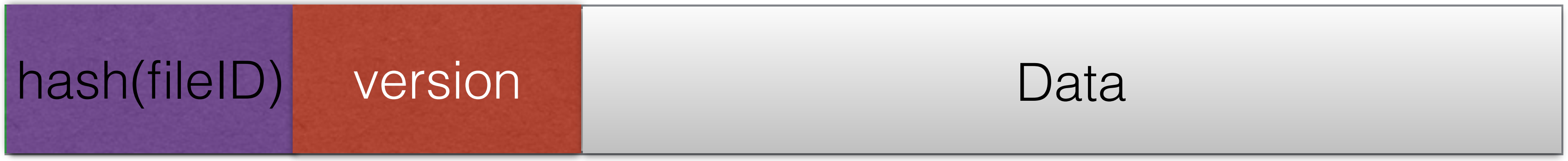
hash(fileID)

version

Data

First block of a file

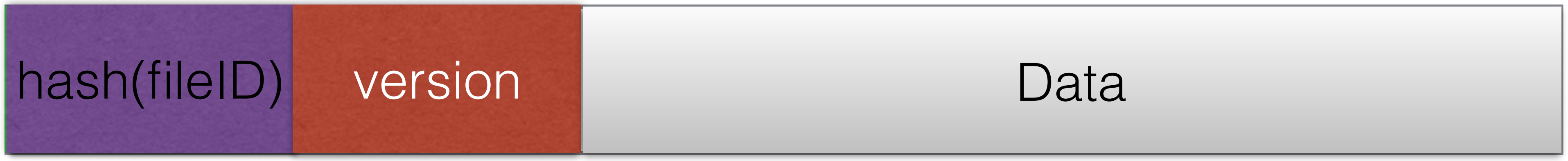
Block format



hash(fileID) version Data

First block of a file

Block format

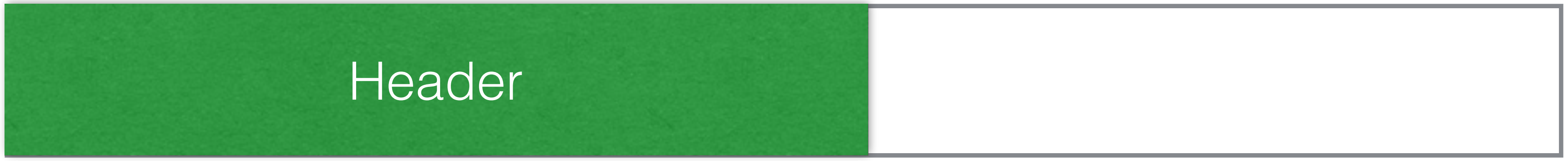


hash(fileID)

version

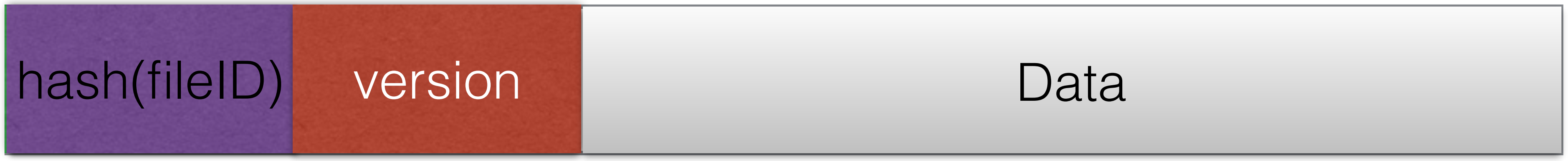
Data

First block of a file



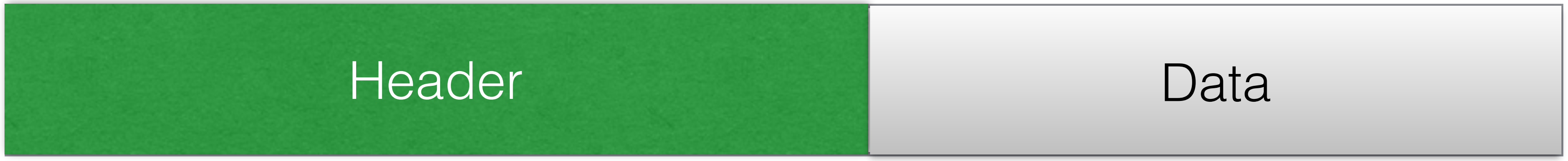
Header

Block format



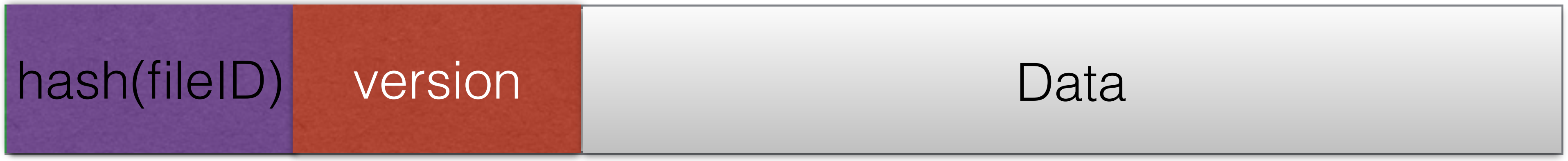
hash(fileID) | version | Data

First block of a file



Header | Data

Block format

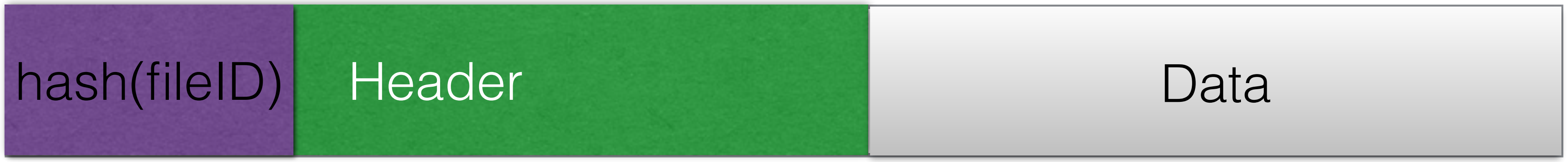


hash(fileID)

version

Data

First block of a file

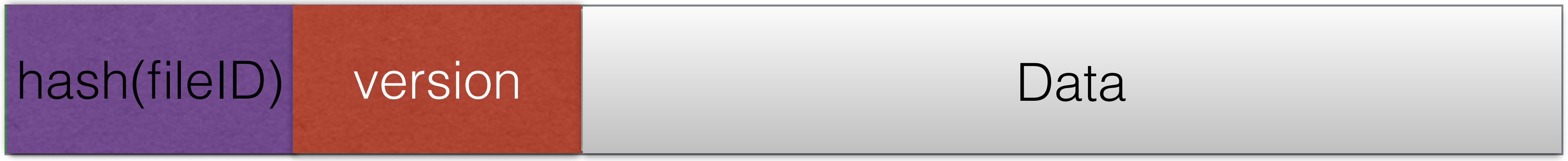


hash(fileID)

Header

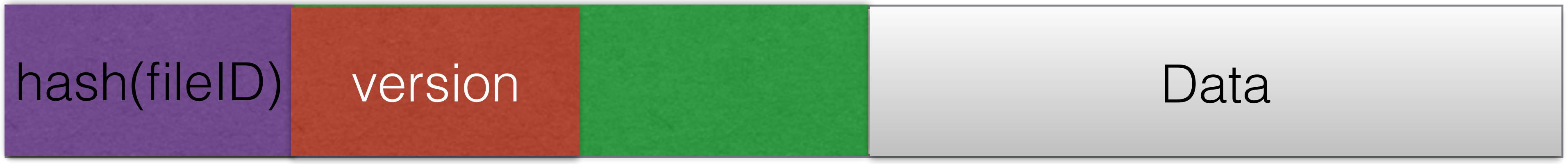
Data

Block format



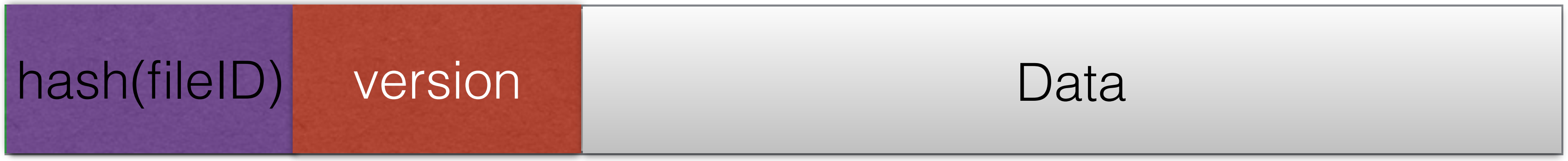
hash(fileID) version Data

First block of a file

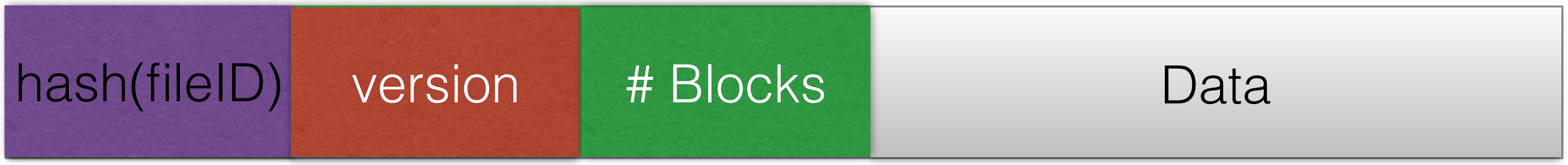


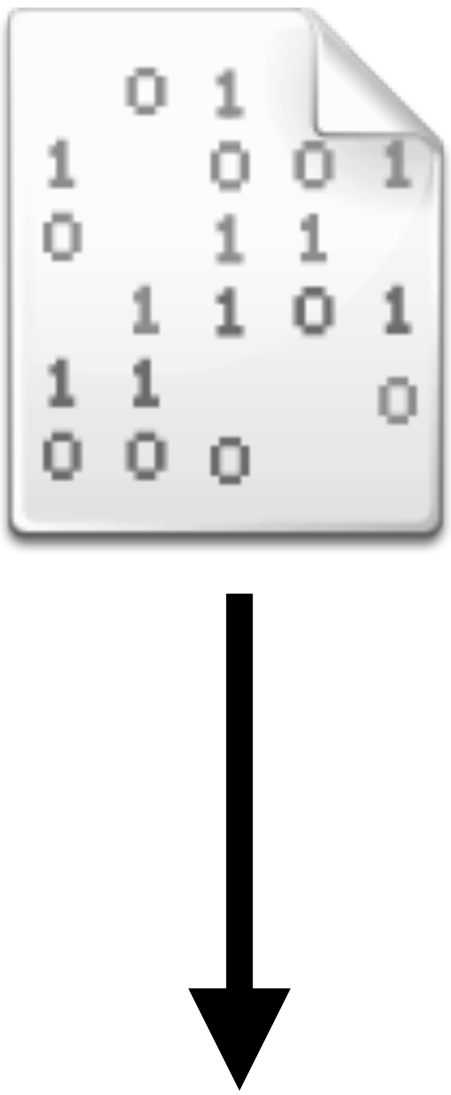
hash(fileID) version Data

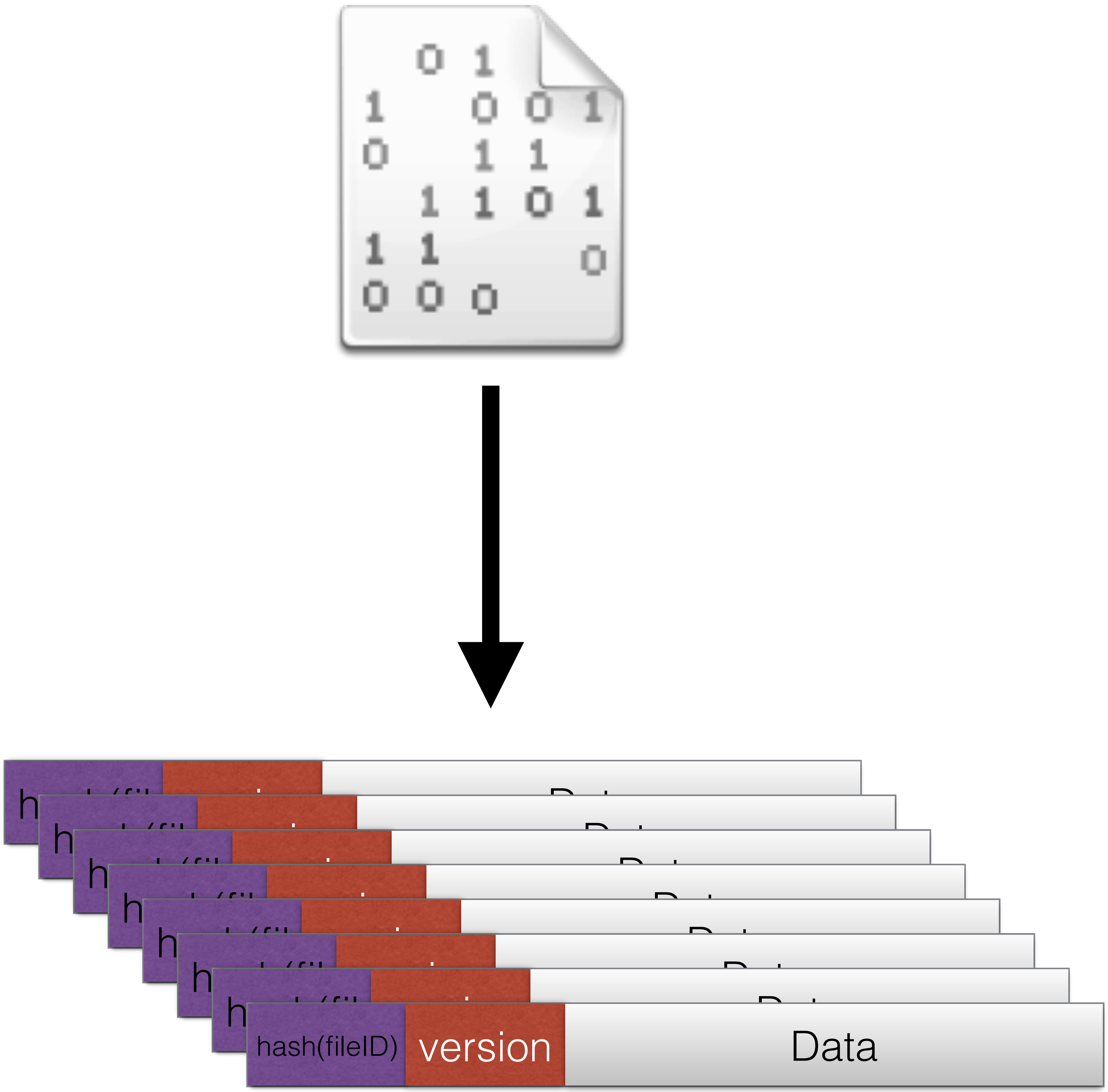
Block format



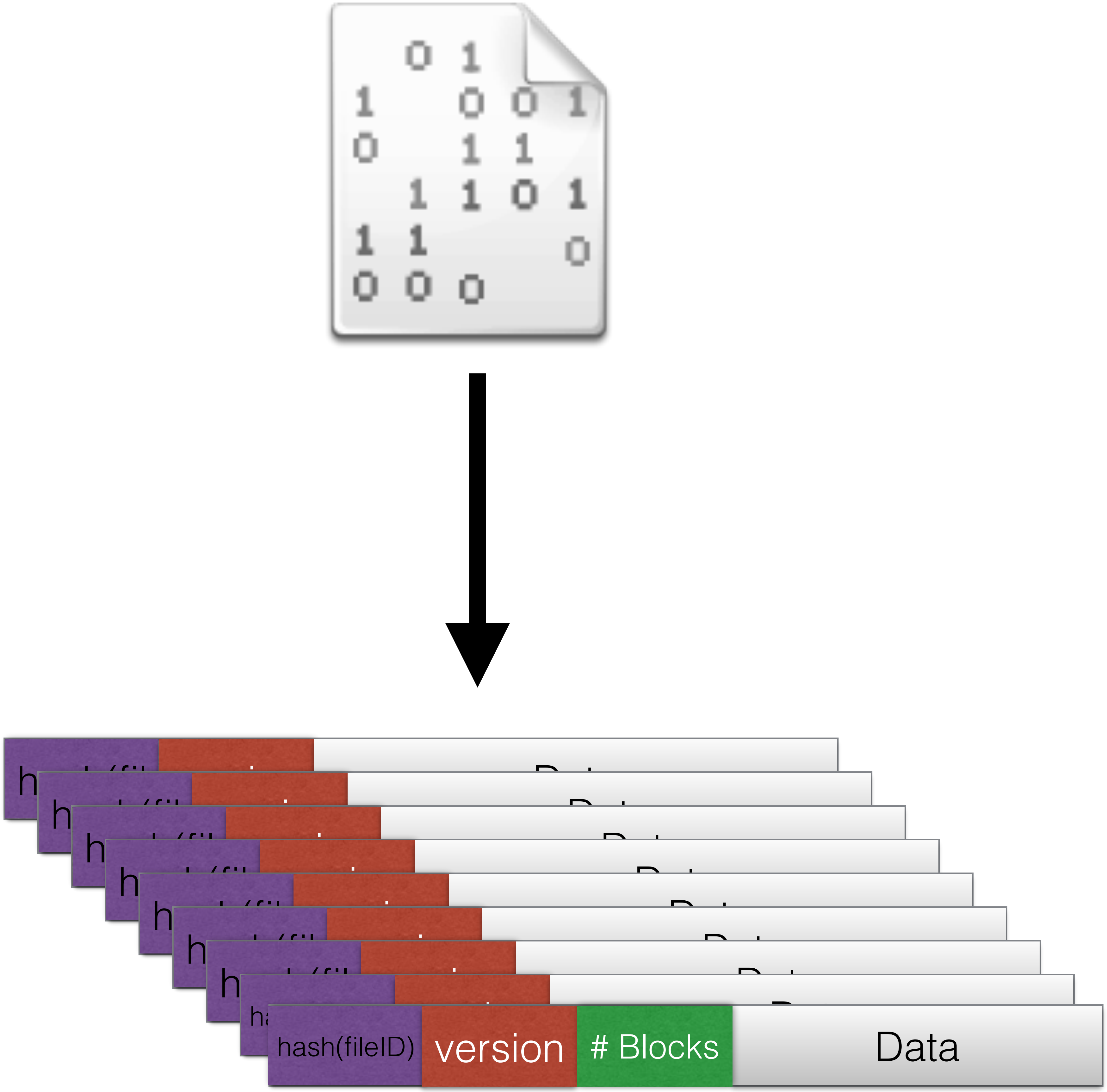
First block of a file



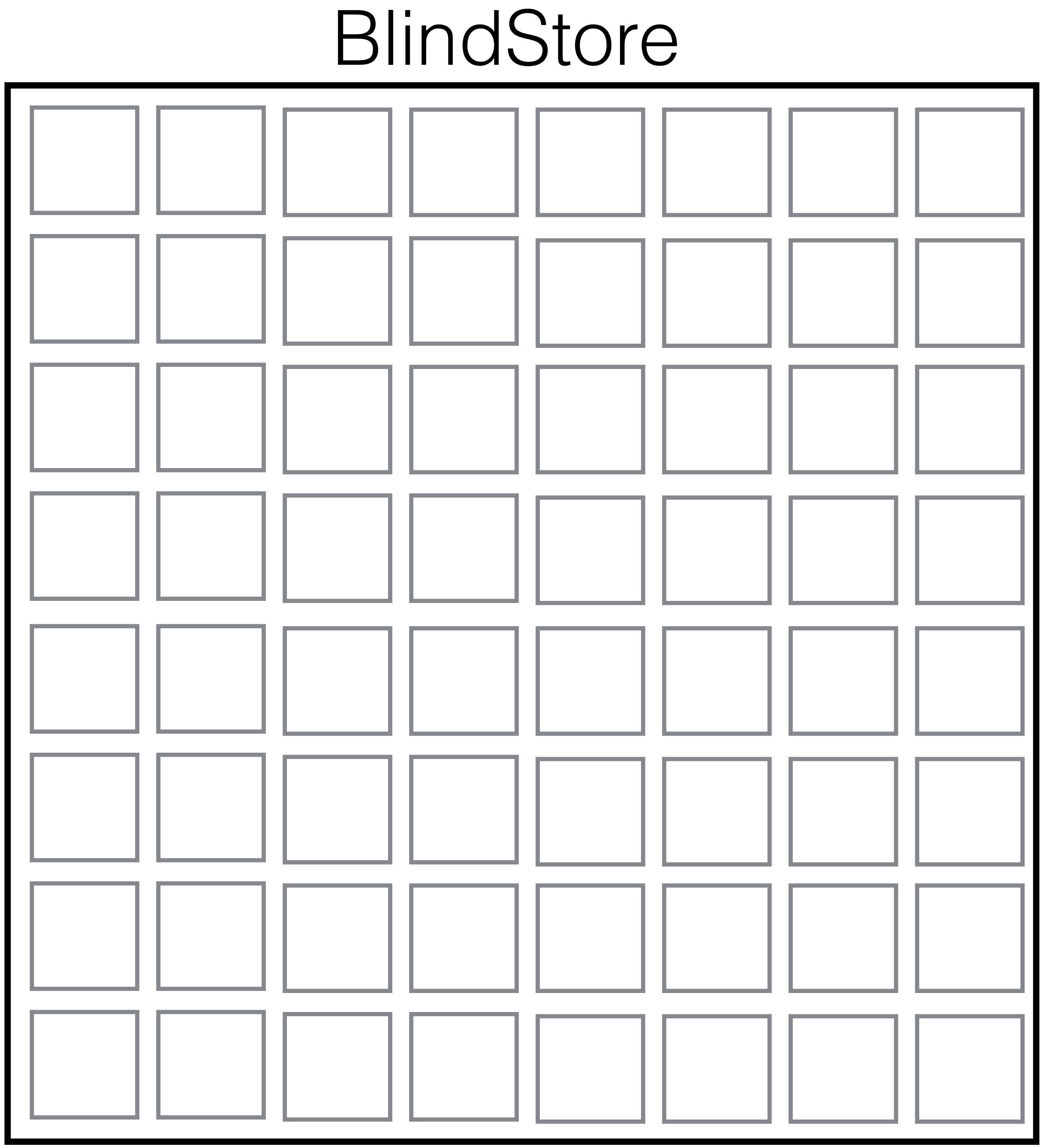




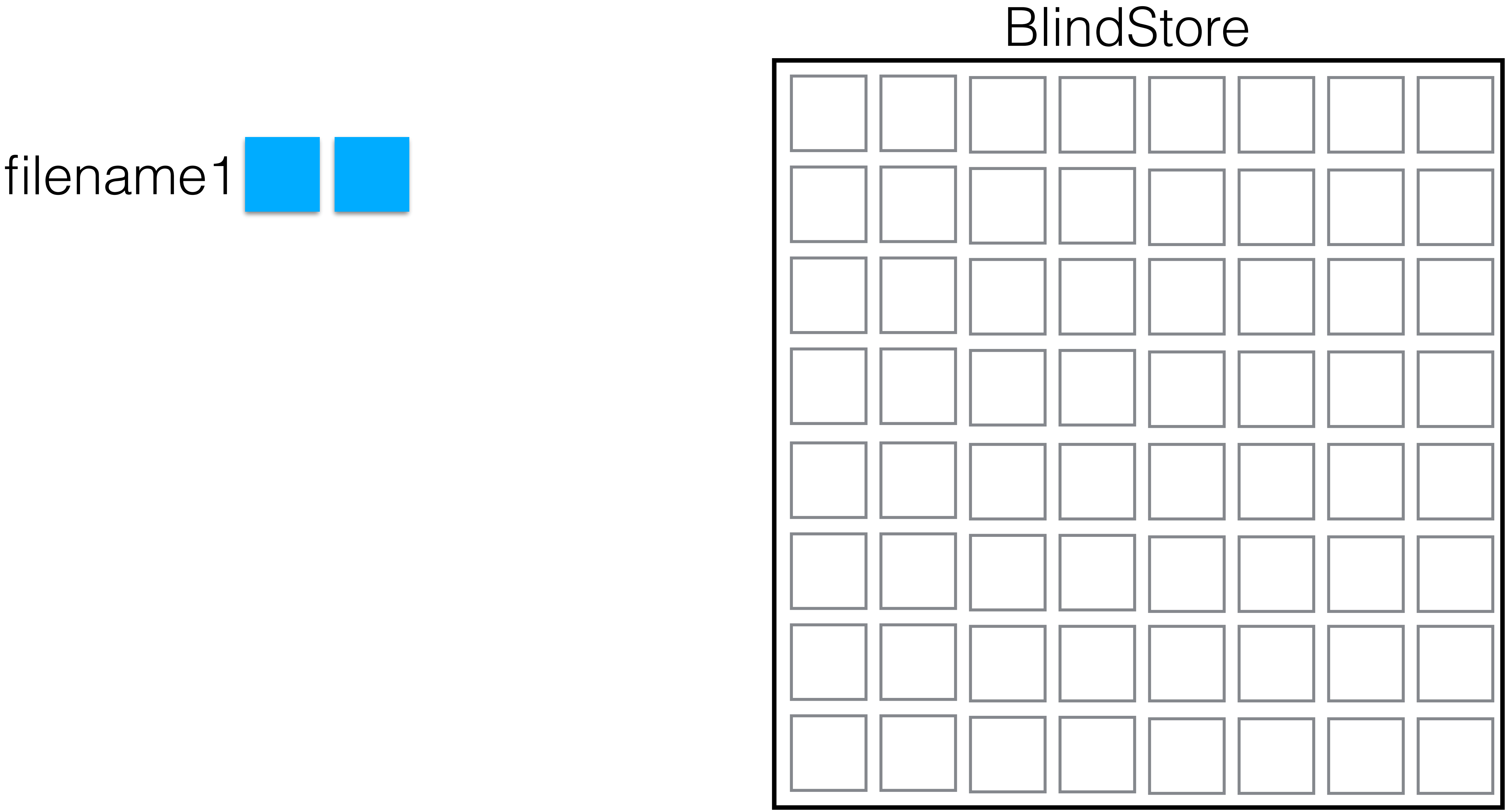
hash(fileID) version Data


hash(fileID)
version
# Blocks
Data

Our Scheme (Setup)



Our Scheme (Setup)



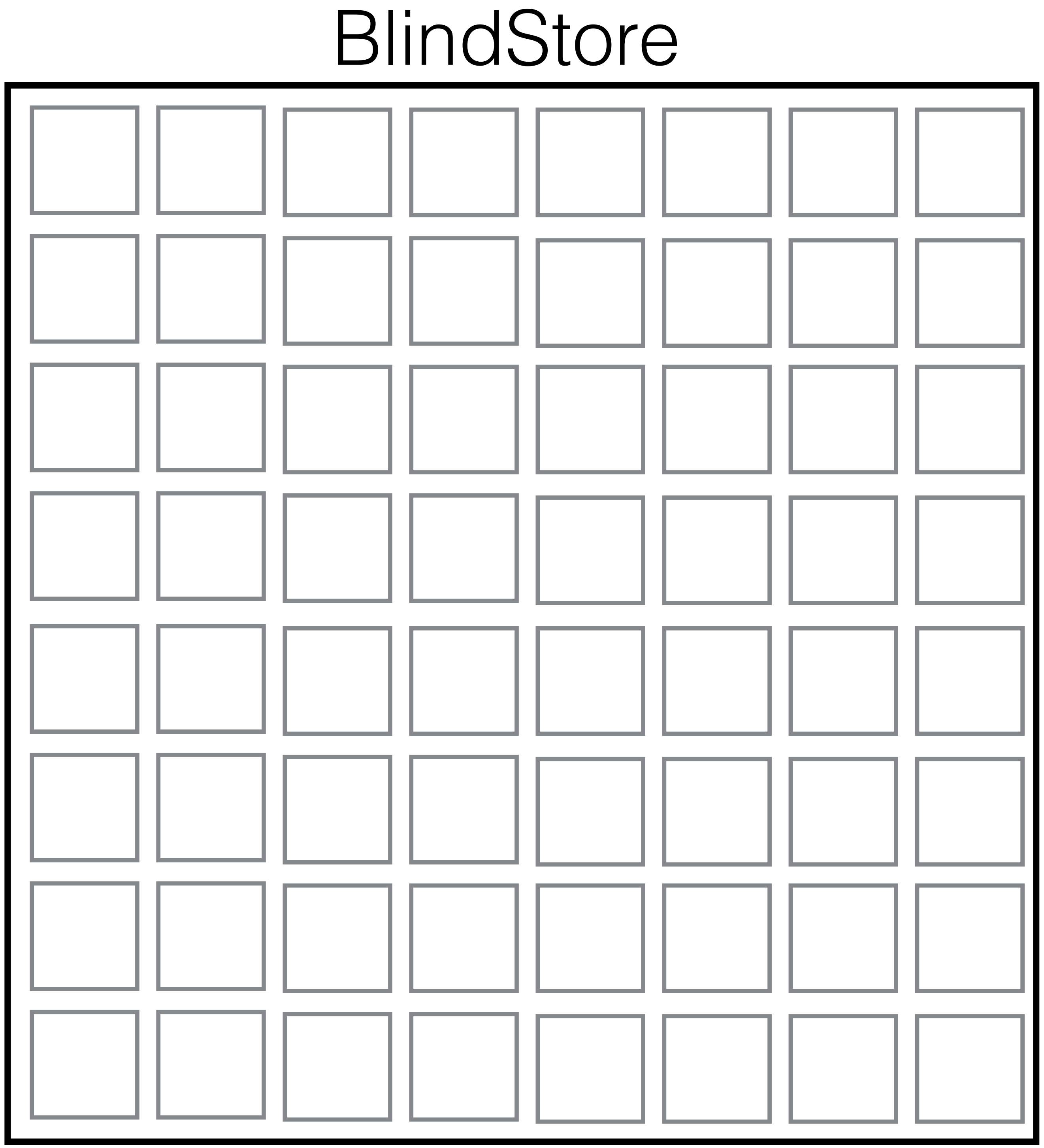
BlindStore

filename1

Our Scheme (Setup)

filename1 🟦 🟦

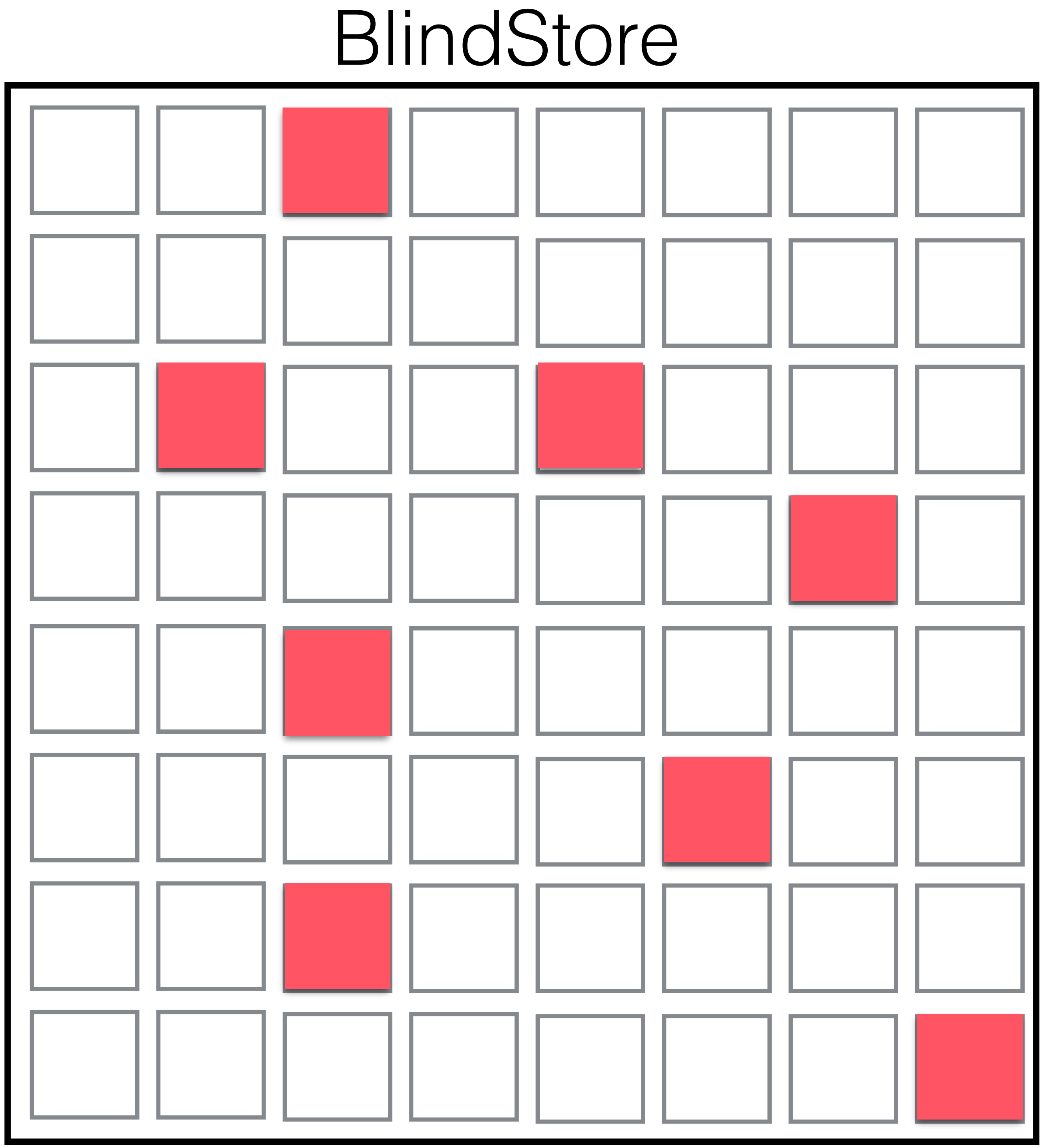
Seed1 = Hash(filename1)



Our Scheme (Setup)

filename1 🟦 🟦

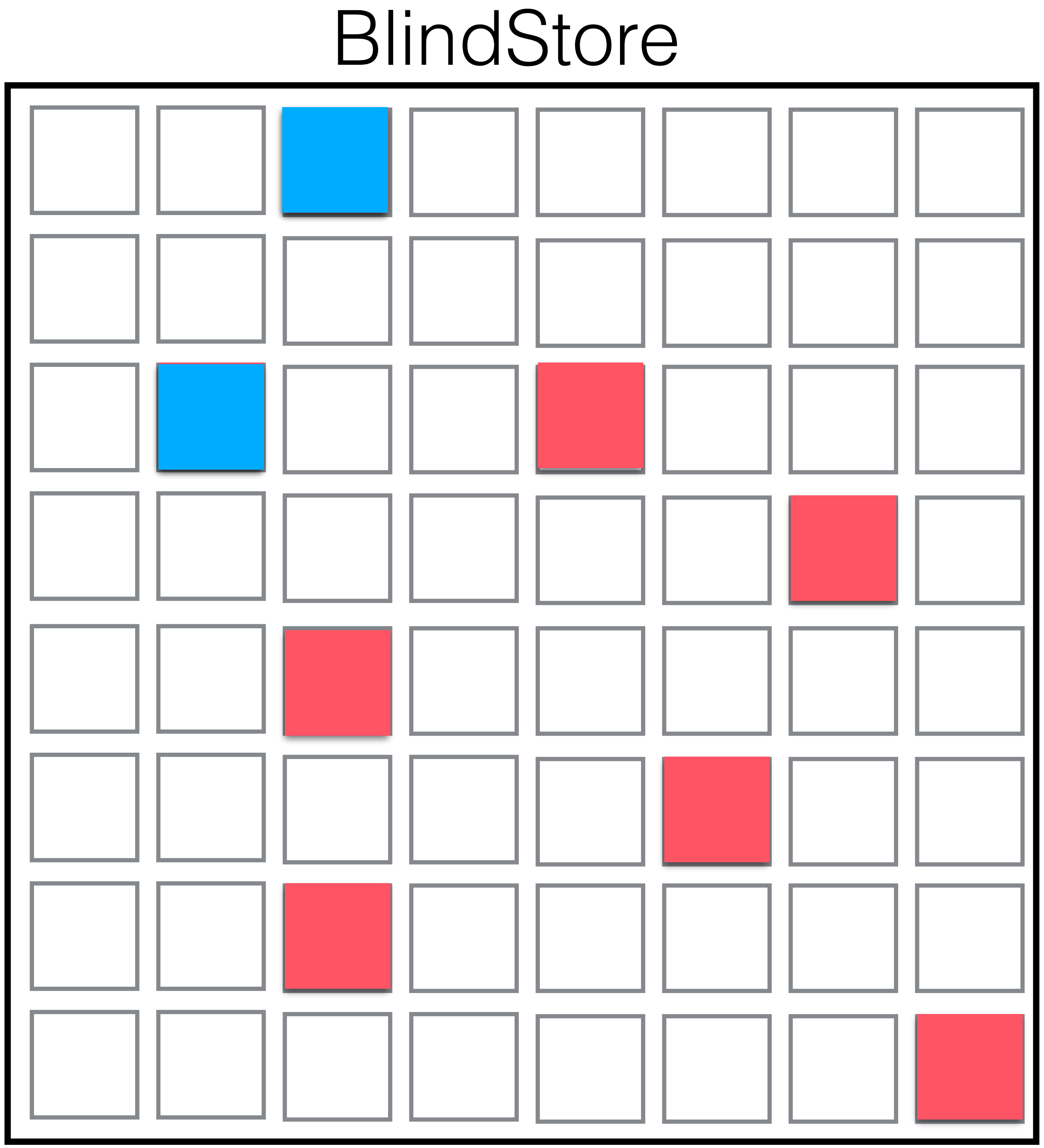
Seed1 = Hash(filename1)



Our Scheme (Setup)

filename1

Seed1 = Hash(filename1)

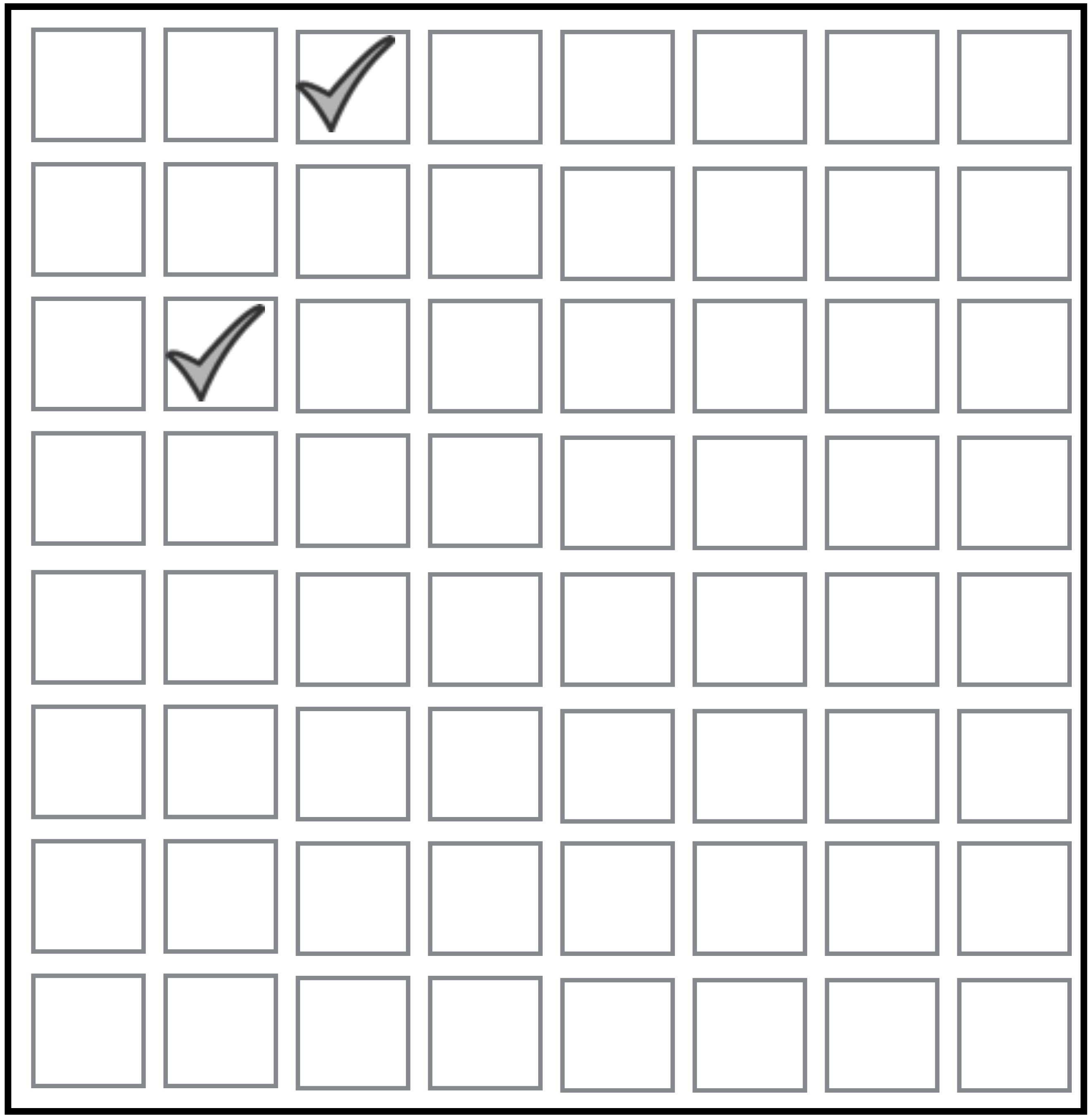


Our Scheme (Setup)

filename1

Seed1 = Hash(filename1)

BlindStore

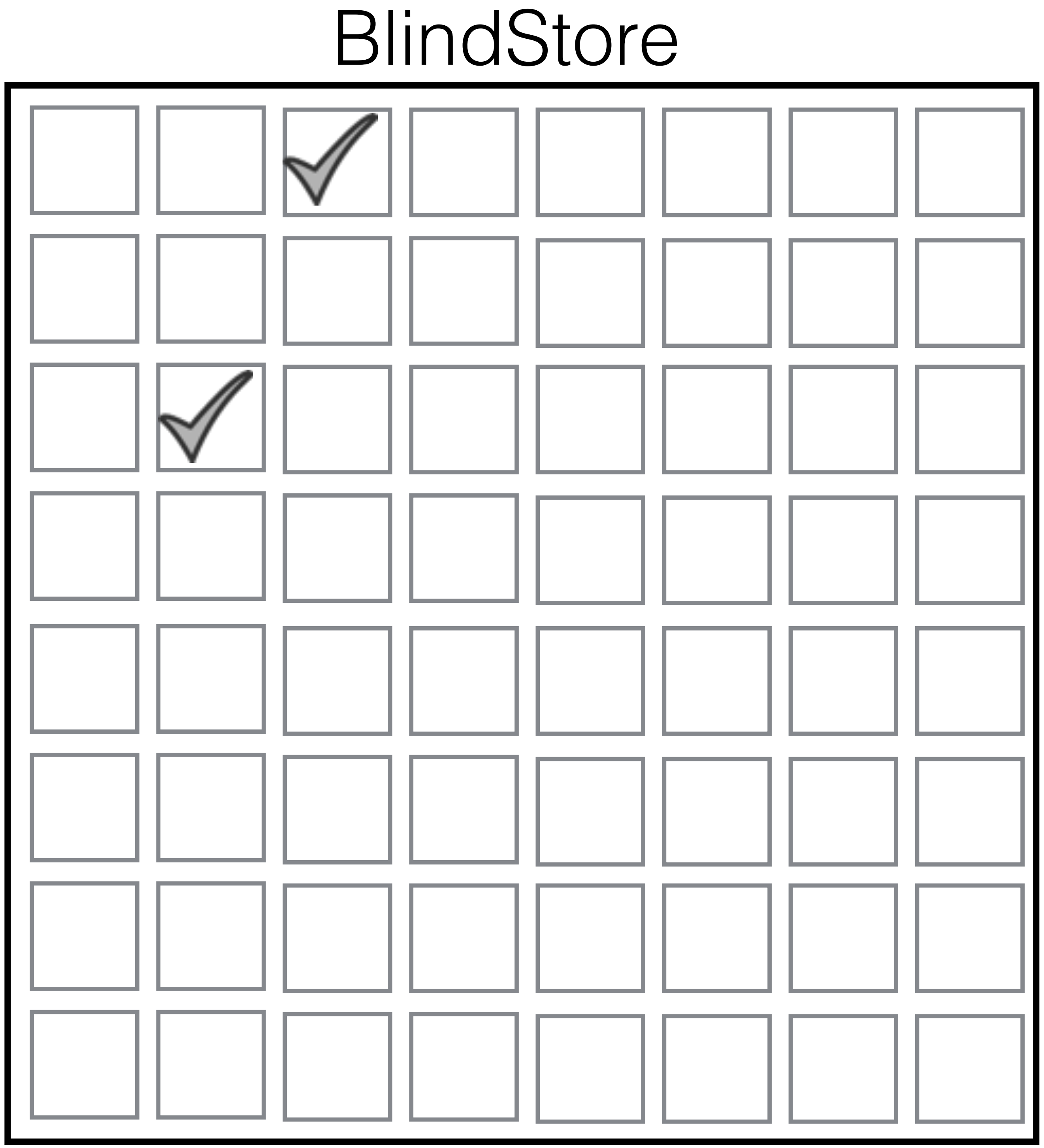


Our Scheme (Setup)

filename1

filename2 🟦 🟦

Seed1 = Hash(filename1)



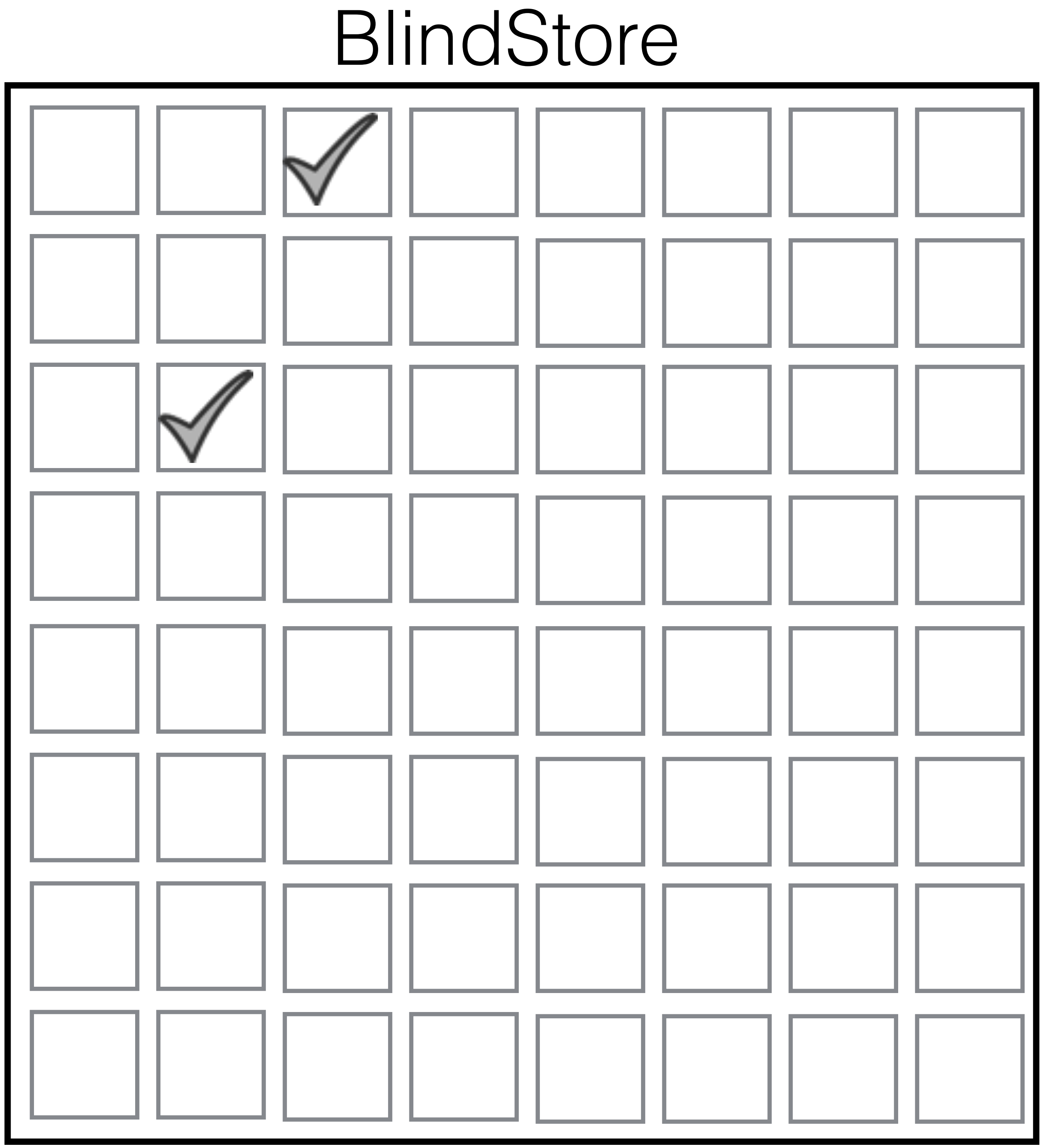
Our Scheme (Setup)

filename1

filename2 🟦 🟦

Seed1 = Hash(filename1)

Seed2 = Hash(filename2)



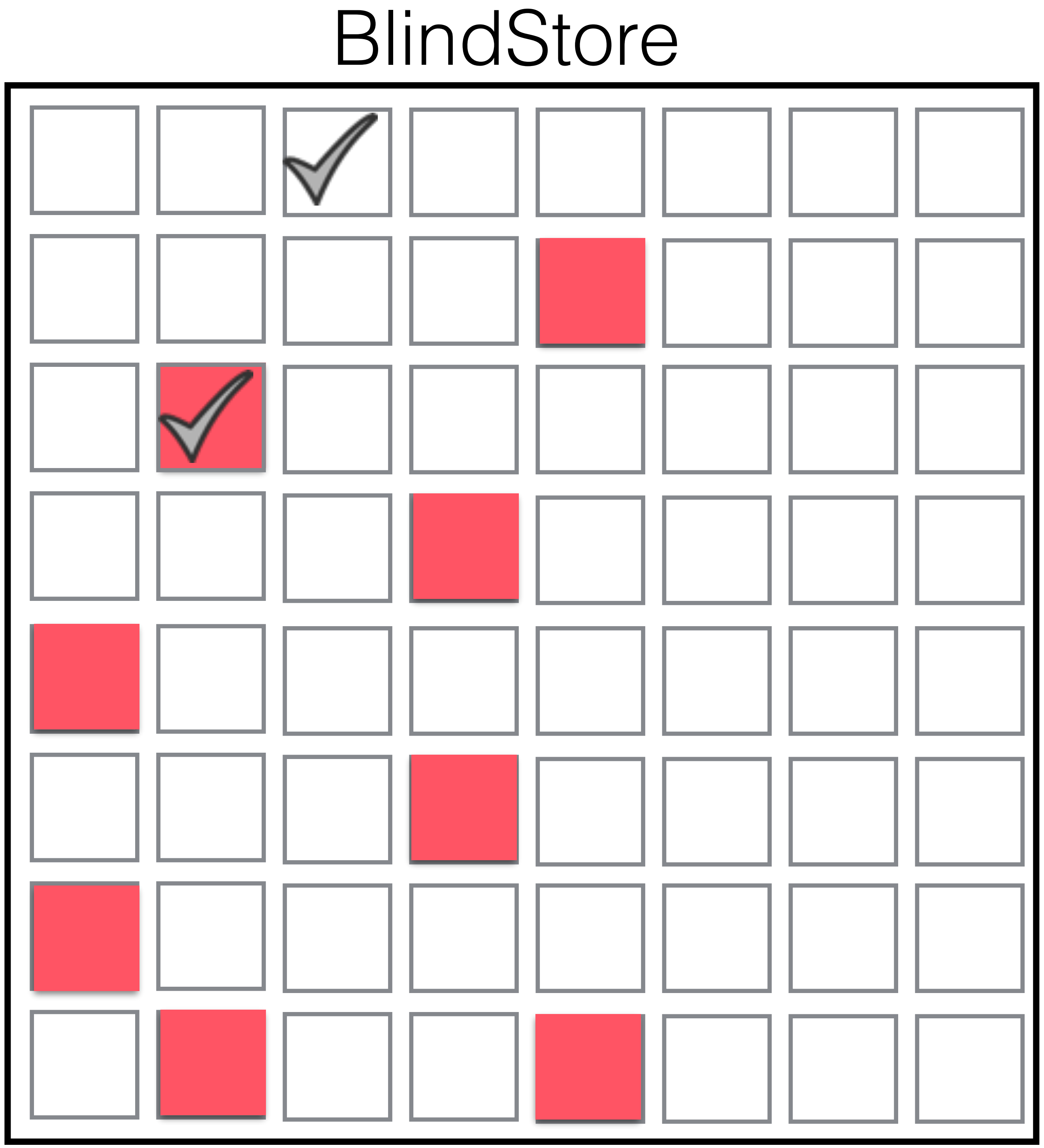
Our Scheme (Setup)

filename1

filename2 🟦 🟦

Seed1 = Hash(filename1)

Seed2 = Hash(filename2)



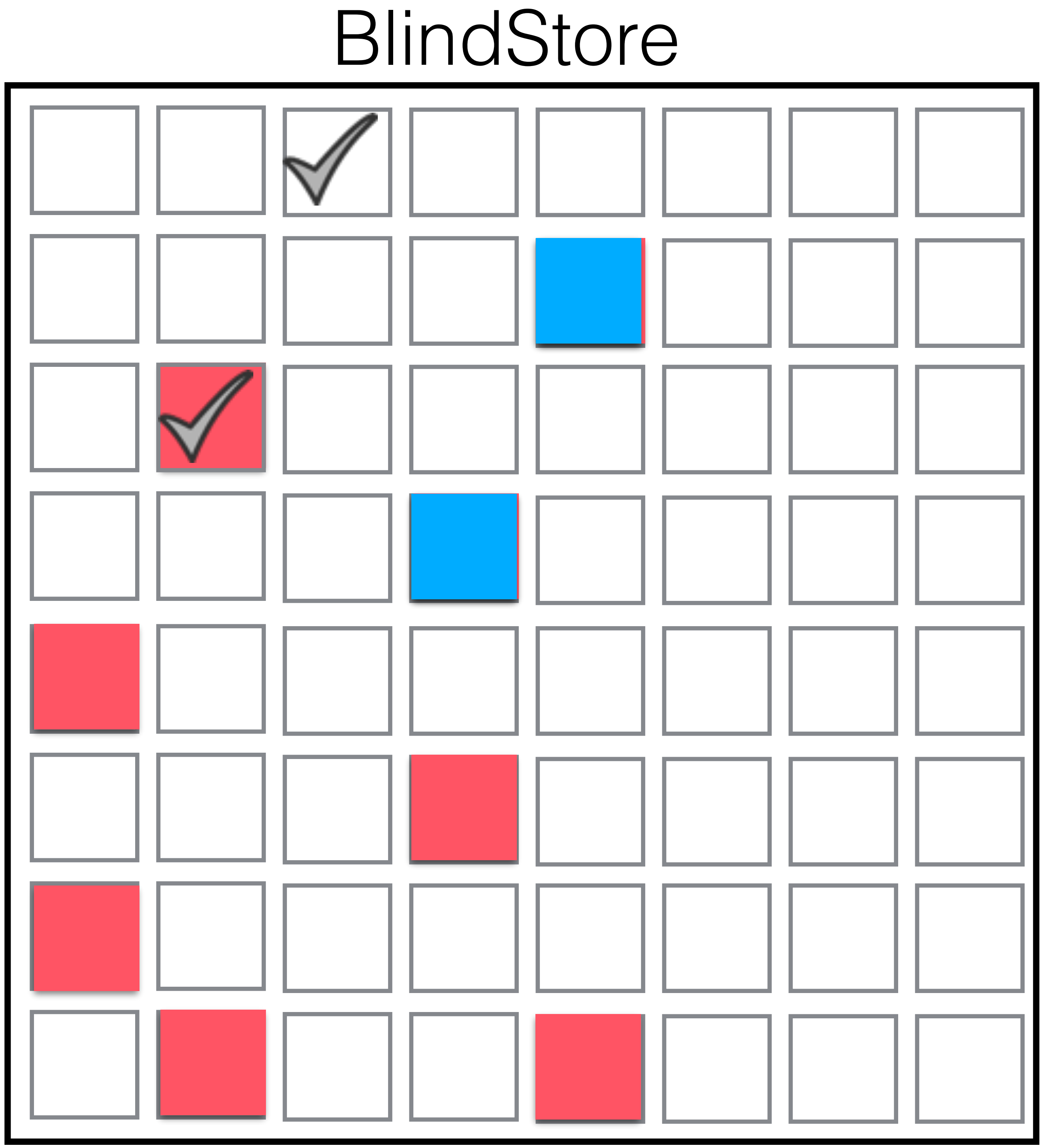
Our Scheme (Setup)

filename1

filename2

Seed1 = Hash(filename1)

Seed2 = Hash(filename2)



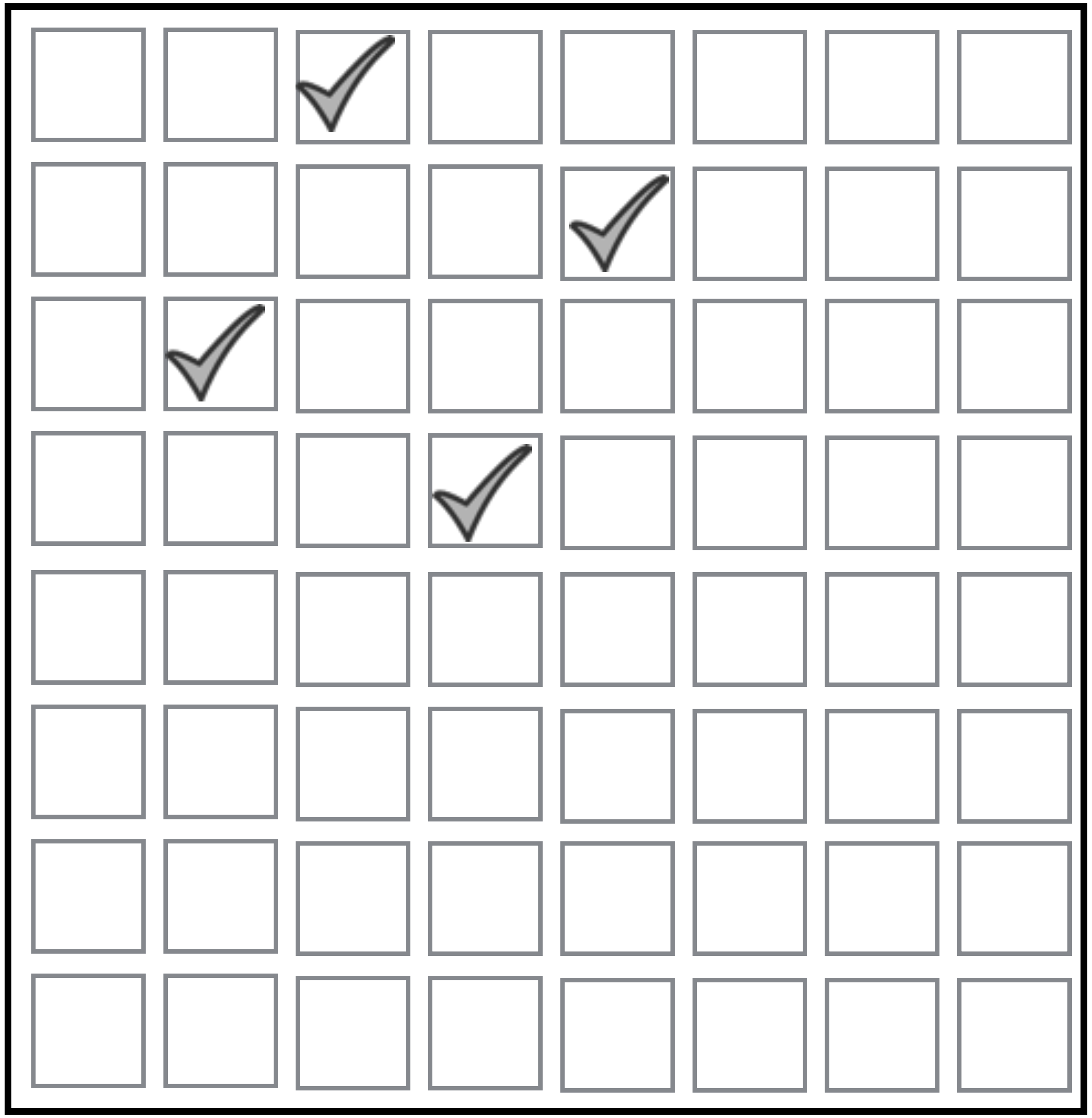
Our Scheme (Setup)

filename1

filename2

Seed1 = Hash(filename1)

Seed2 = Hash(filename2)


BlindStore

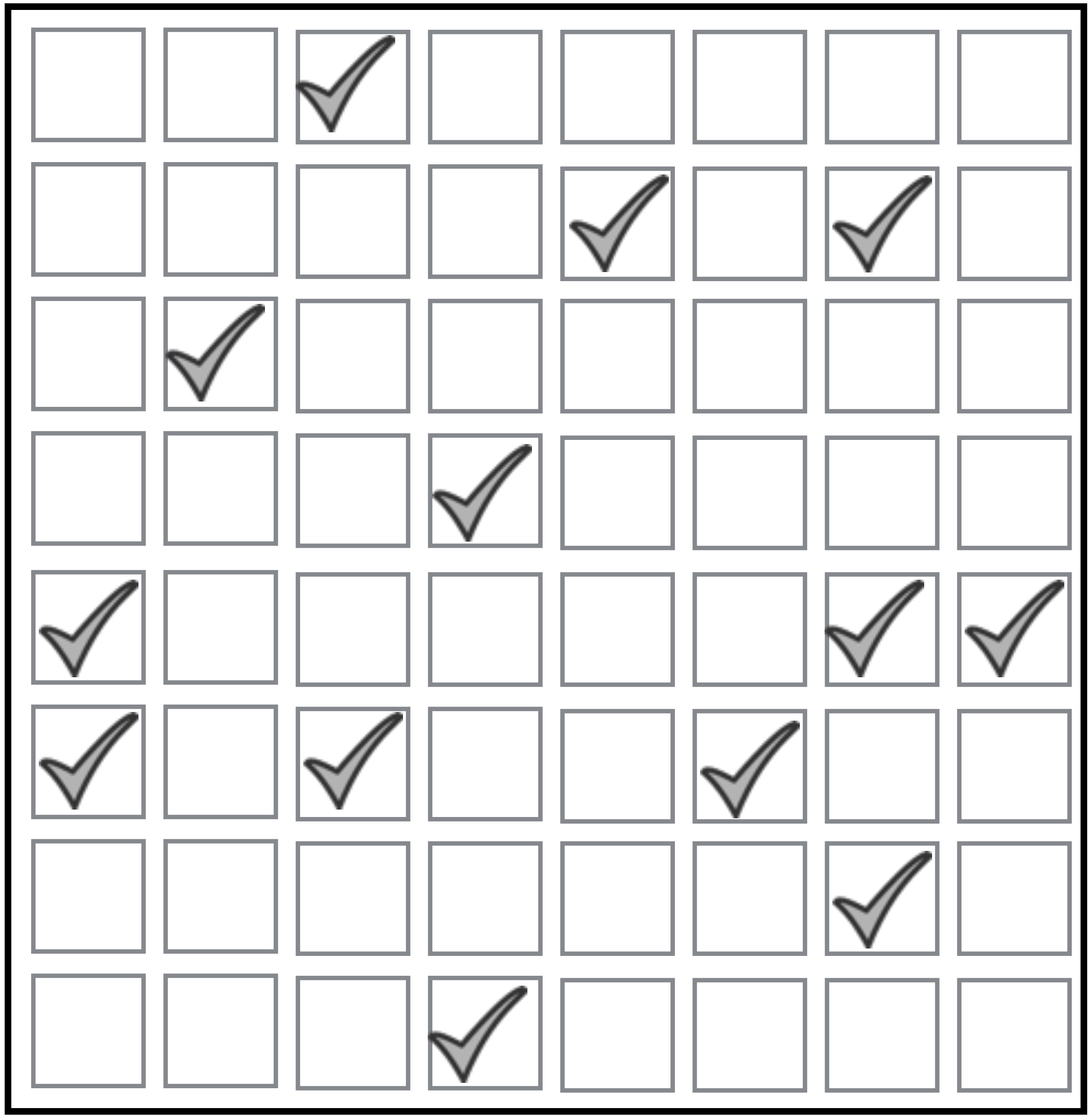
Our Scheme (Setup)

filename1

filename2

Seed1 = Hash(filename1)
Seed2 = Hash(filename2)

BlindStore



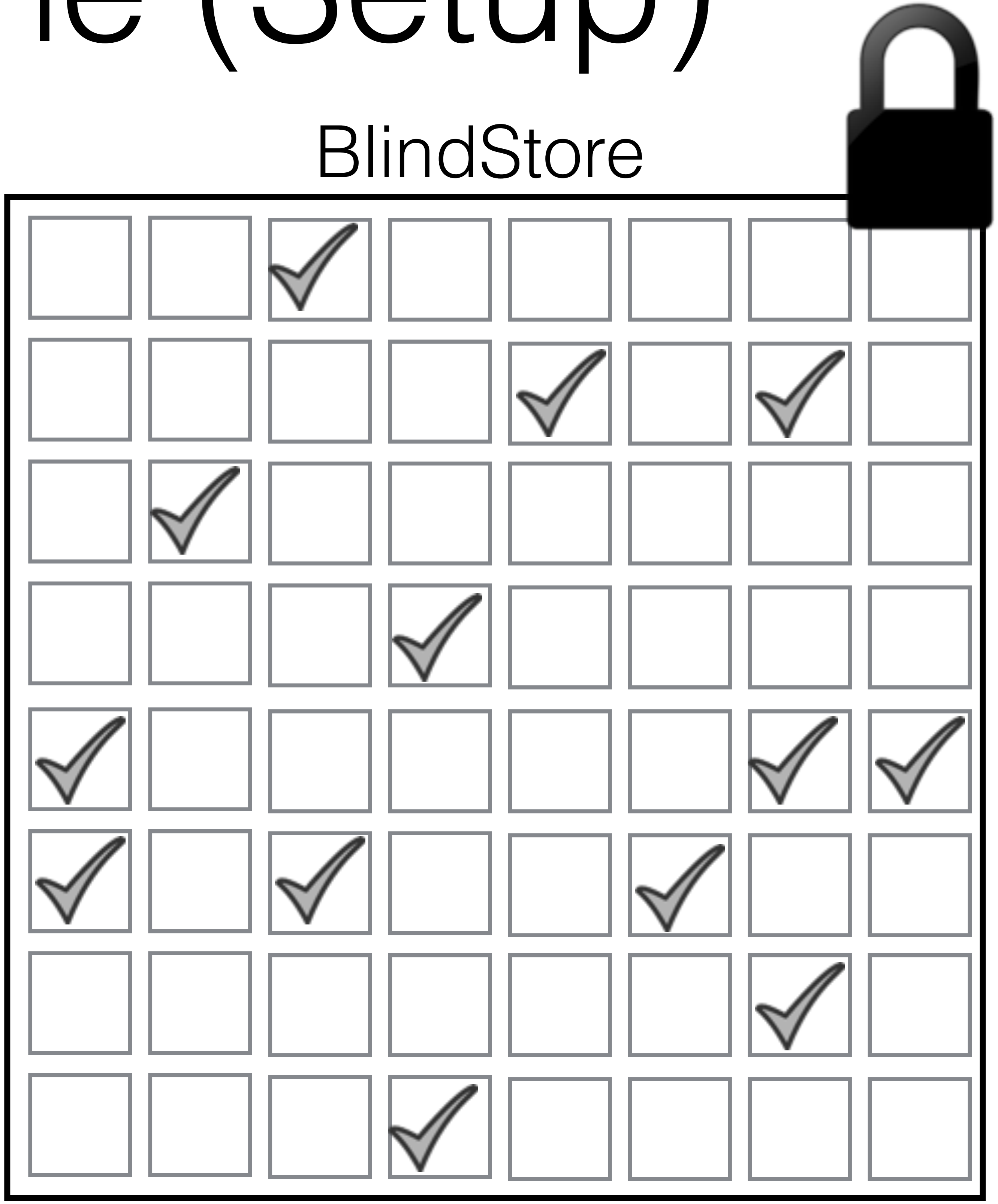
Our Scheme (Setup)

filename1

filename2

Seed1 = Hash(filename1)

Seed2 = Hash(filename2)



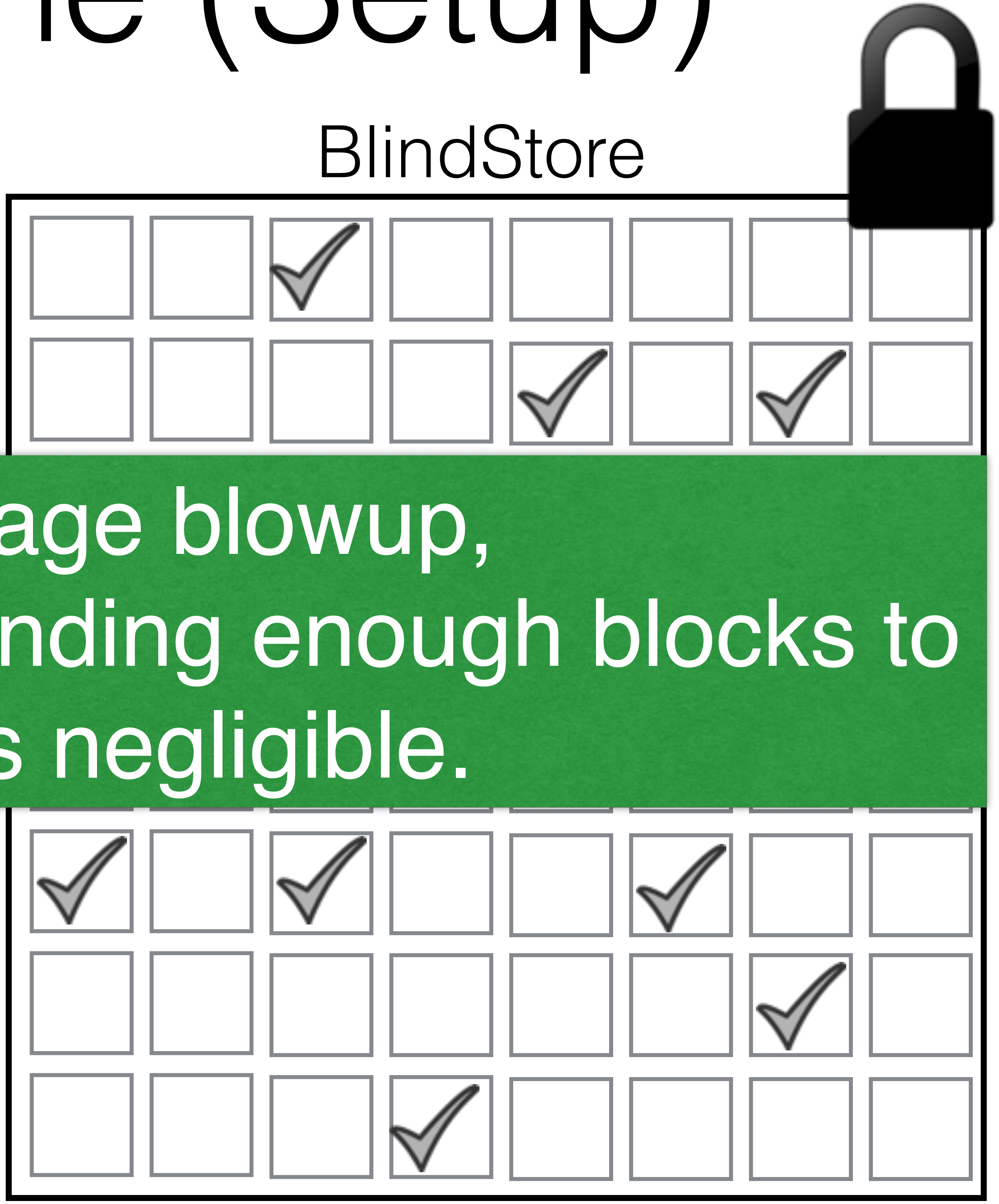
Our Scheme (Setup)

filename1

With 4X storage blowup,
the probability of NOT finding enough blocks to store a file is negligible.

Seed2 = Hash(filename2)

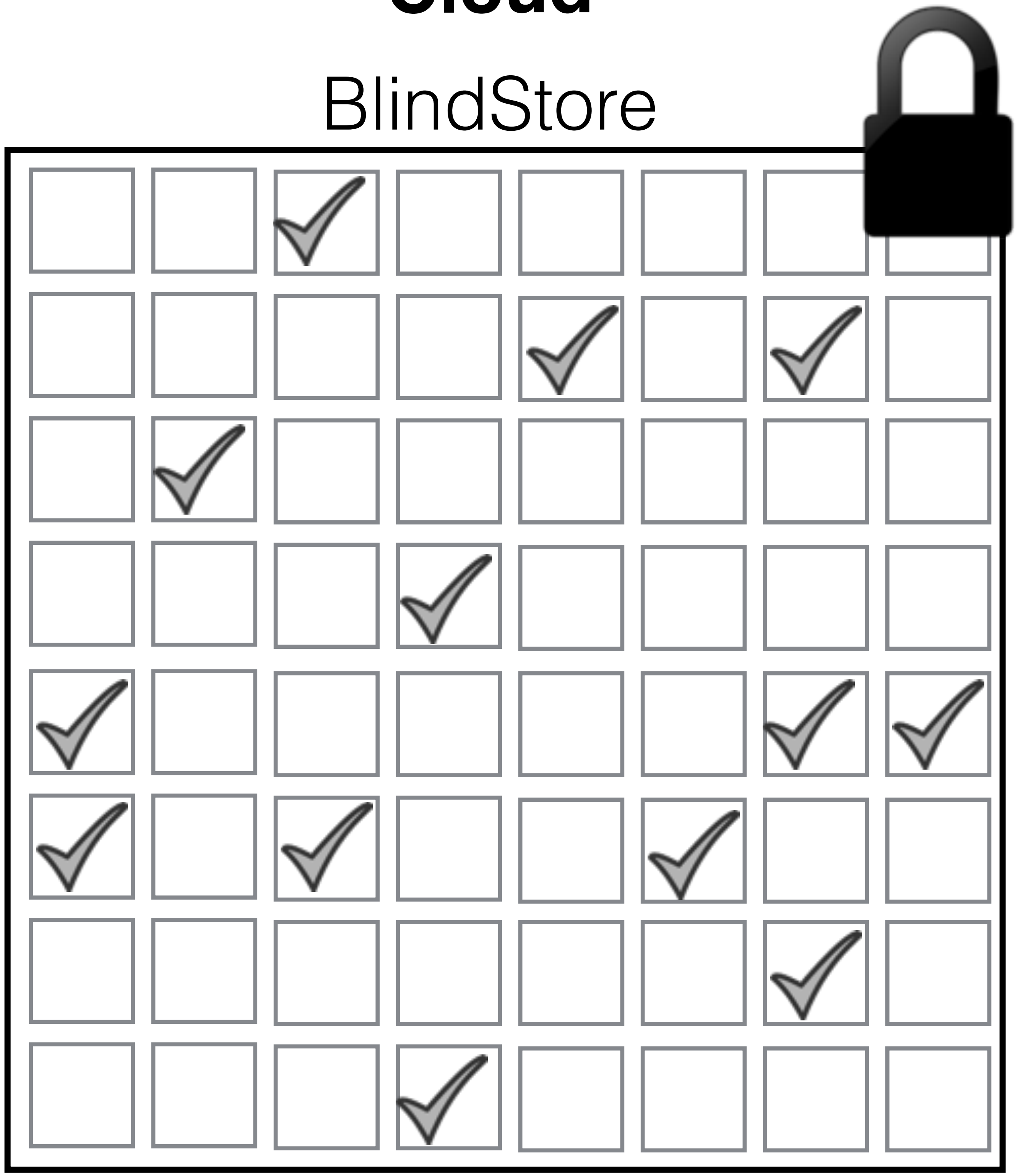
BlindStore



Access

Client

Cloud



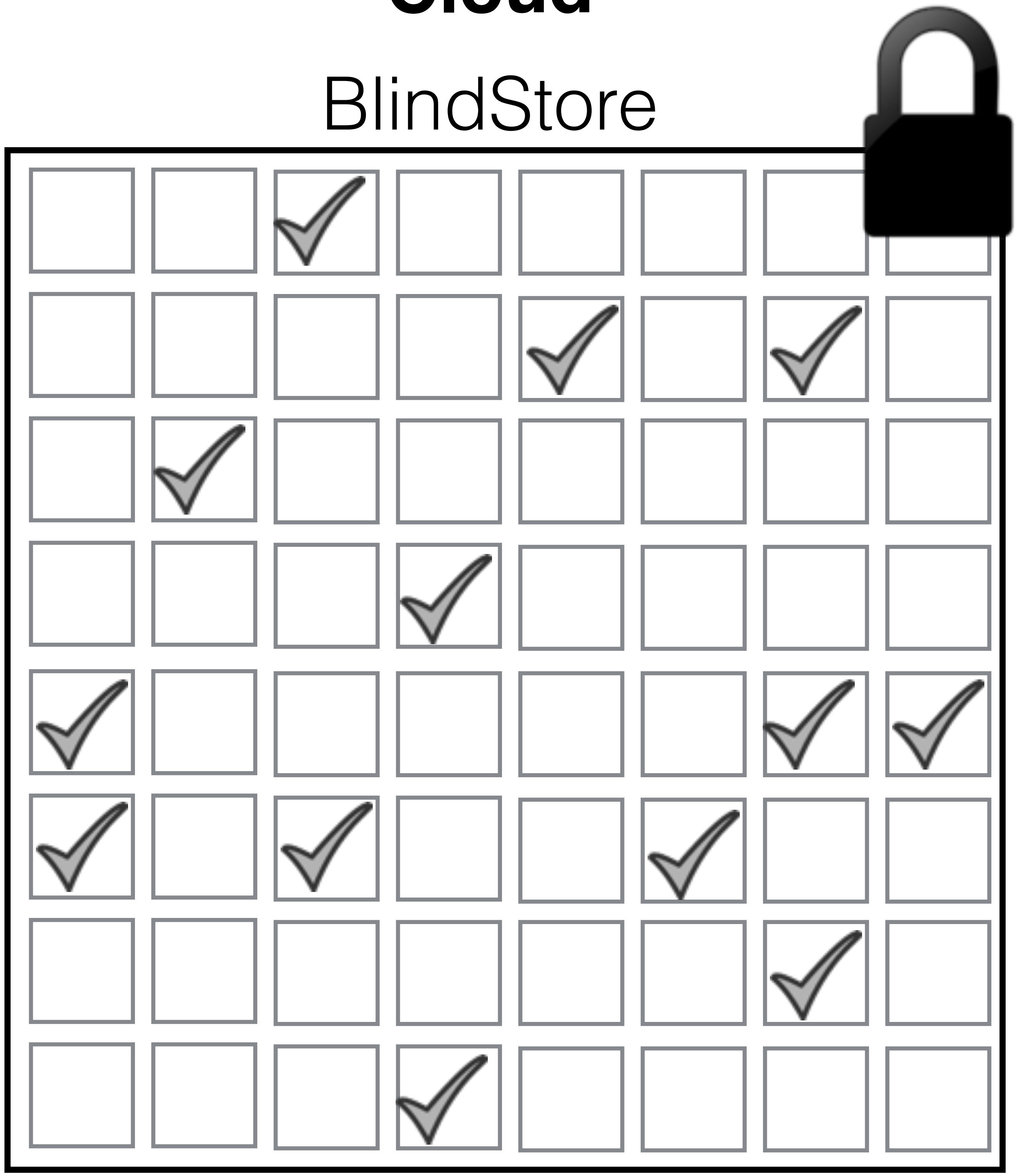
Access

Client

Access filename2

Cloud

BlindStore



		✓					
				✓		✓	
	✓						
			✓				
✓						✓	✓
✓		✓			✓		
						✓	
			✓				

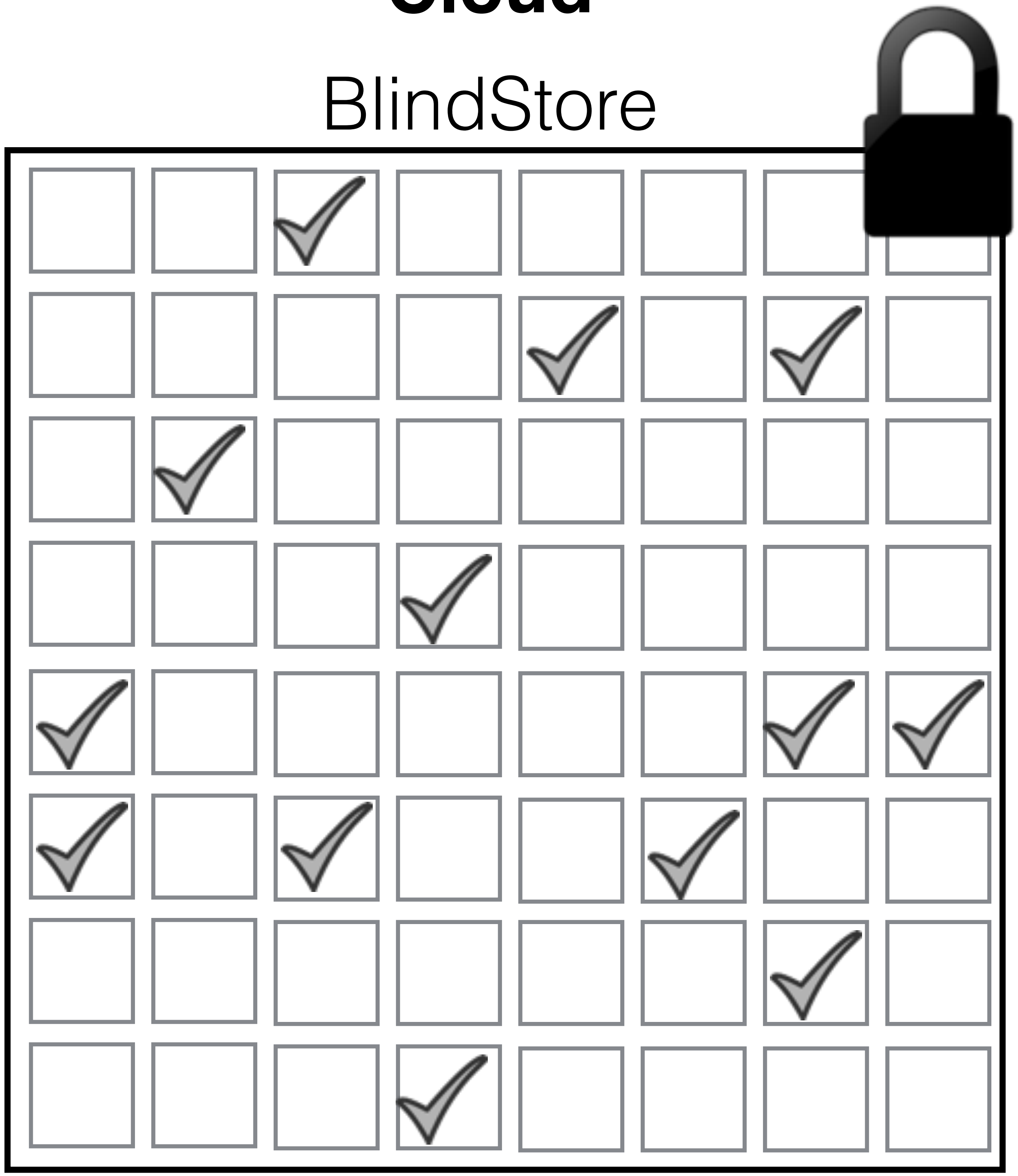
Access

Client

Access filename2

Seed2 = Hash(filename2)

Cloud



		✓					
				✓		✓	
	✓						
			✓				
✓						✓	✓
✓		✓			✓		
						✓	
			✓				

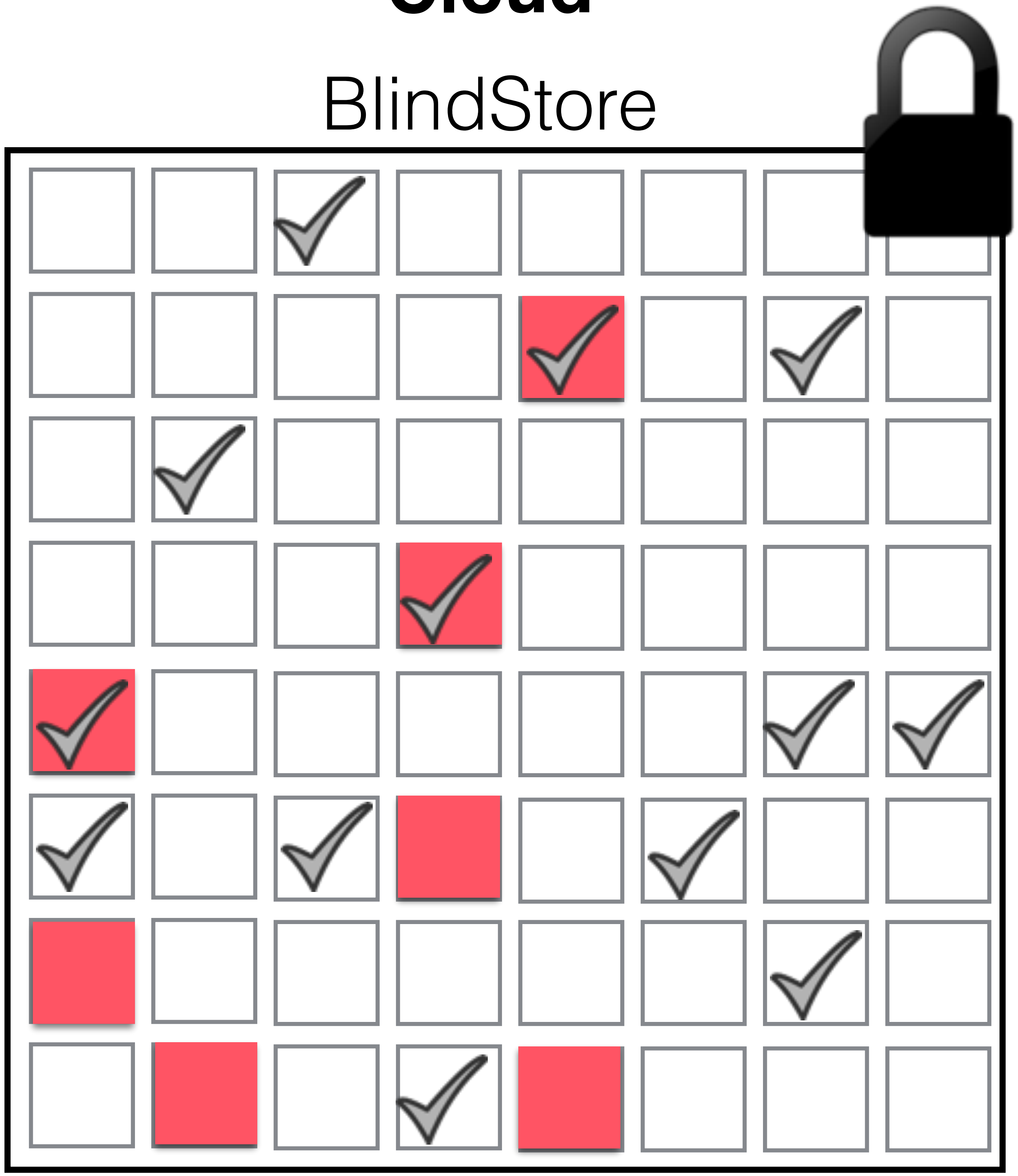
Access

Client

Access filename2

Seed2 = Hash(filename2)

Cloud

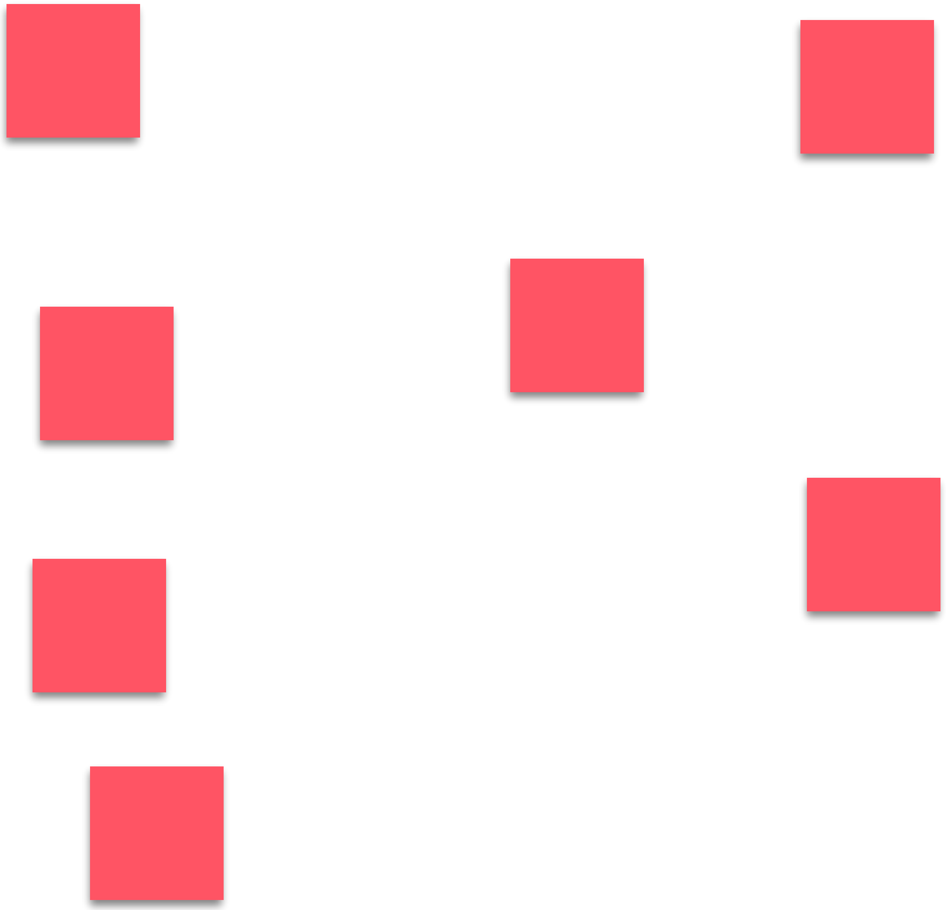


Access

Client

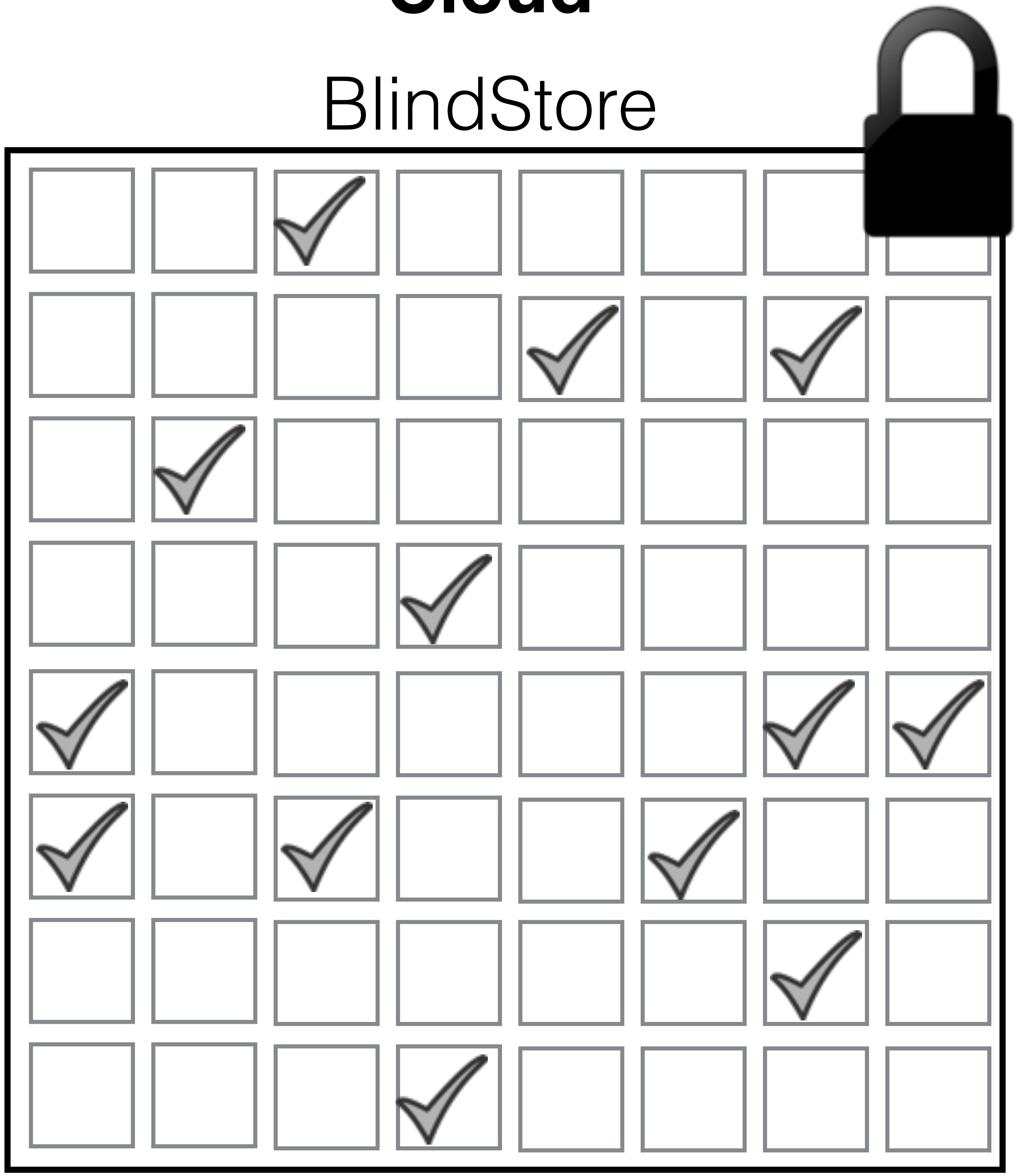
Access filename2

Seed2 = Hash(filename2)



Cloud

BlindStore



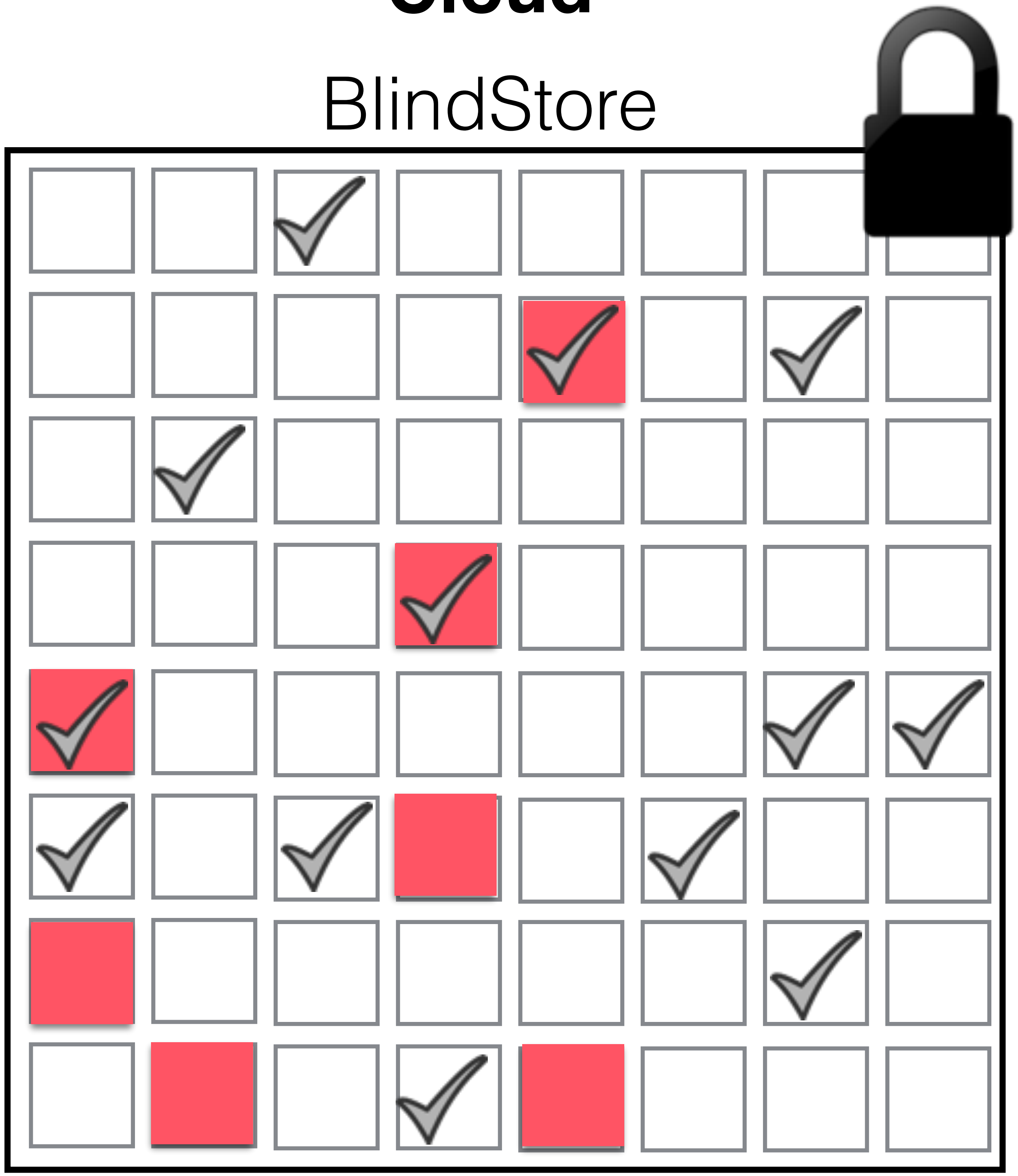
Access

Client

Access filename2

Seed2 = Hash(filename2)

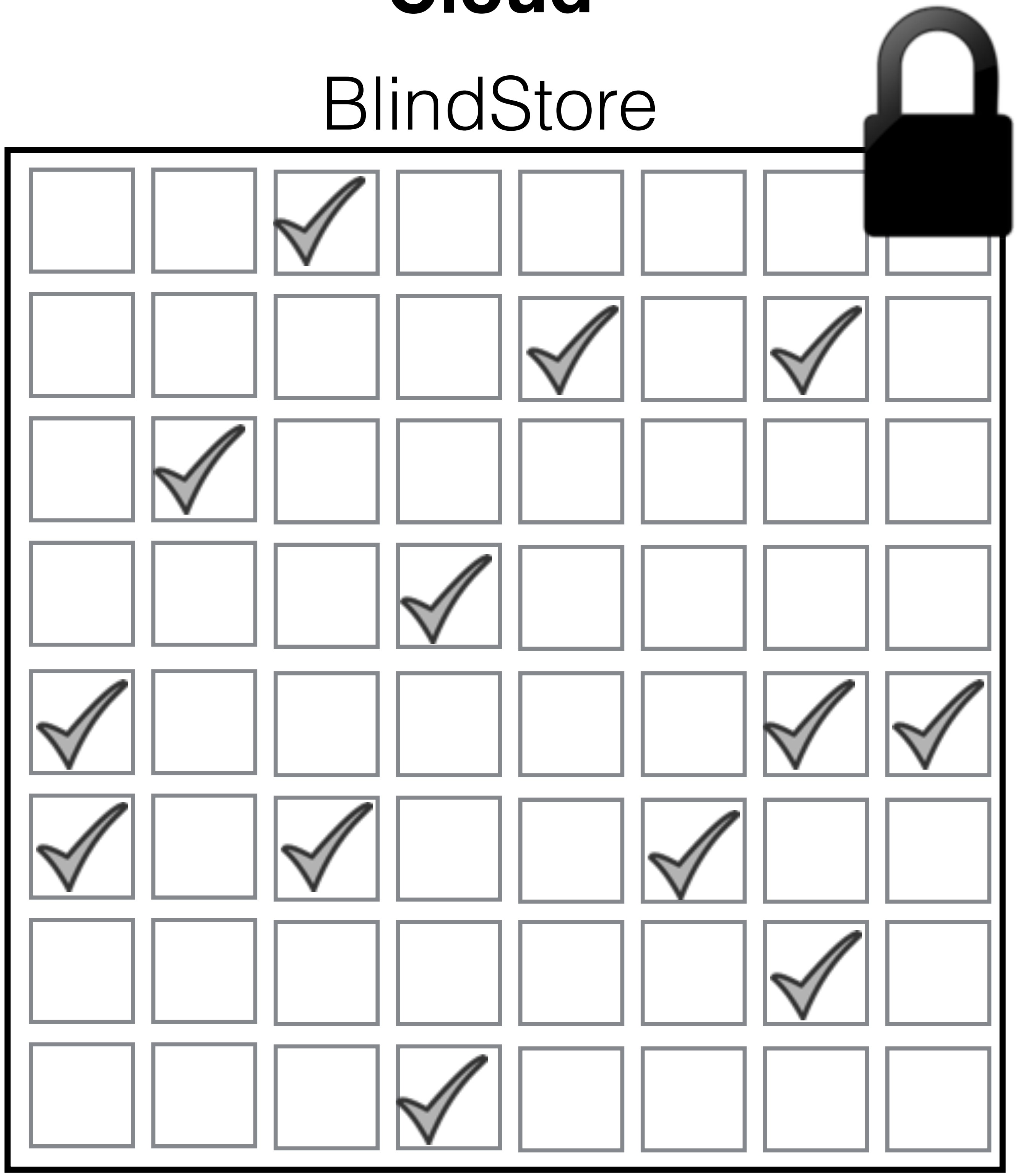
Cloud



Access (with details)

Client

Cloud



BlindStore

		✓					
				✓		✓	
	✓						
			✓				
✓						✓	✓
✓		✓			✓		
						✓	
			✓				

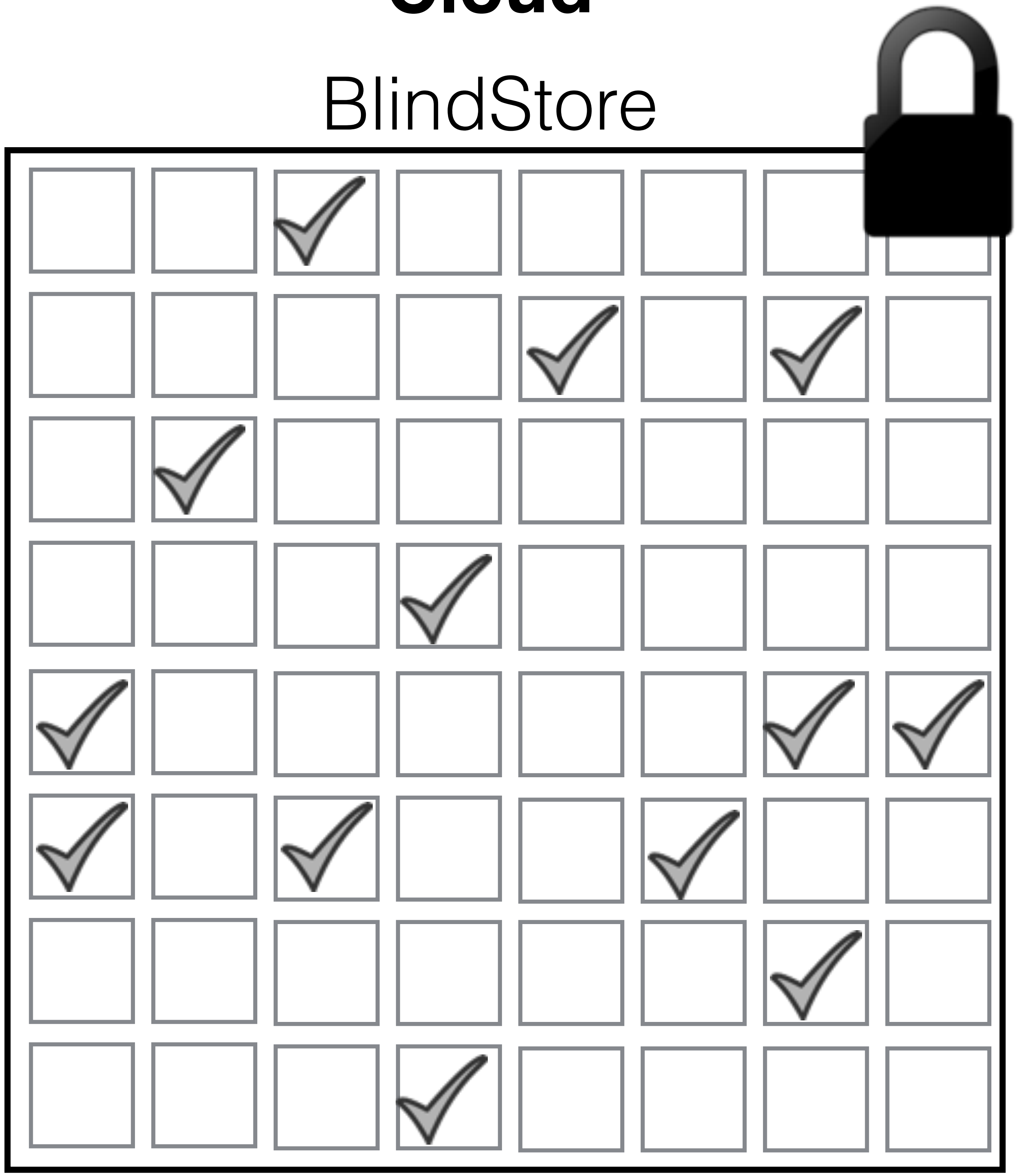
Access (with details)

Client

Access filename2

Cloud

BlindStore



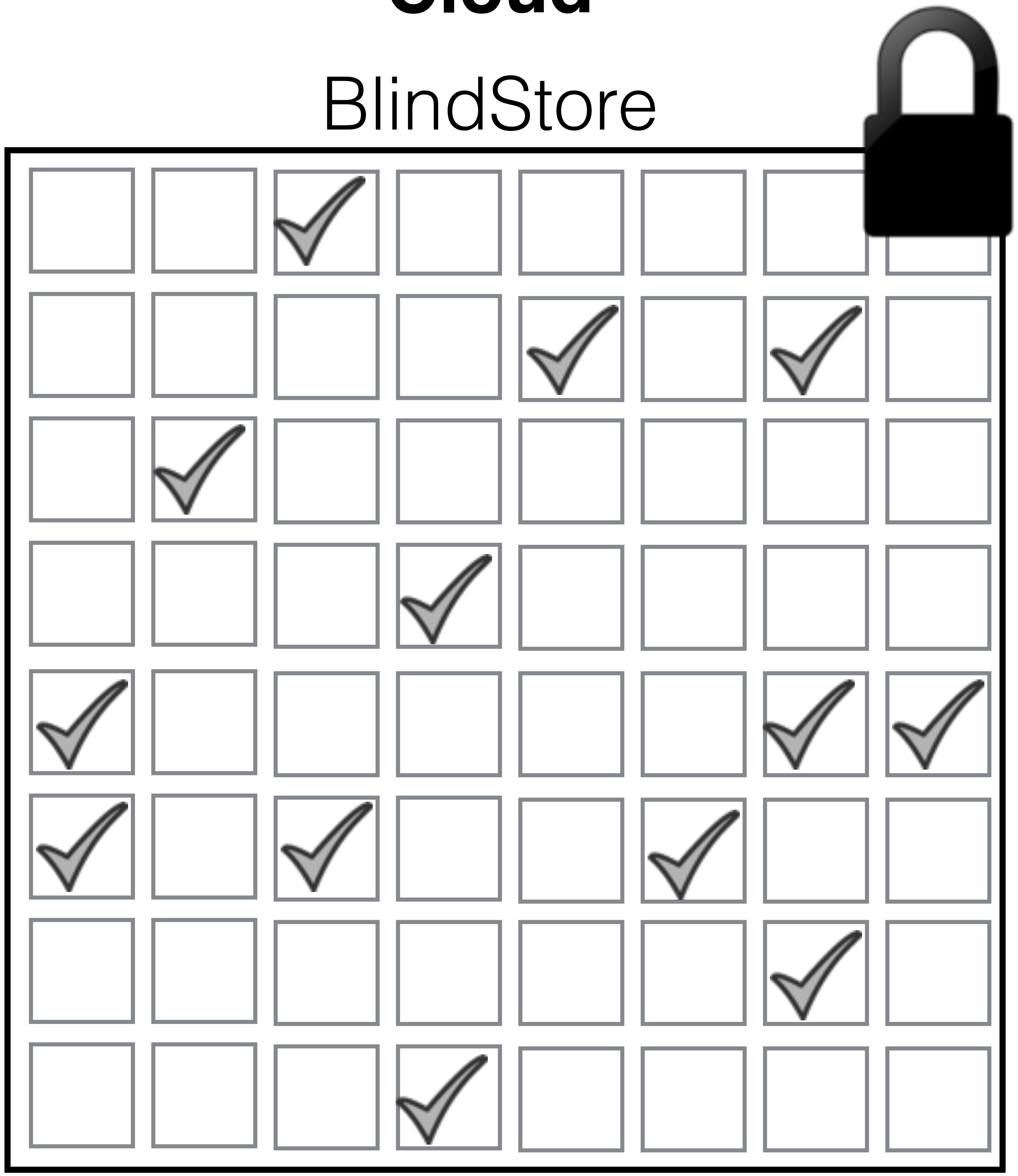
Access (with details)

Client

Cloud

Access filename2

First round



BlindStore

Access (with details)

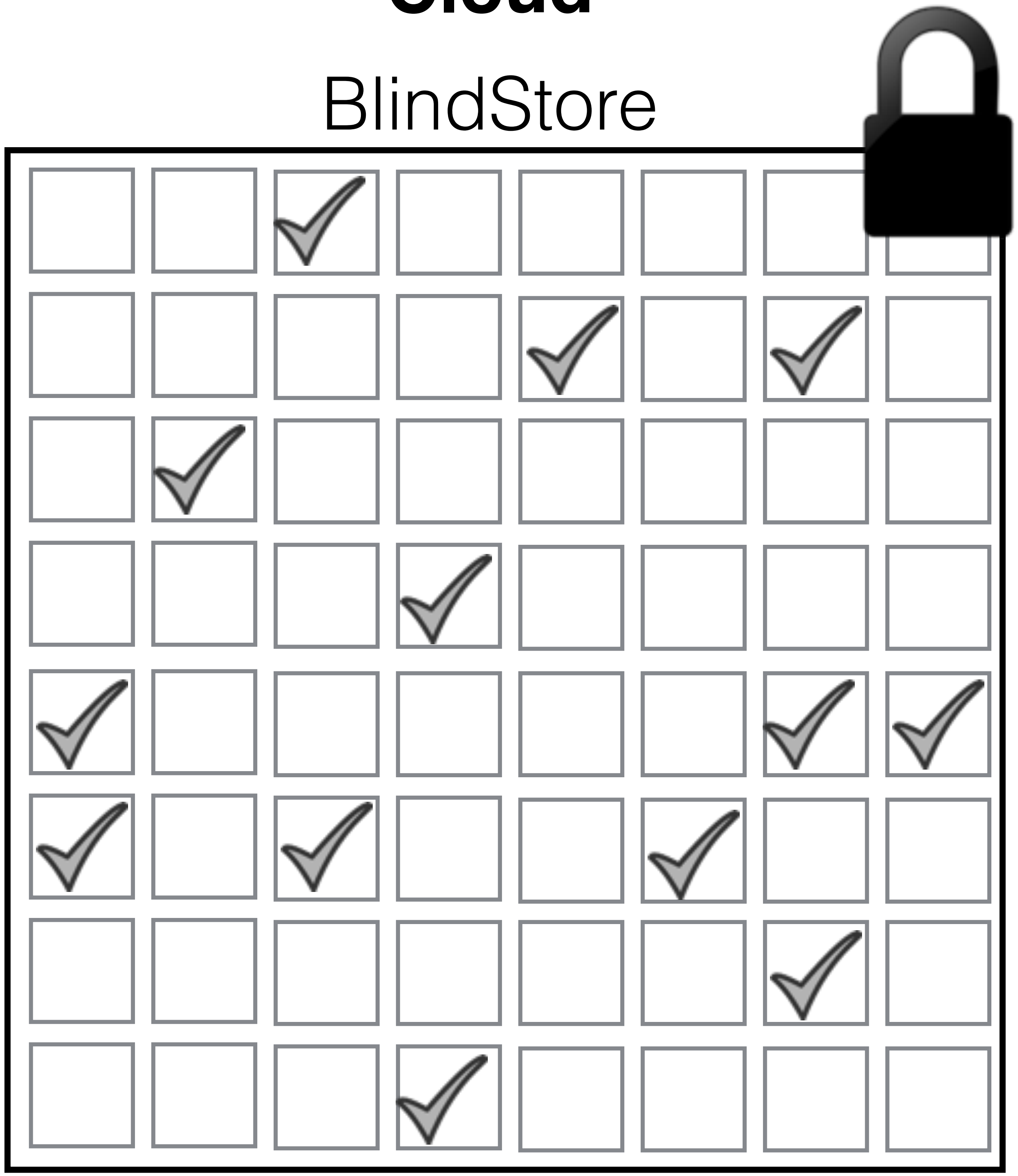
Client

Access filename2

First round

Seed2 = Hash(filename2)

Cloud



Access (with details)

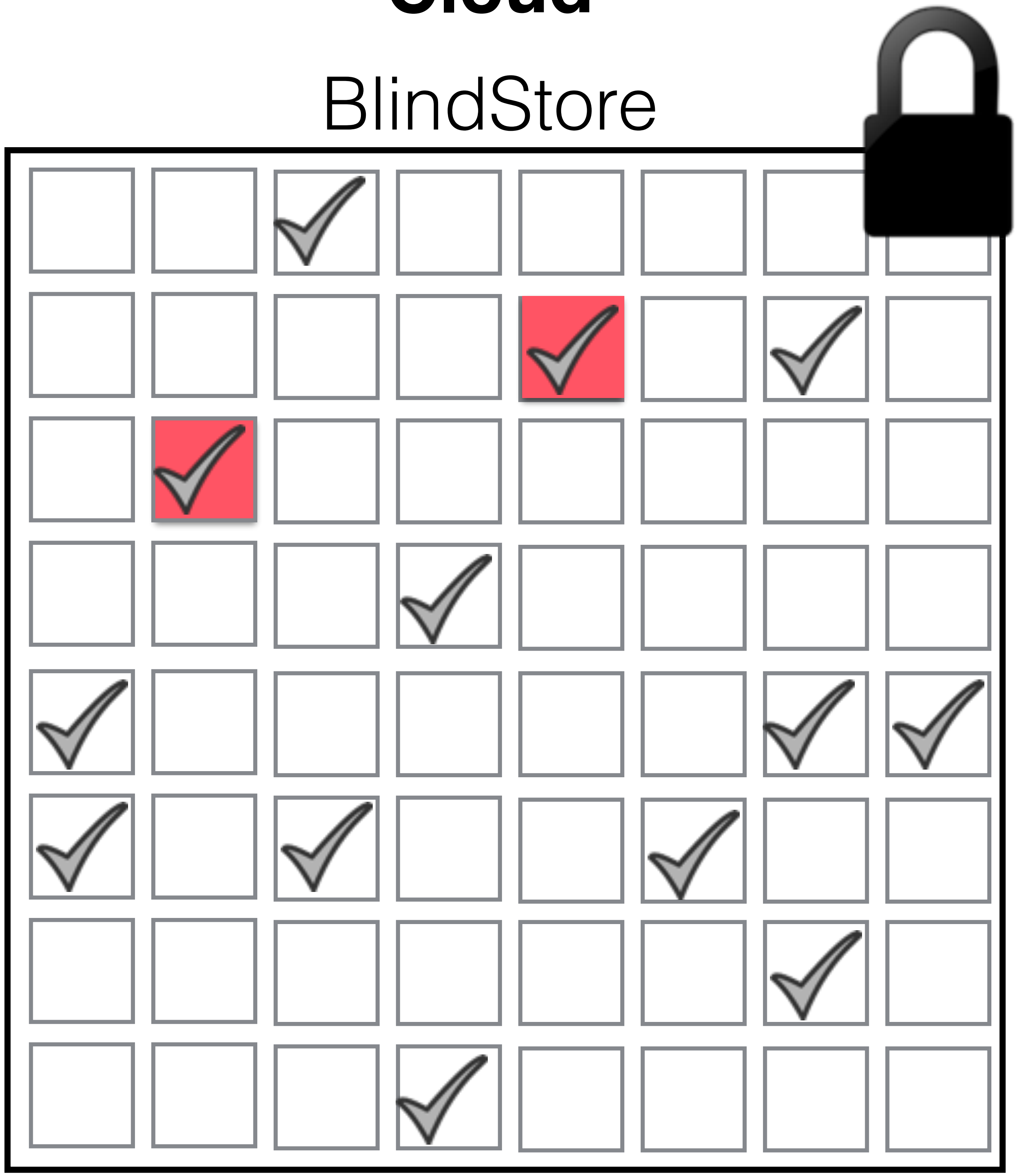
Client

Access filename2

First round

Seed2 = Hash(filename2)

Cloud



Access (with details)

Client

Cloud

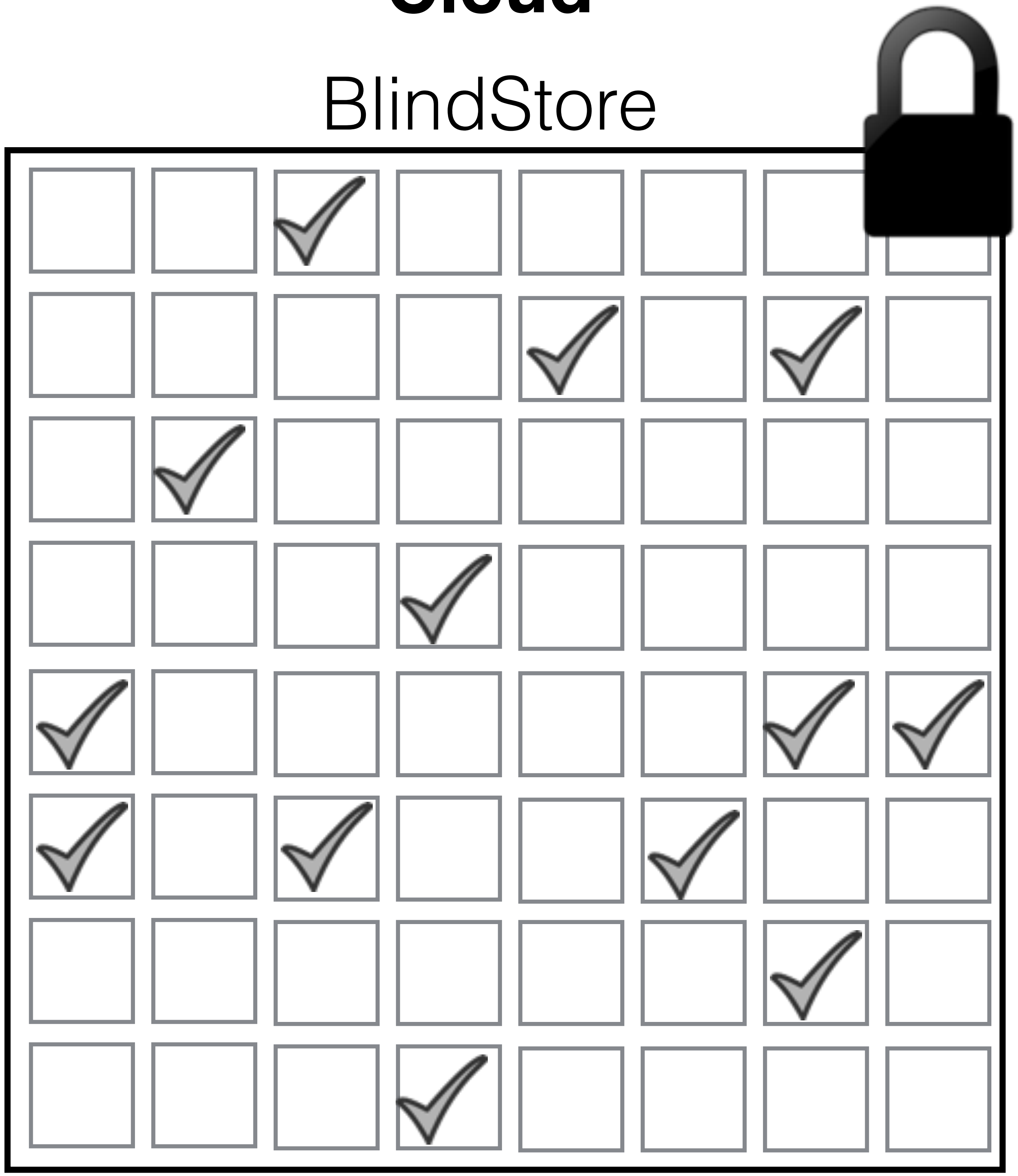
Access filename2

First round

Seed2 = Hash(filename2)

🟥 🟥

BlindStore



		✓					
				✓		✓	
	✓						
			✓				
✓						✓	✓
✓		✓			✓		
						✓	
			✓				

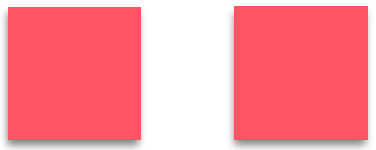
Access (with details)

Client

Access filename2

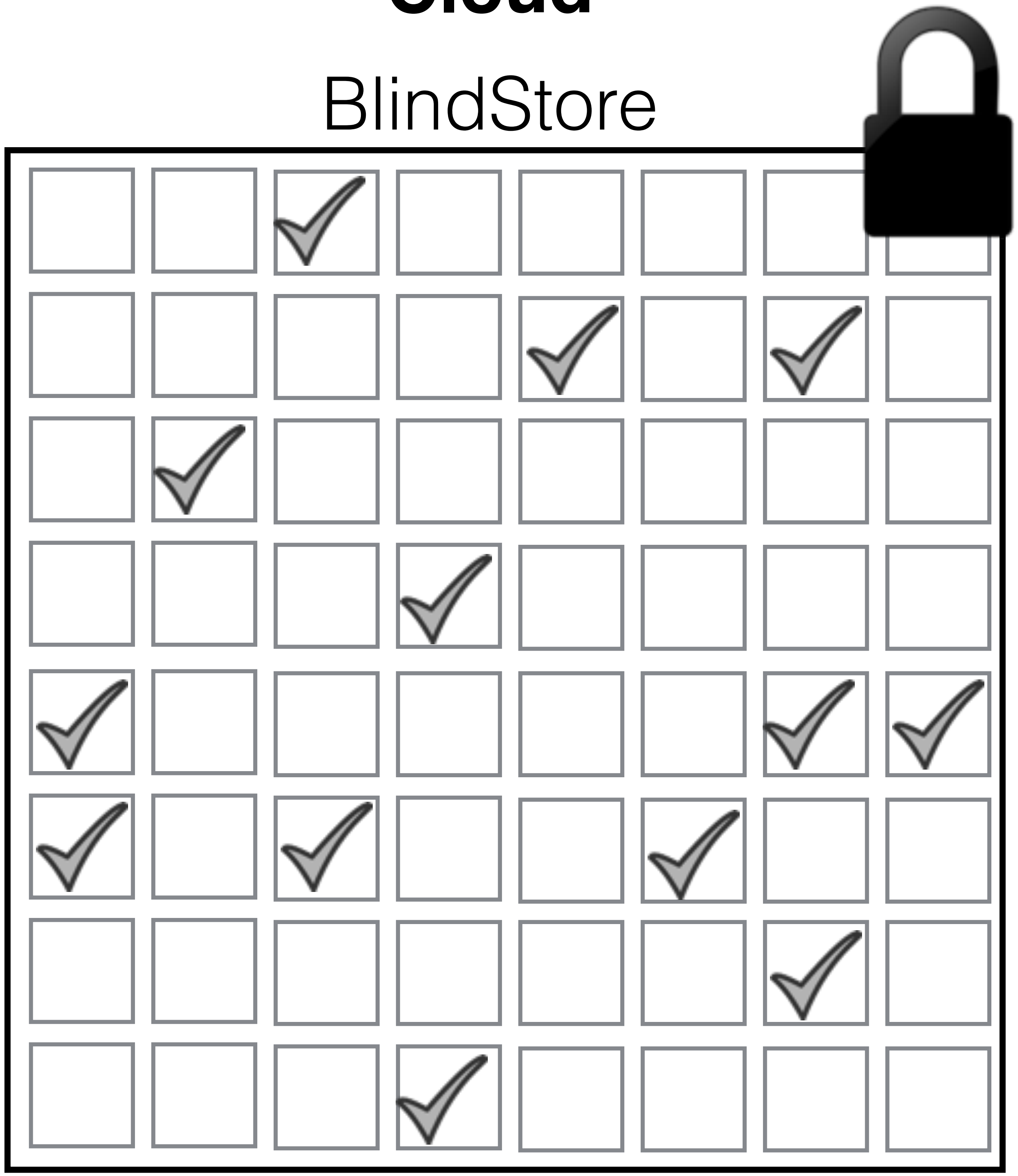
First round

Seed2 = Hash(filename2)



Size = 8 blocks

Cloud



BlindStore

		✓					
				✓		✓	
	✓						
			✓				
✓						✓	✓
✓		✓			✓		
						✓	
			✓				

Access (with details)

Client

Access filename2

First round

Seed2 = Hash(filename2)

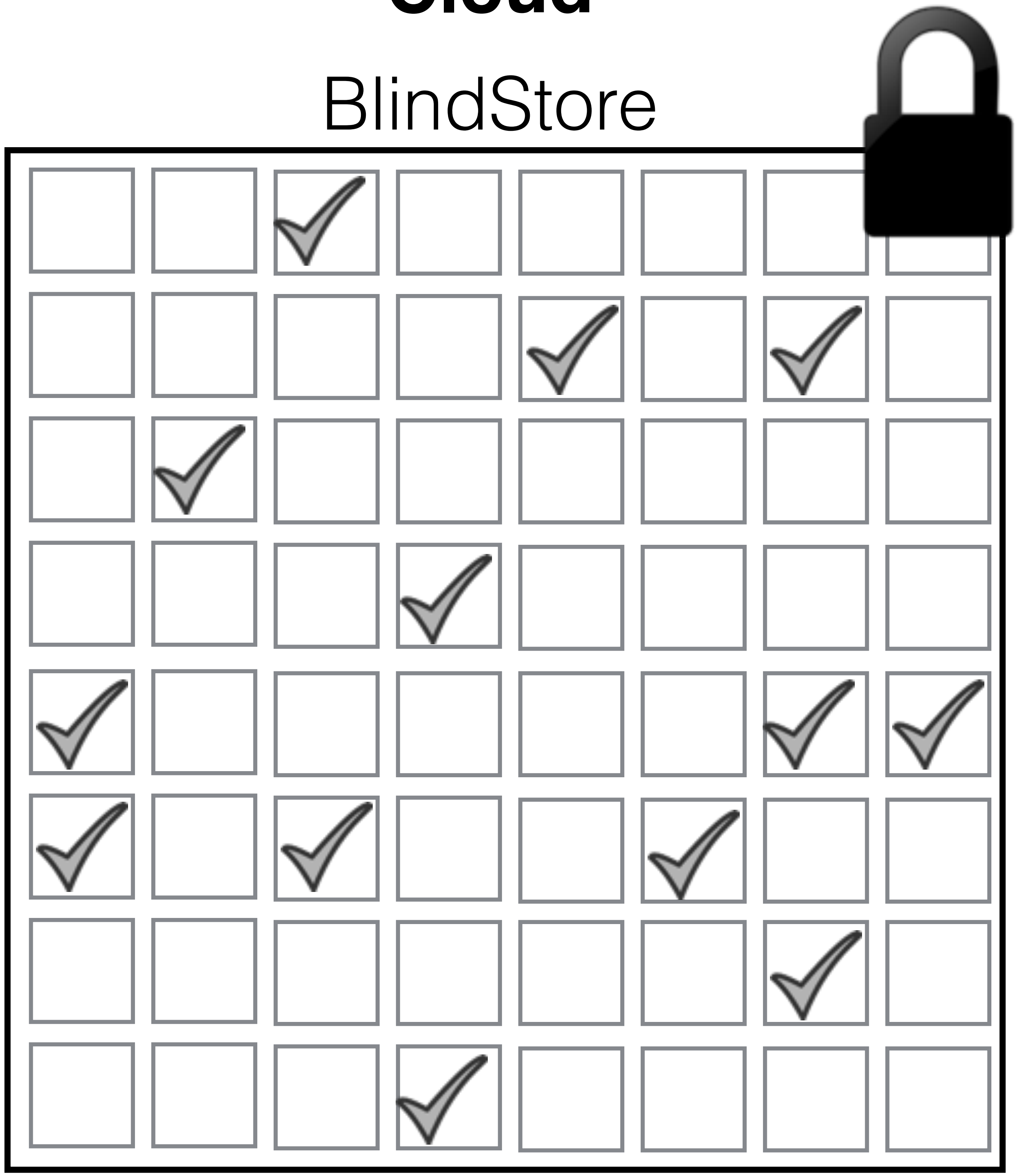
🟥 🟥

Size = 8 blocks

Second round

Cloud

BlindStore



Access (with details)

Client

Access filename2

First round

Seed2 = Hash(filename2)

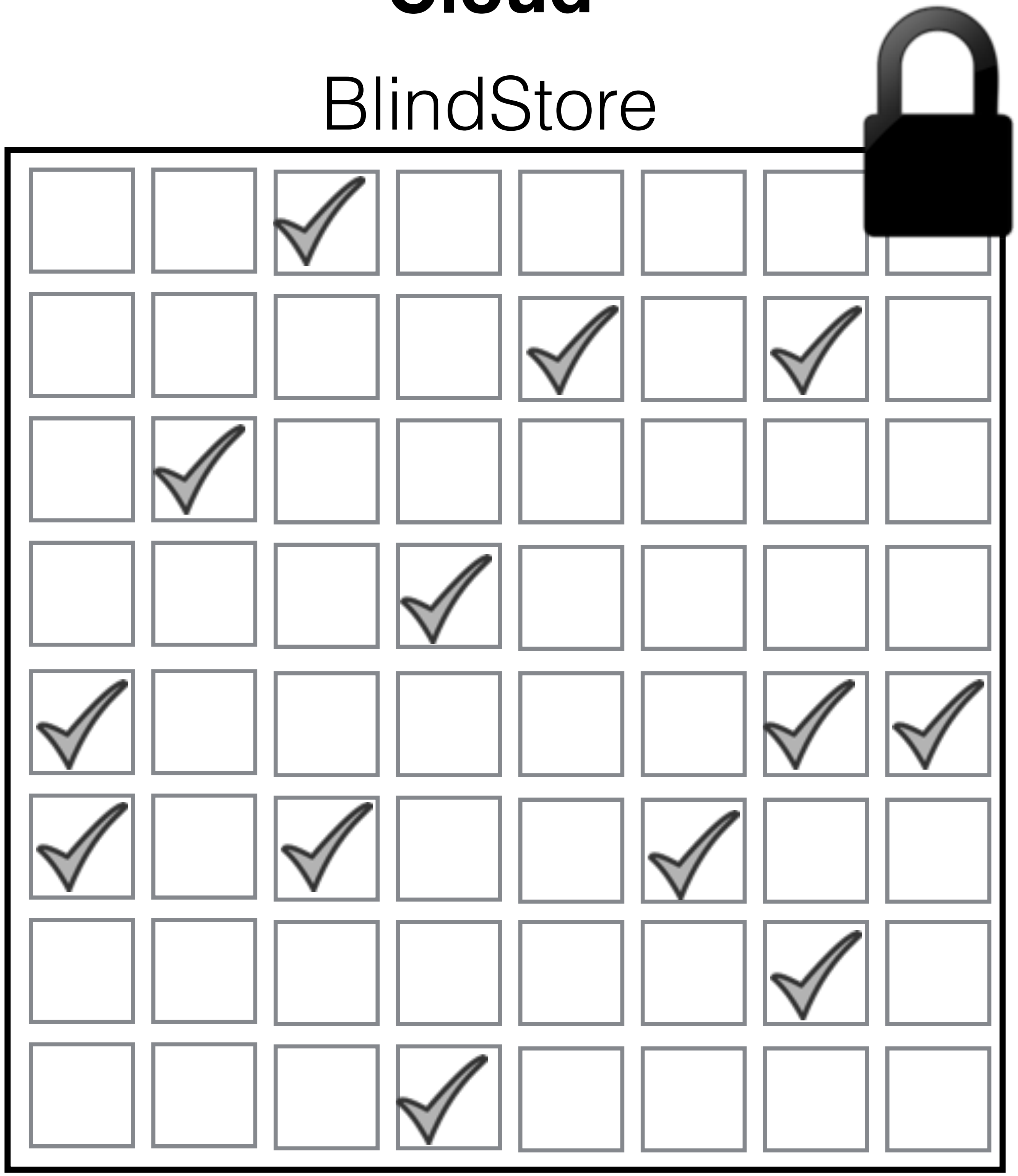
🟥 🟥

Size = 8 blocks

Second round

Retrieve remaining 6 blocks

Cloud



		✓					
				✓		✓	
	✓						
			✓				
✓						✓	✓
✓		✓			✓		
						✓	
			✓				

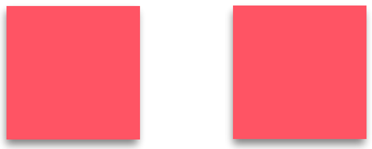
Access (with details)

Client

Access filename2

First round

Seed2 = Hash(filename2)

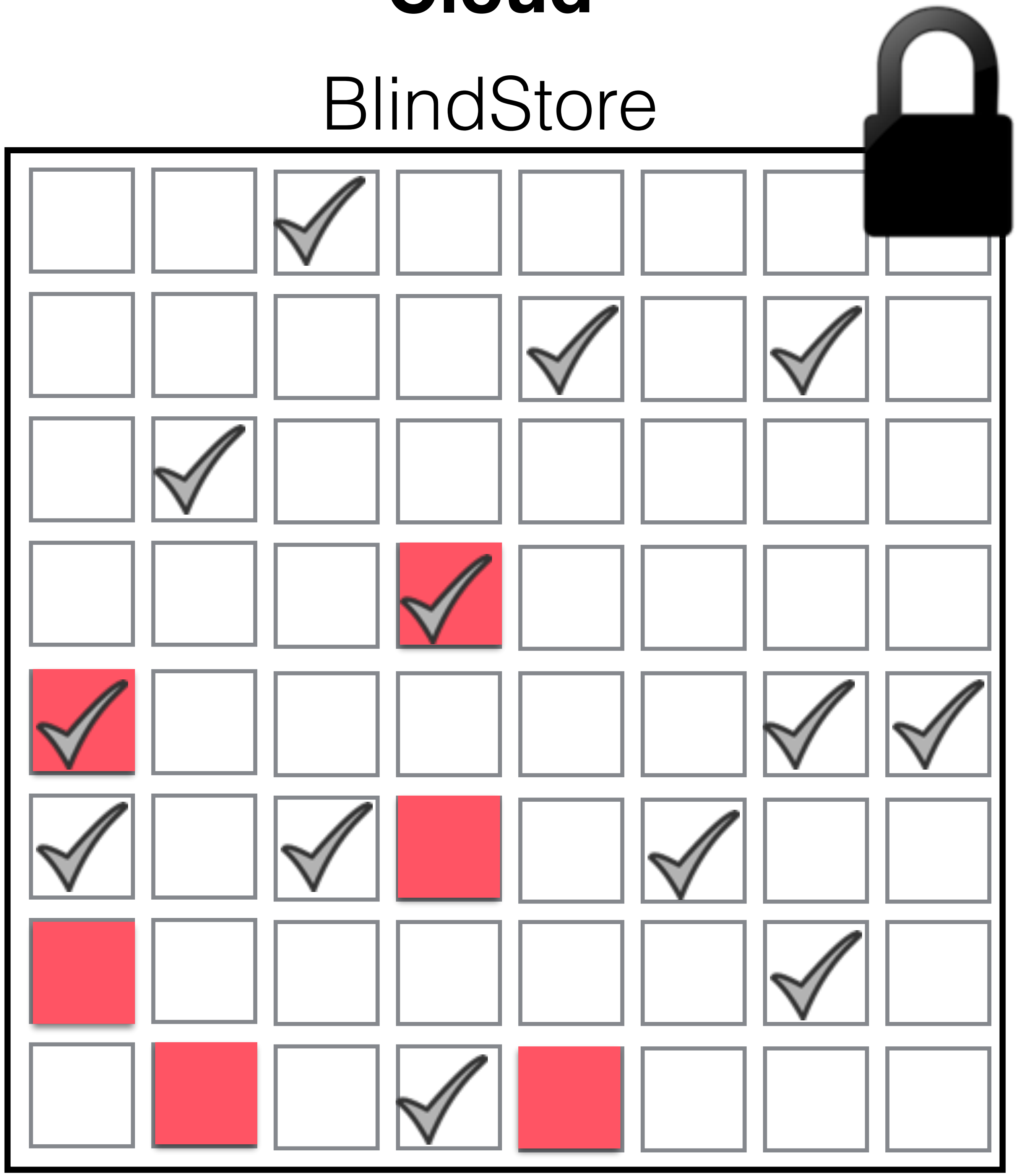


Size = 8 blocks

Second round

Retrieve remaining 6 blocks

Cloud



Access (with details)

Client

Access filename2

First round

Seed2 = Hash(filename2)

🟥 🟥

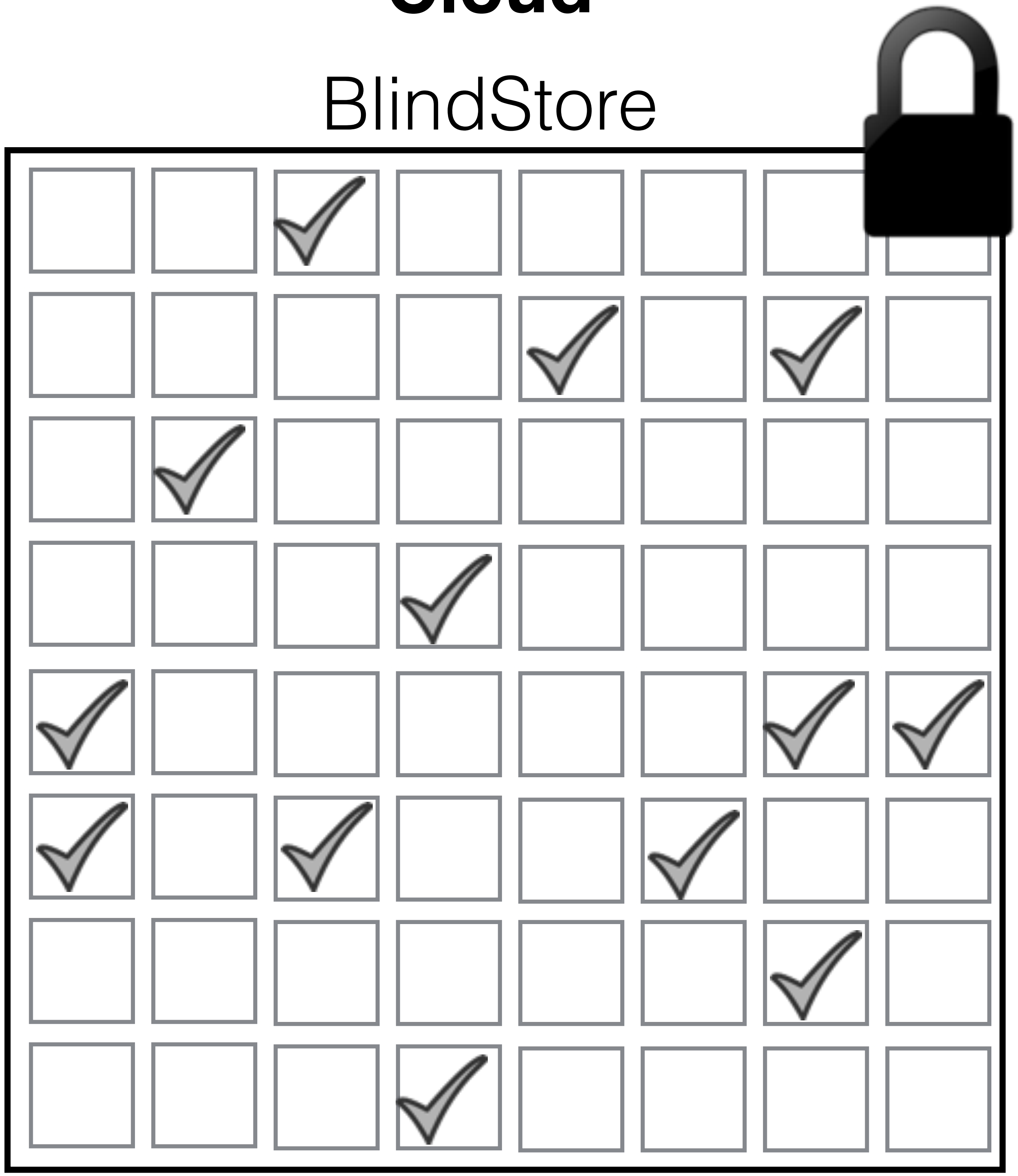
Size = 8 blocks

Second round

Retrieve remaining 6 blocks

🟥 🟥 🟥 🟥 🟥 🟥

Cloud



Access (with details)

Client

Access filename2

First round

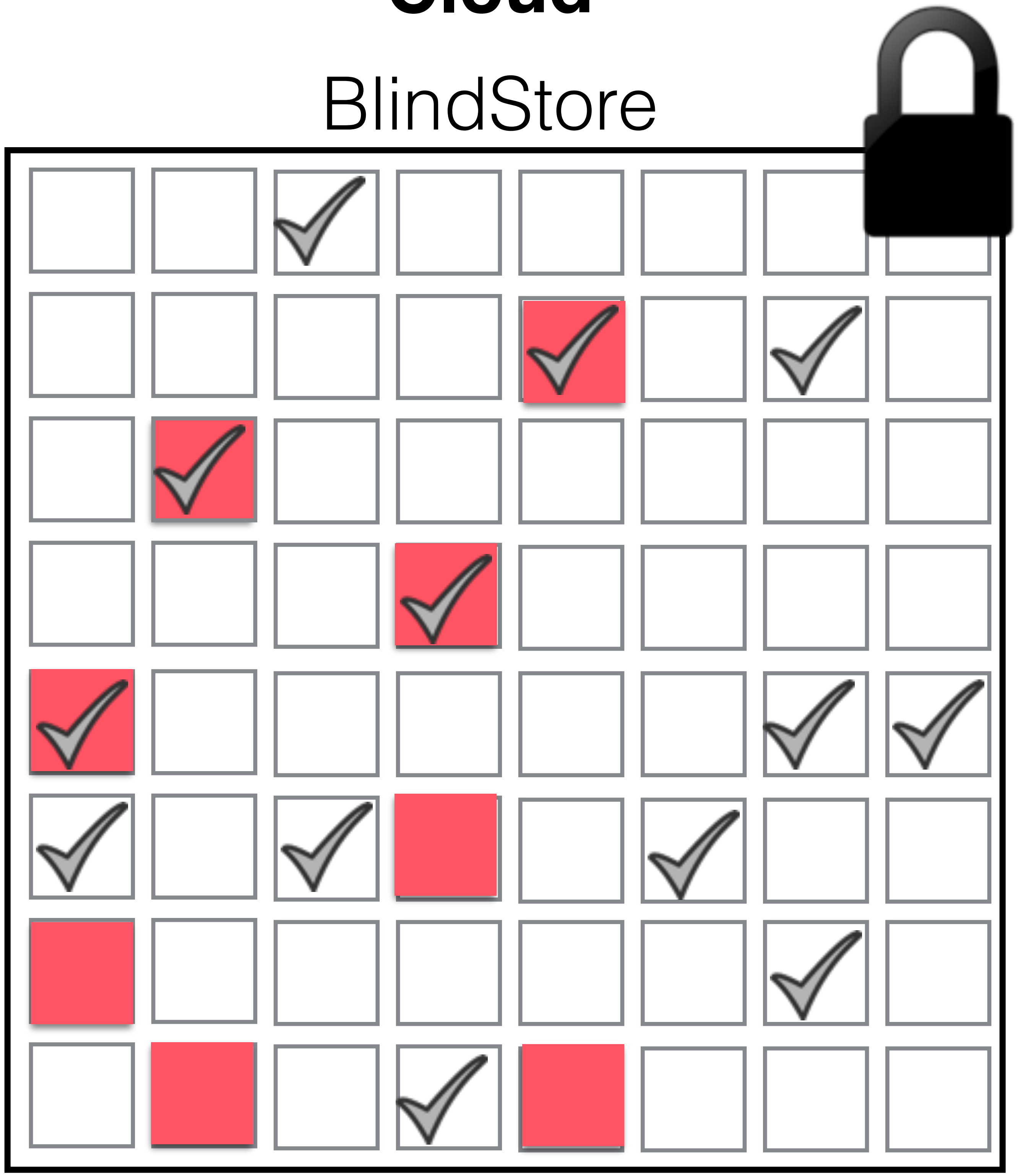
Seed2 = Hash(filename2)

Size = 8 blocks

Second round

Retrieve remaining 6 blocks

Cloud



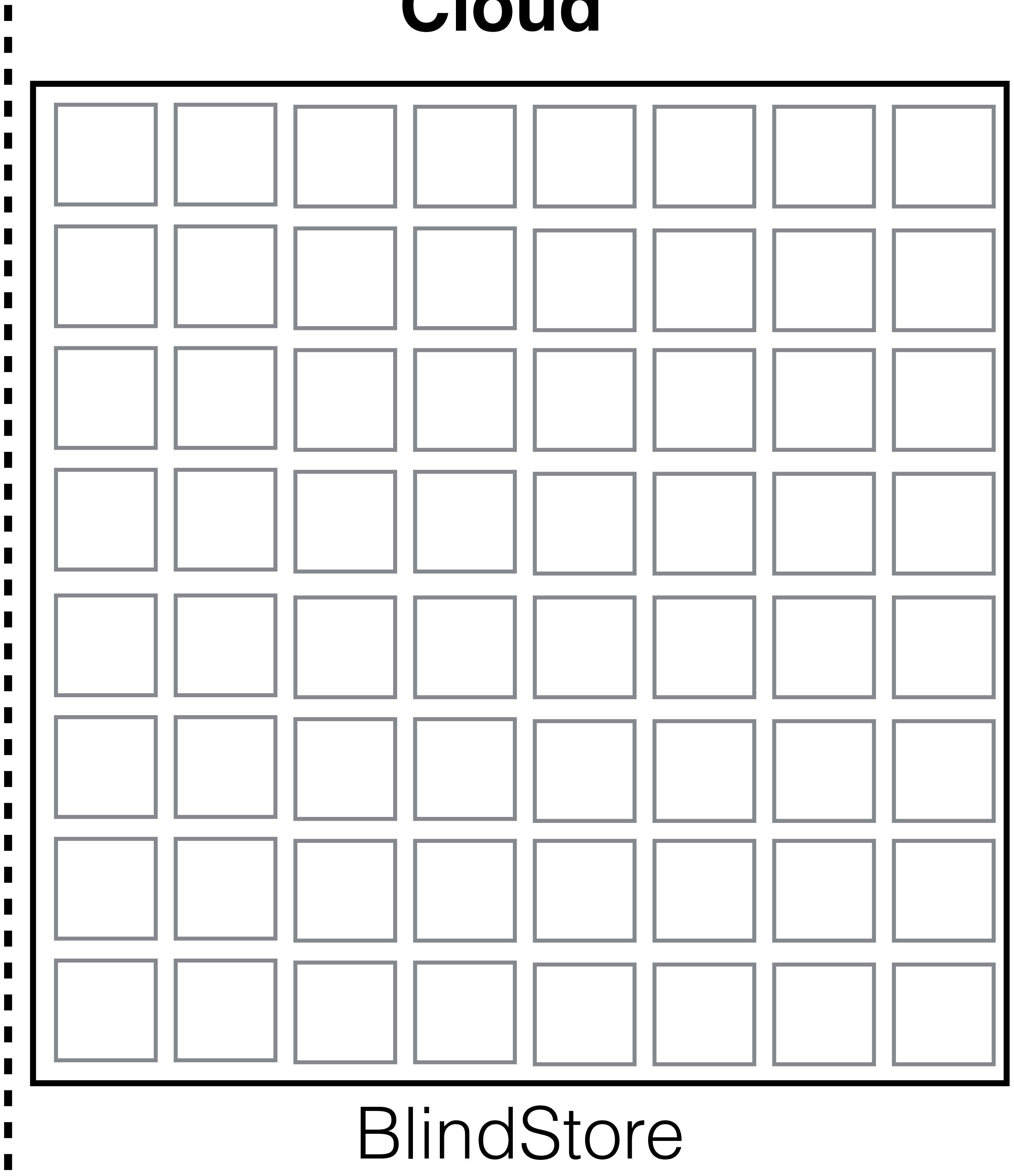
Access (with details)

- *k* blocks are accessed in the first round, where *k* is the security parameter
    - We set k = 80 for our experiments
- Total communication per access:
    - 80 blocks for small files (i.e. 20KB for files smaller than 5KB)
    - 4 times the file’s size (for files larger than 5KB)

Why read more?

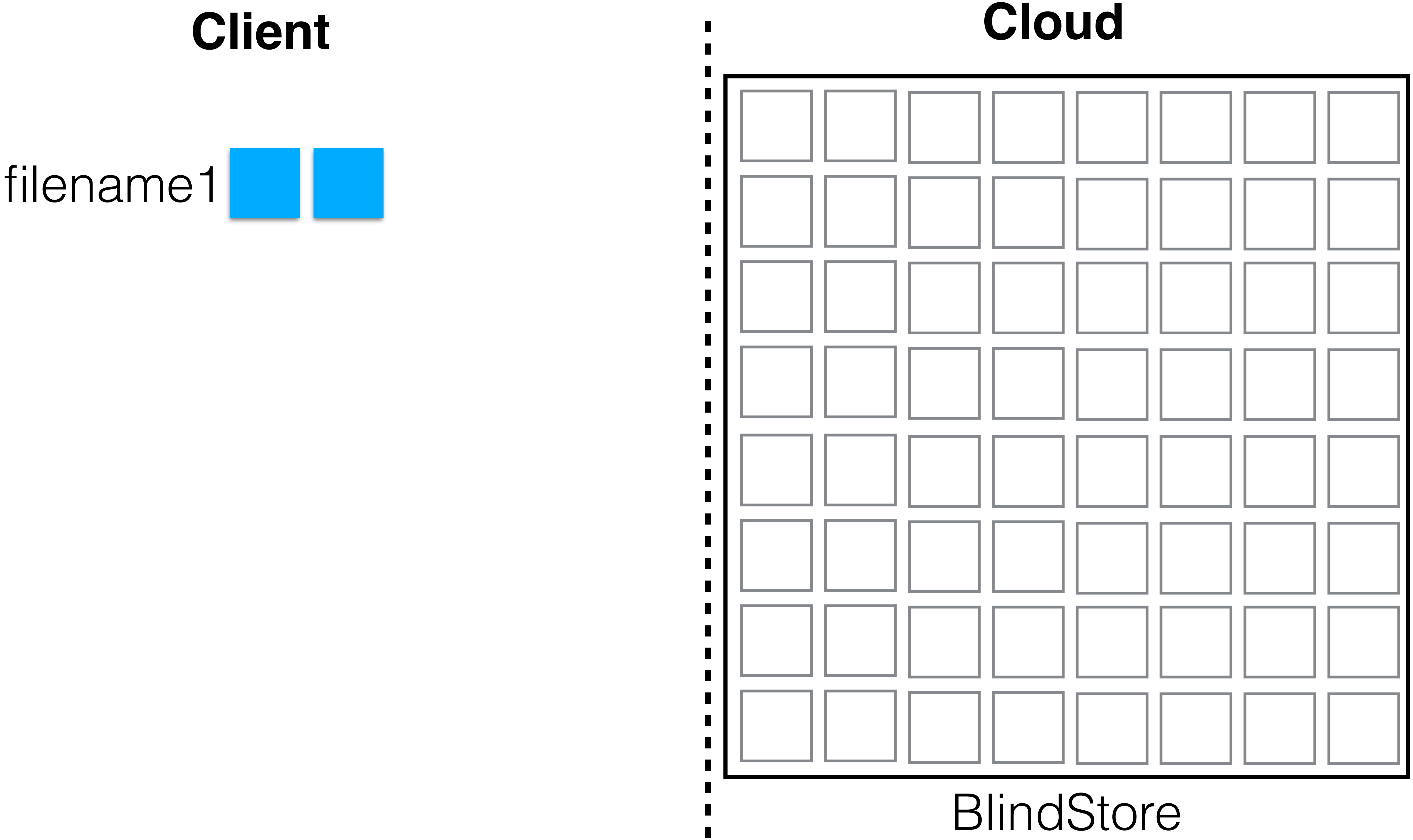
Client

Cloud



BlindStore

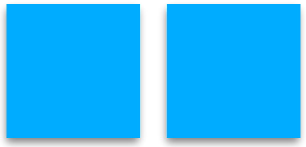
Why read more?



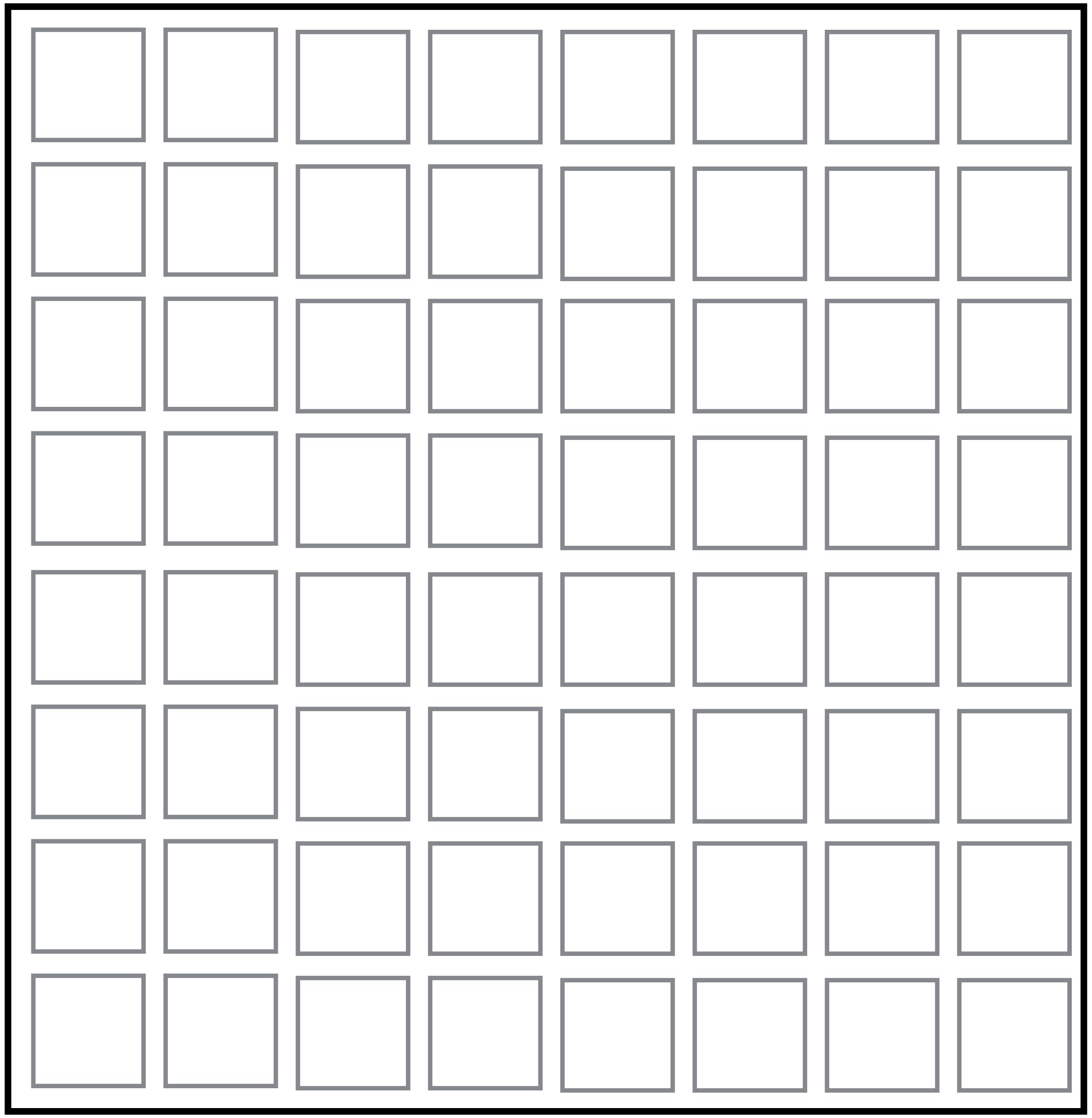
Why read more?

Client

Cloud

filename1 

Seed1 = Hash(filename1)



BlindStore

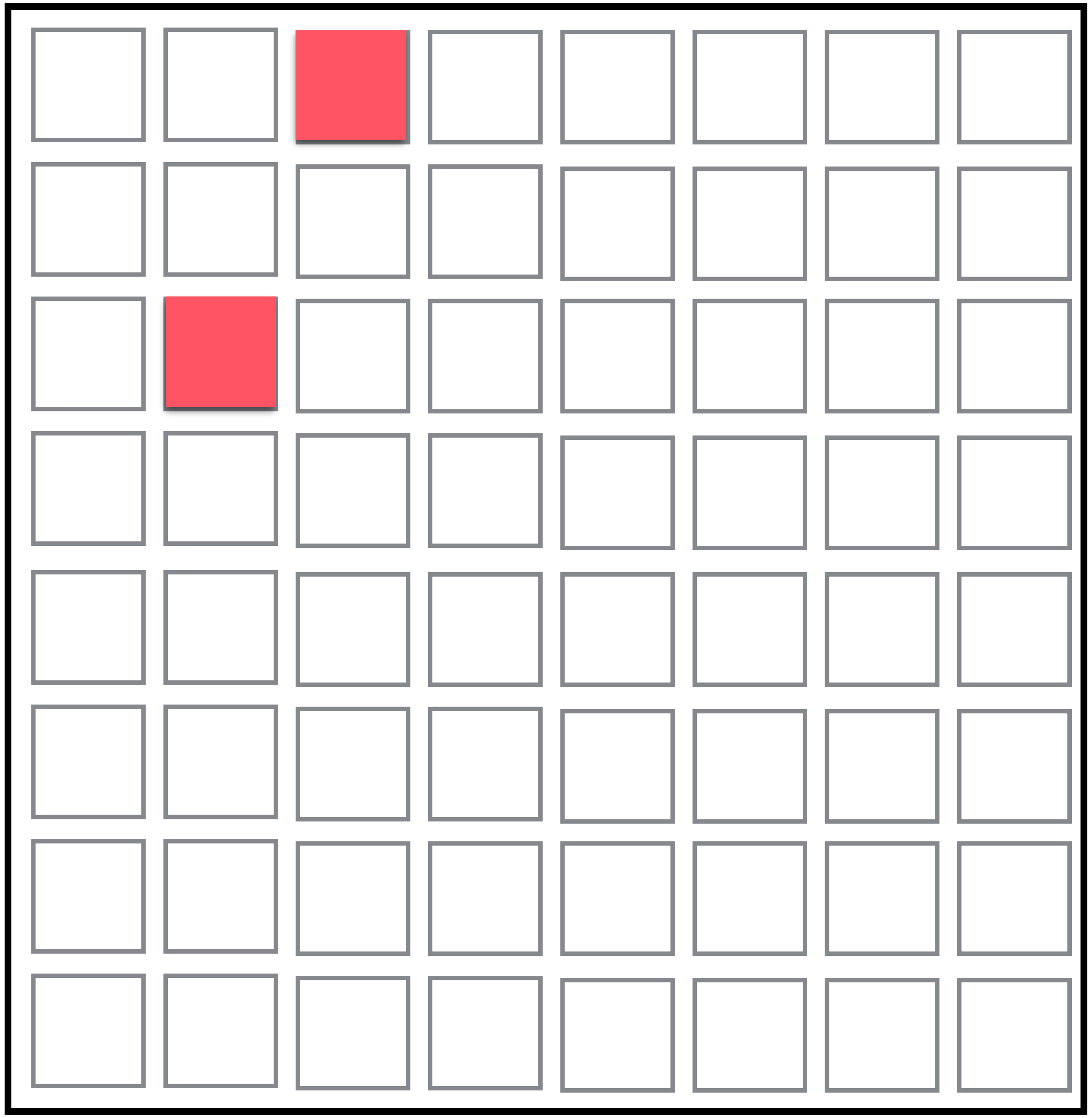
Why read more?

Client

Cloud

filename1 🟦 🟦

Seed1 = Hash(filename1)



BlindStore

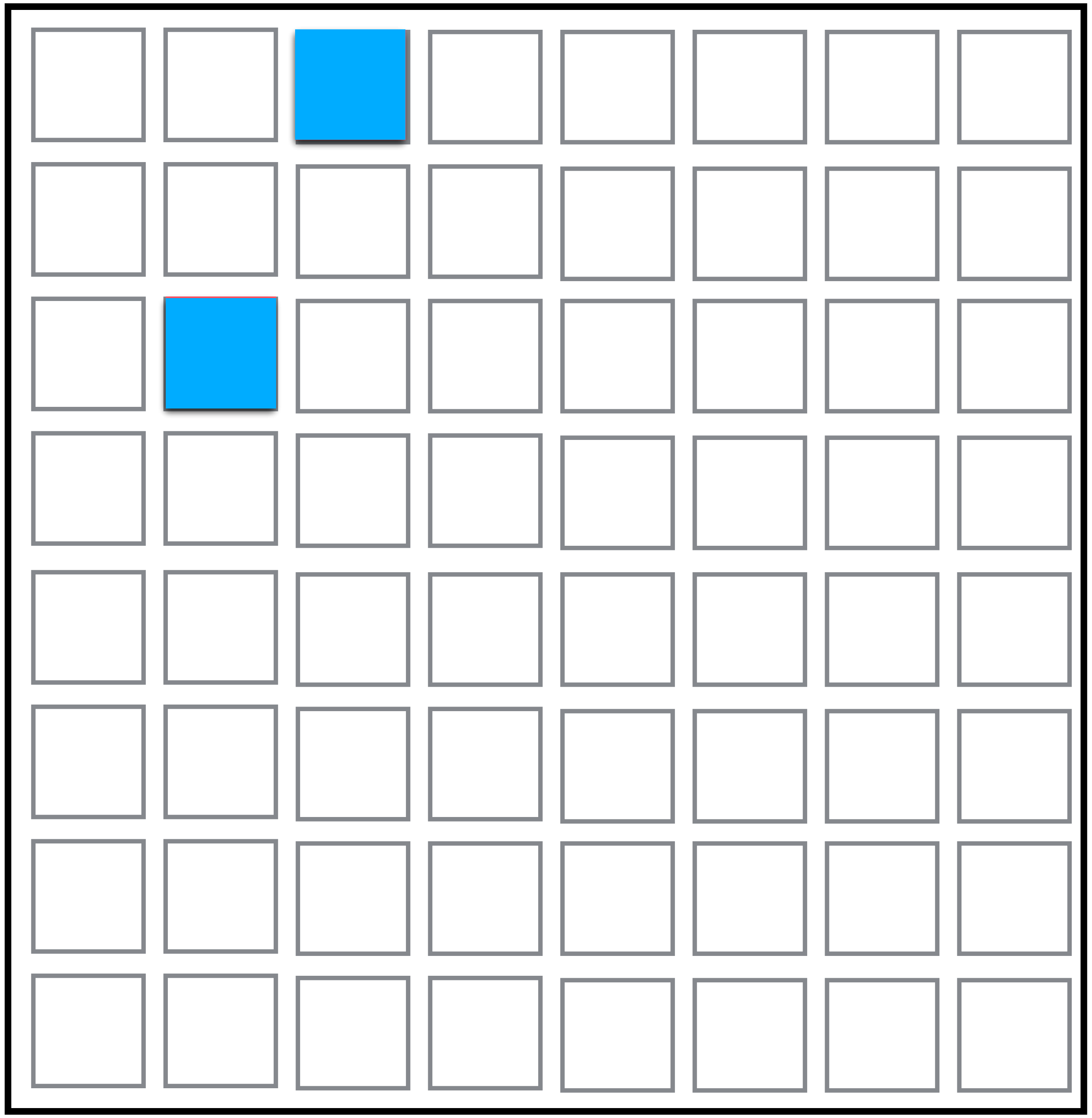
Why read more?

Client

Cloud

filename1

Seed1 = Hash(filename1)



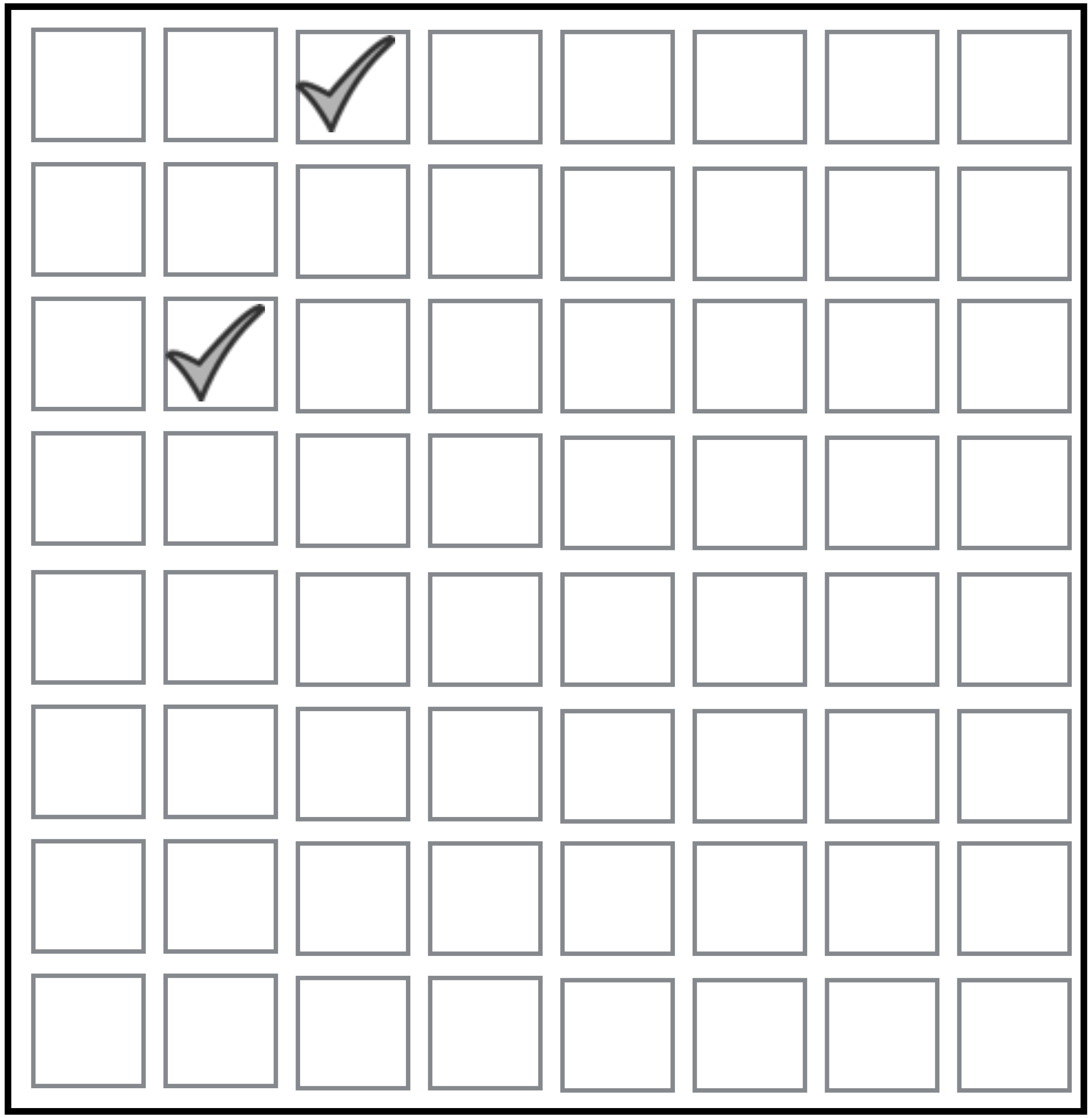
Why read more?

Client

Cloud

filename1

Seed1 = Hash(filename1)



BlindStore

Why read more?

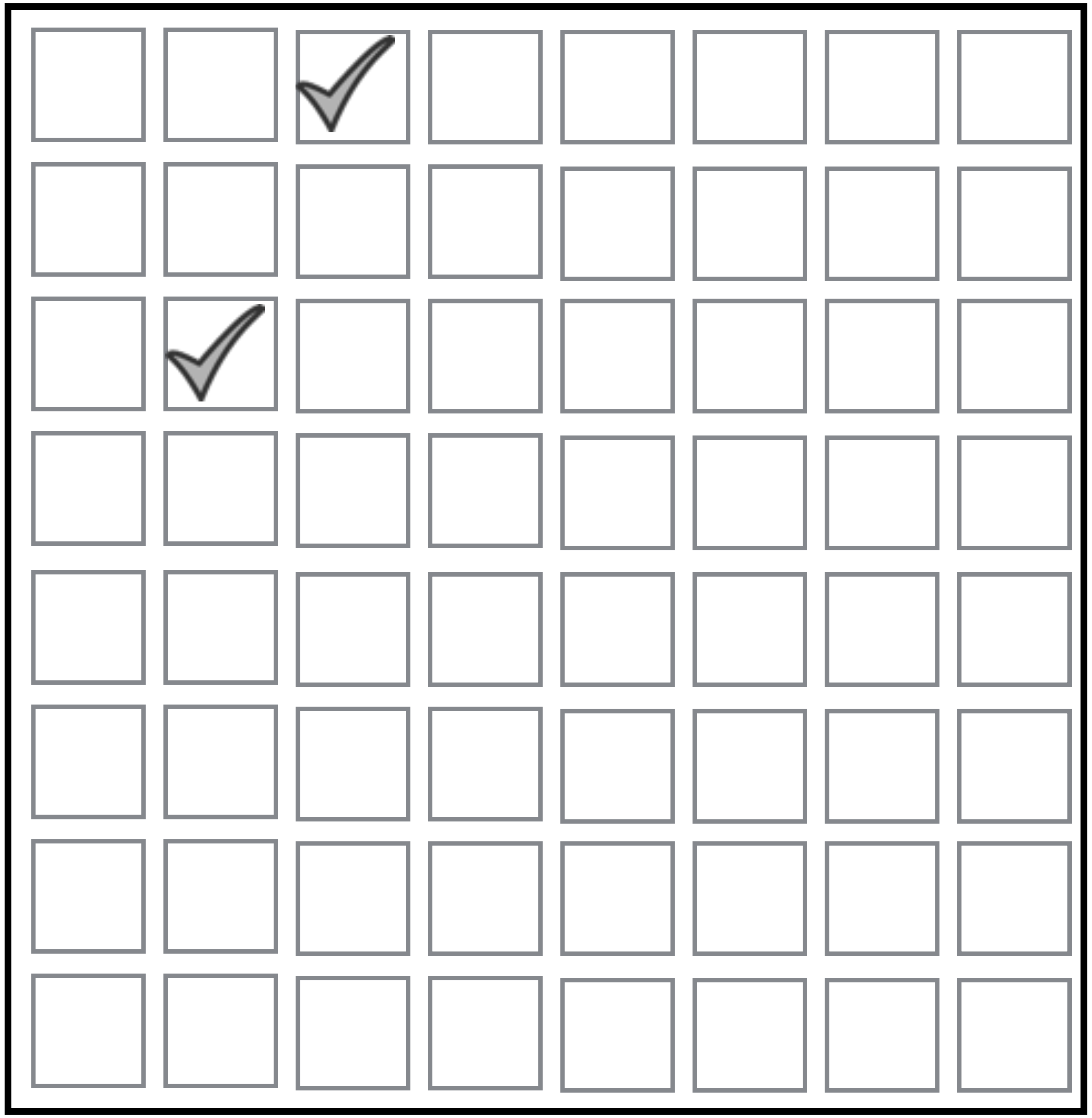
Client

Cloud

filename1

filename2 🟦 🟦

Seed1 = Hash(filename1)



Why read more?

Client

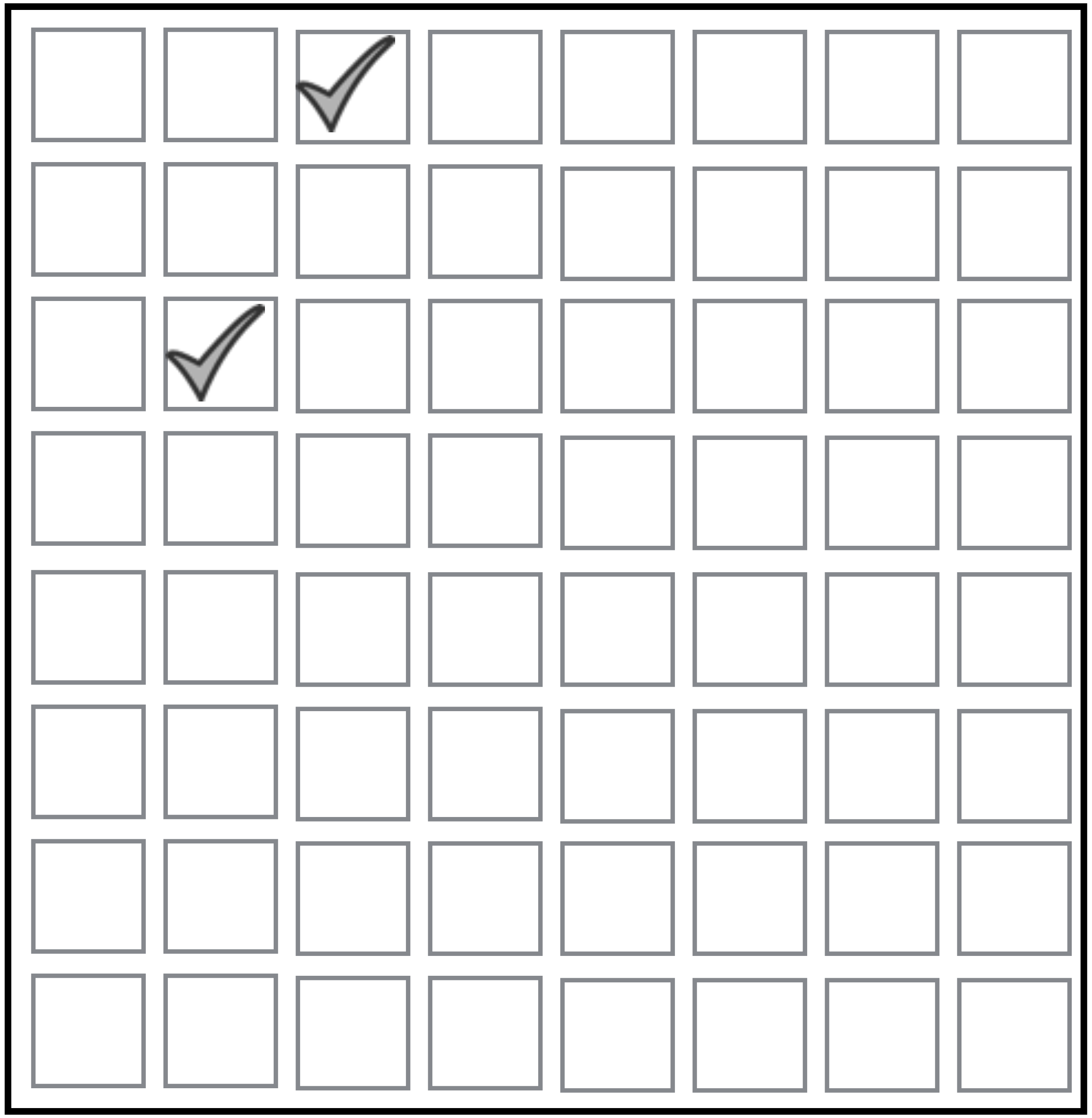
filename1

filename2 🟦 🟦

Seed1 = Hash(filename1)

Seed2 = Hash(filename2)

Cloud



BlindStore

Why read more?

Client

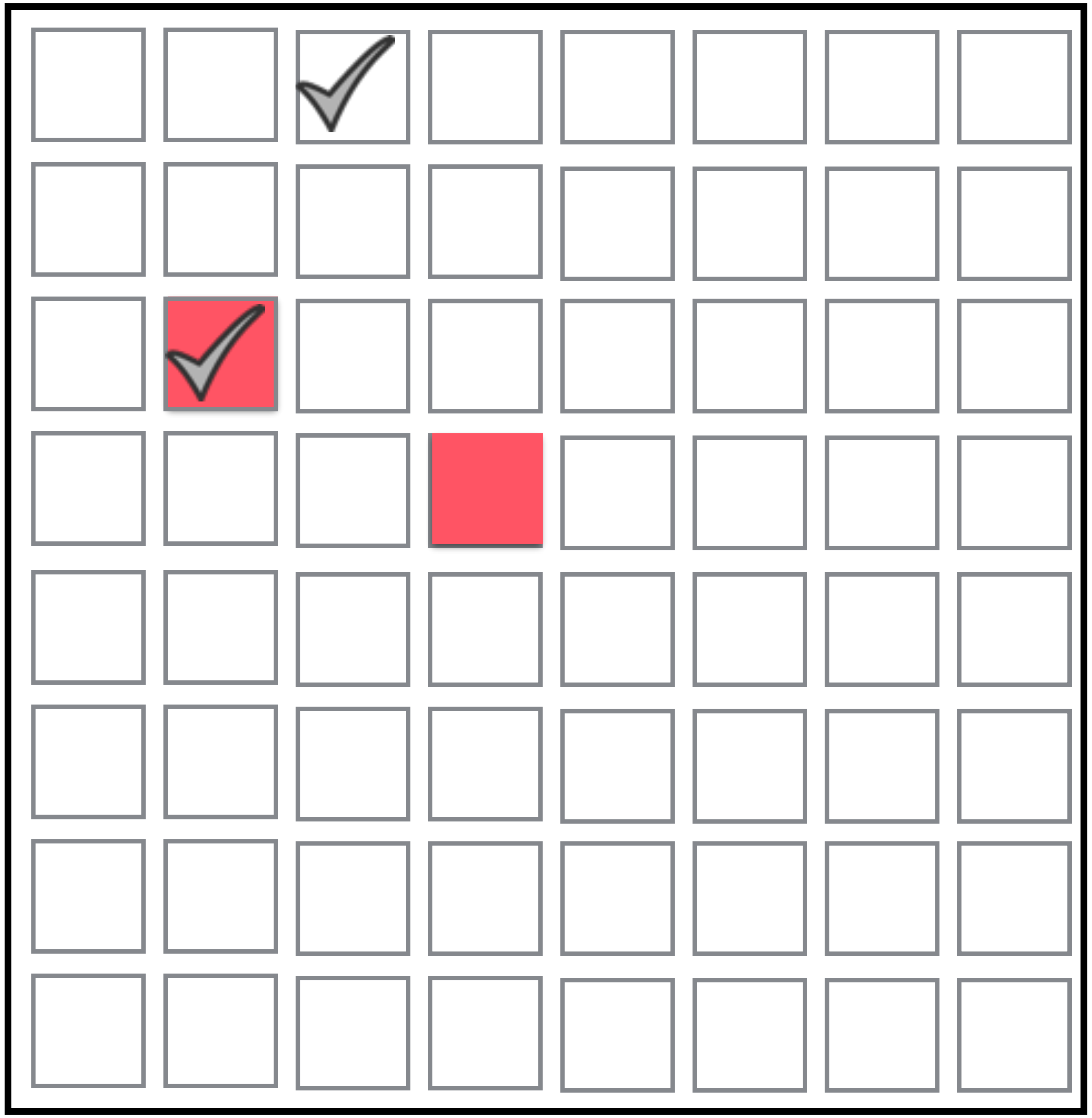
filename1

filename2 🟦 🟦

Seed1 = Hash(filename1)

Seed2 = Hash(filename2)

Cloud



BlindStore

Why read more?

Client

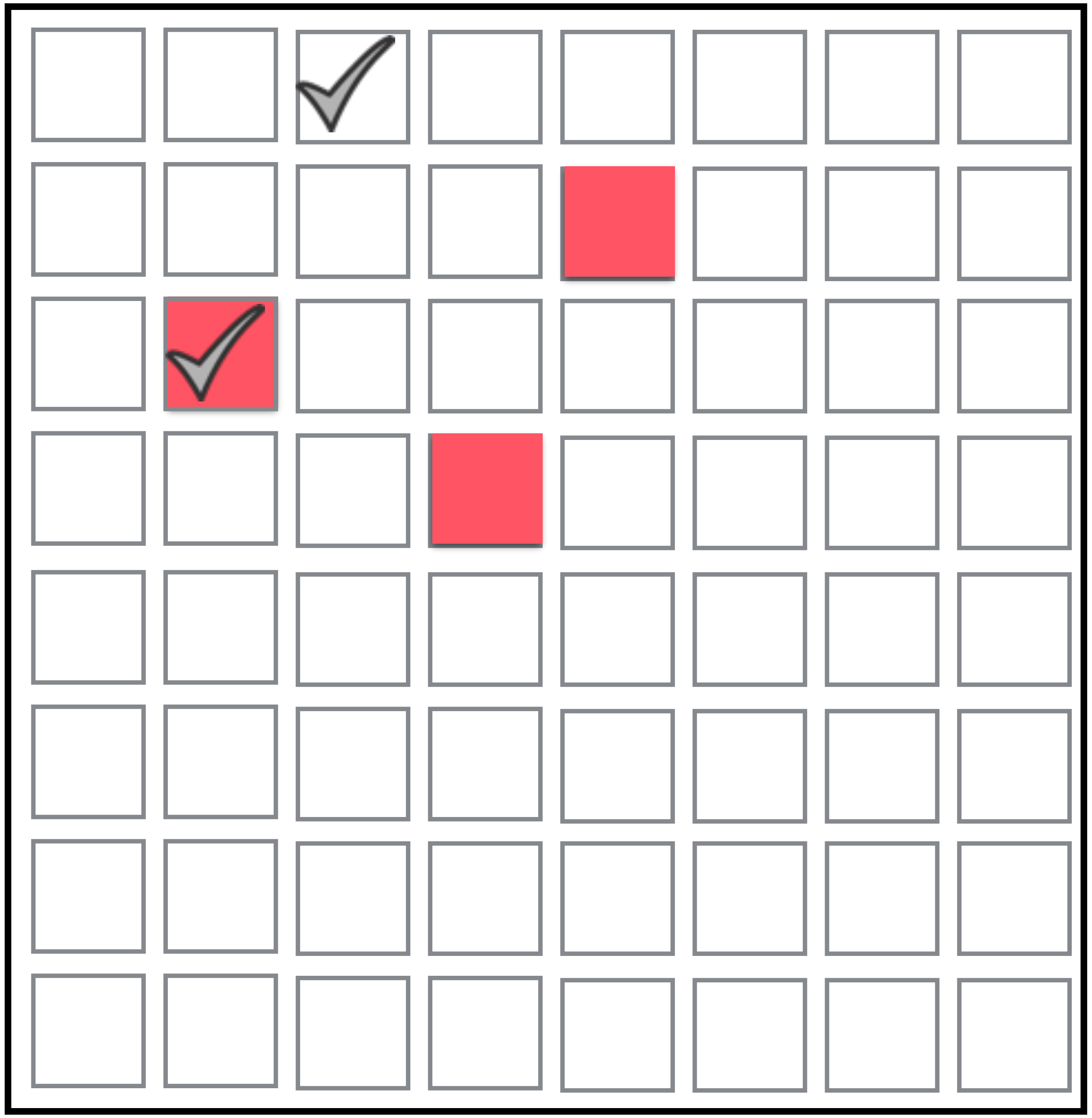
filename1

filename2 🟦 🟦

Seed1 = Hash(filename1)

Seed2 = Hash(filename2)

Cloud



BlindStore

Why read more?

Client

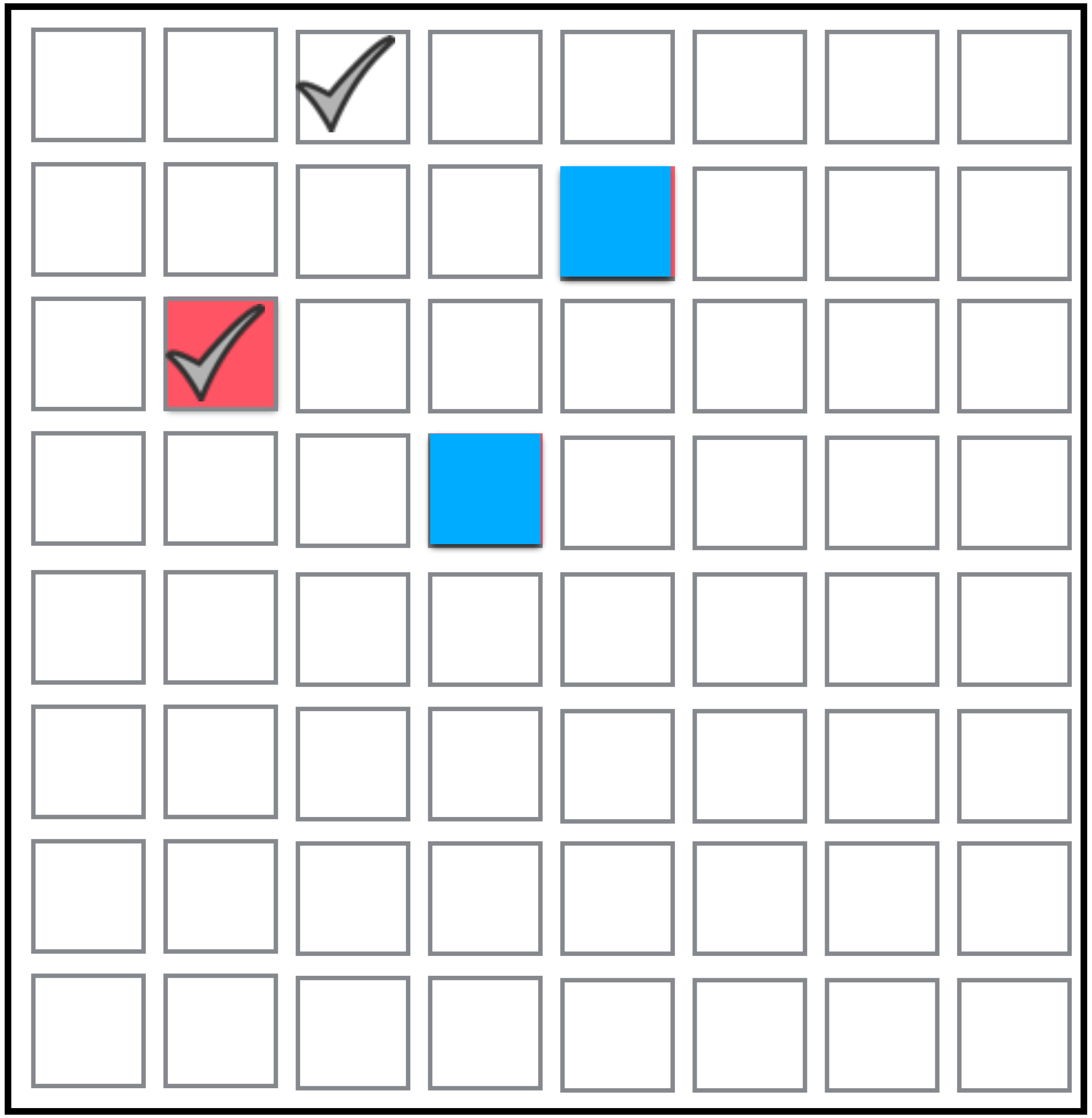
Cloud

filename1

filename2

Seed1 = Hash(filename1)

Seed2 = Hash(filename2)



BlindStore

Why read more?

Client

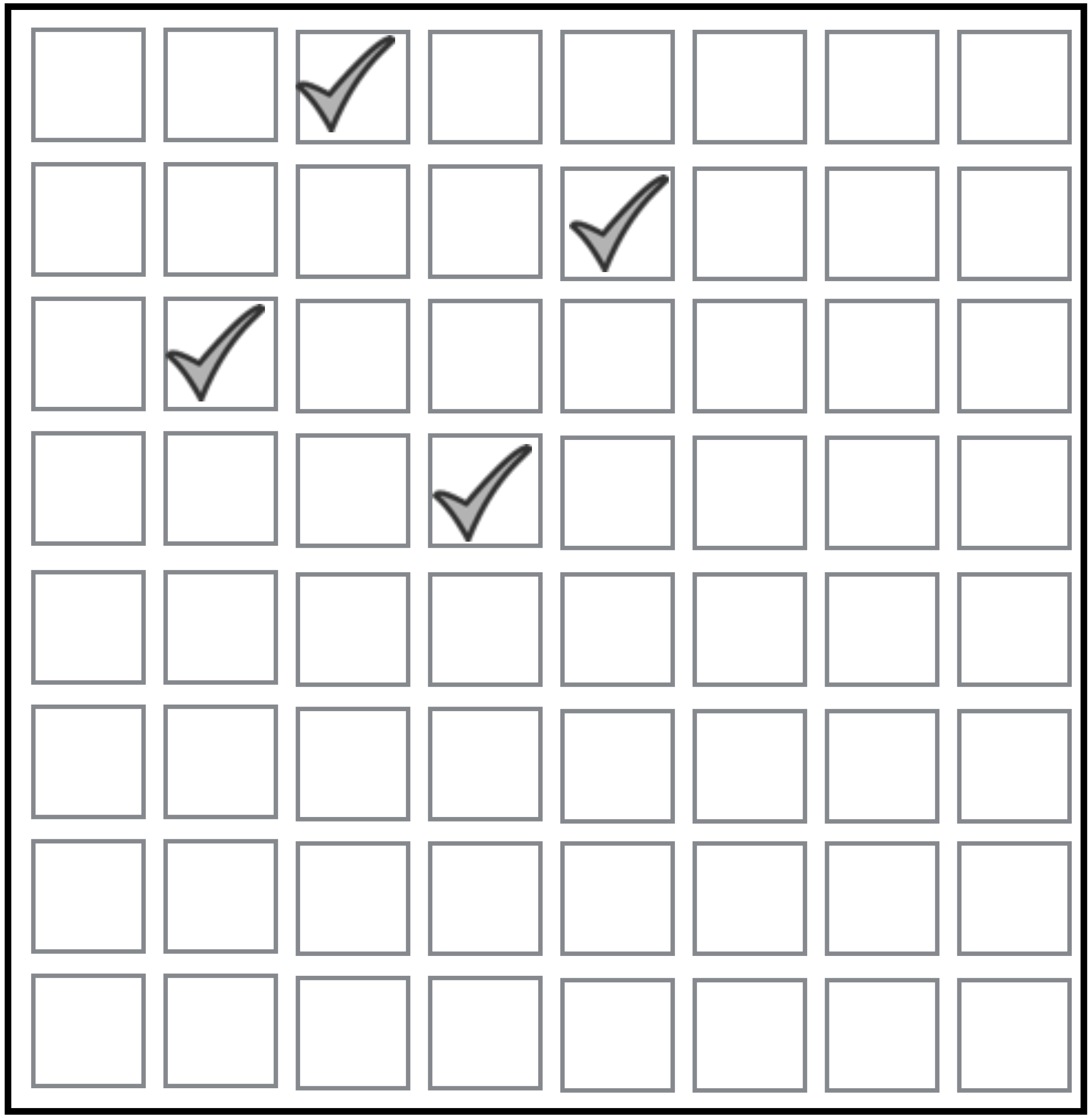
filename1

filename2

Seed1 = Hash(filename1)

Seed2 = Hash(filename2)

Cloud



BlindStore

Why read more?

Client

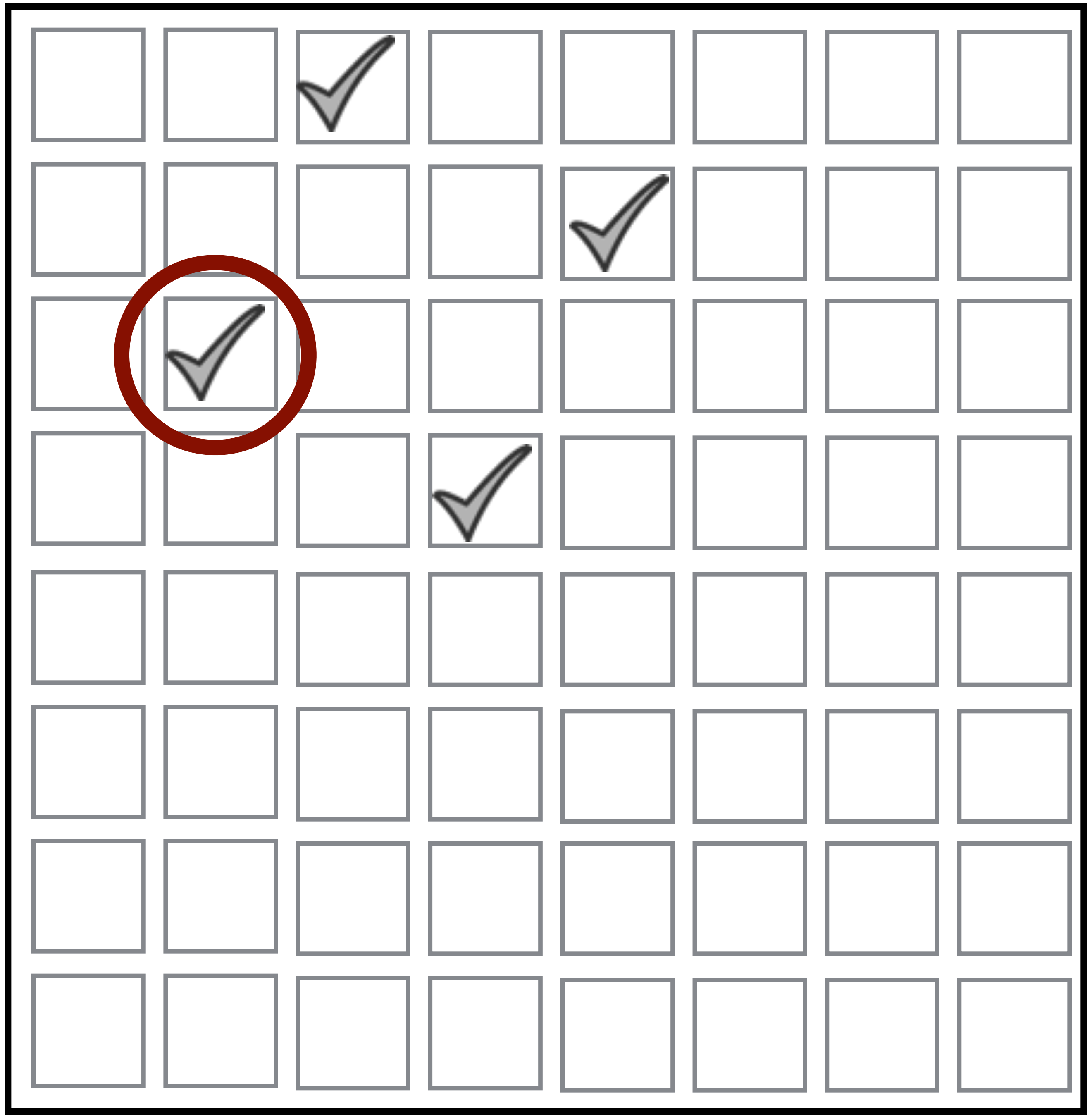
filename1

filename2

Seed1 = Hash(filename1)

Seed2 = Hash(filename2)

Cloud



BlindStore

SSE via Blind Storage

Setup

Client

Cloud

Setup

Client

Cloud

Blind Store

Setup

Client

Cloud

Blind Store

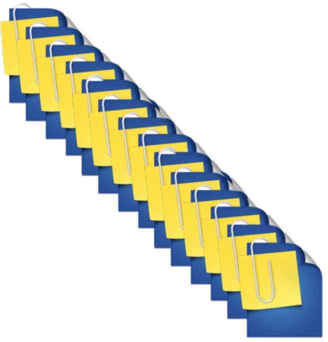
Setup

Client

Cloud

Index

word	document list
best	1, 2
illinois	1, 3
microsoft	1, 4
america	1, 5
naveed2@illinois.ed	1, 6
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6, 7, 8

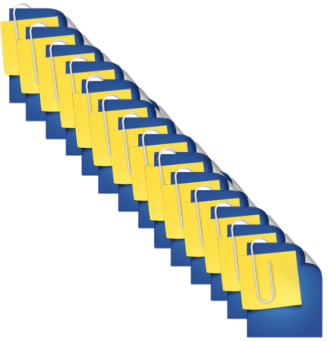


Blind Store

Setup

Client

Cloud



Index

word	document list
best	1, 2
illinois	1, 3
microsoft	1, 4
america	1, 5
naveed2@illinois.ed	1, 6
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6, 7, 8

contents: **1,2**

Blind Store

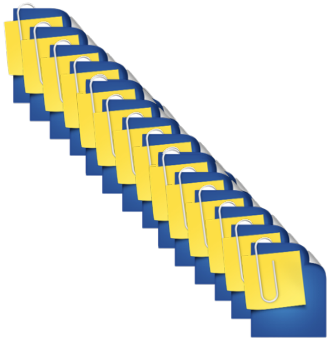
Setup

Client

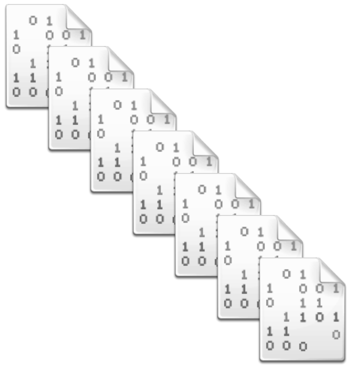
Cloud

Index

word	document list
best	1, 2
illinois	1, 3
microsoft	1, 4
america	1, 5
naveed2@illinois.ed	1, 6
blue	1
pakistan	8, 9
cryptography	10, 11, 12
laptop	13
android	3, 4, 14, 15
genomics	3, 4, 16
privacy	3, 4, 16, 17
security	1, 2, 3, 4, 5, 6, 7, 8

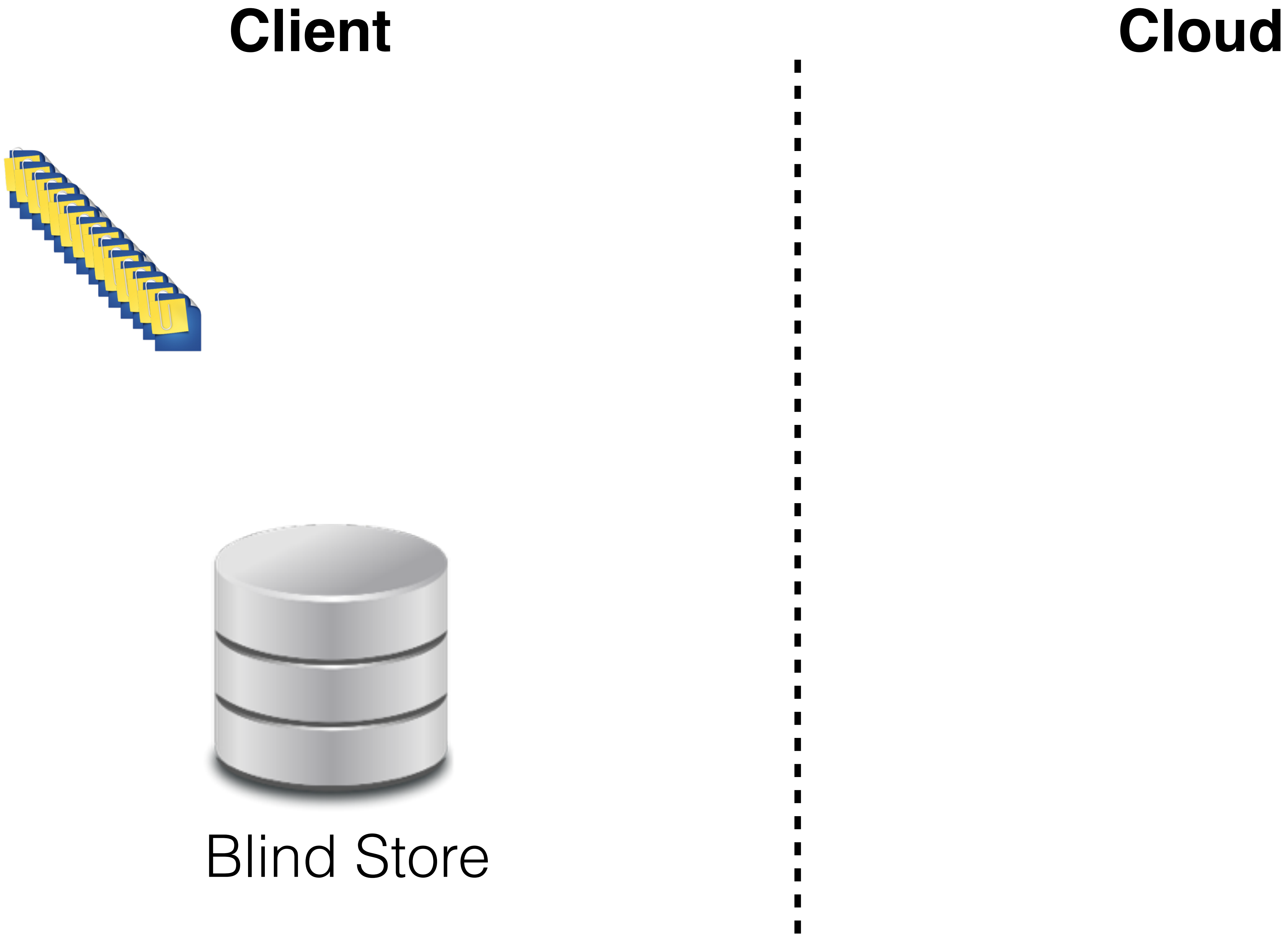


contents: **1,2**



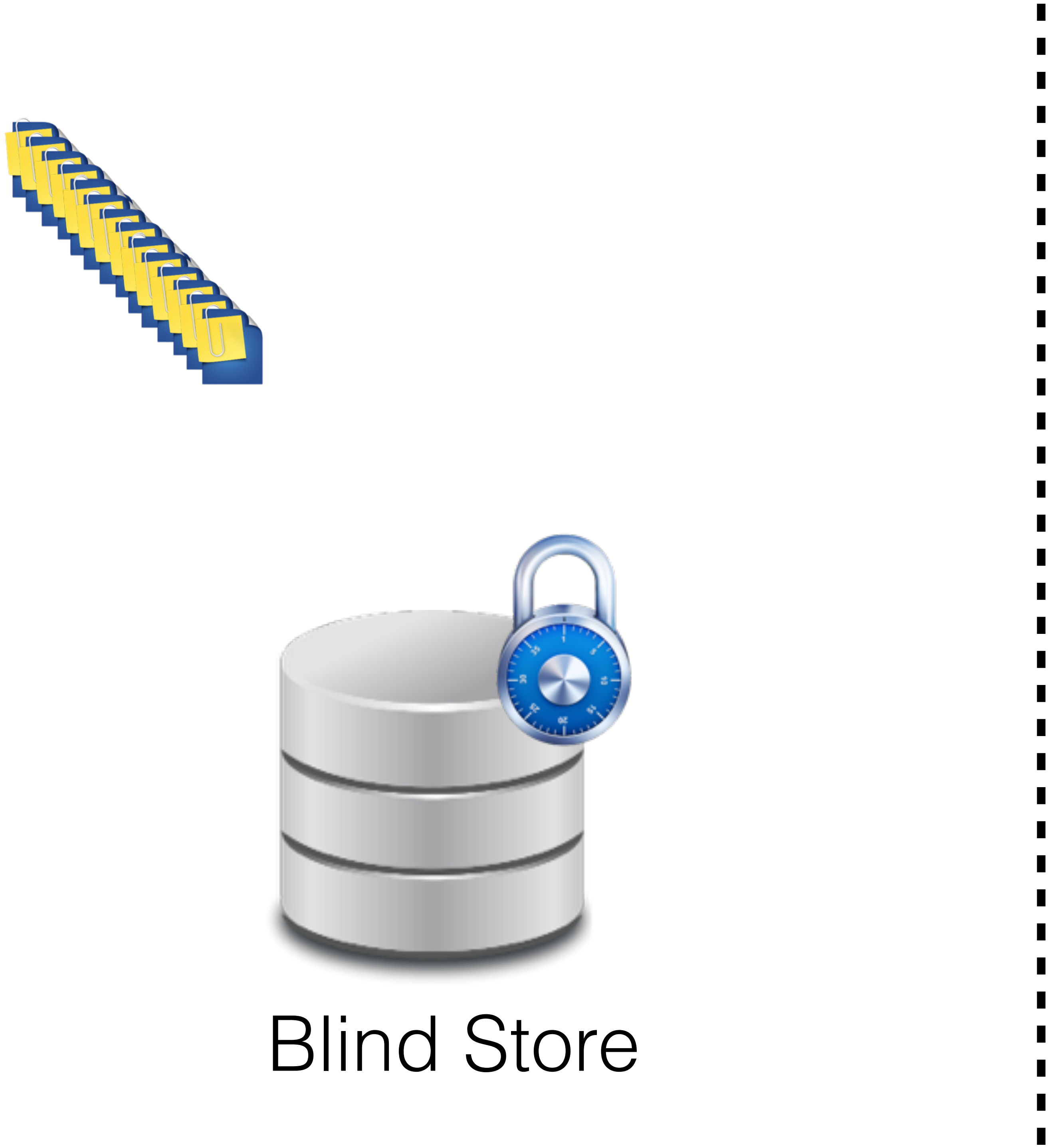
Blind Store

Setup



Setup

Client **Cloud**



Setup

Client **Cloud**

Blind Store

Setup

Client

Cloud

Blind Store

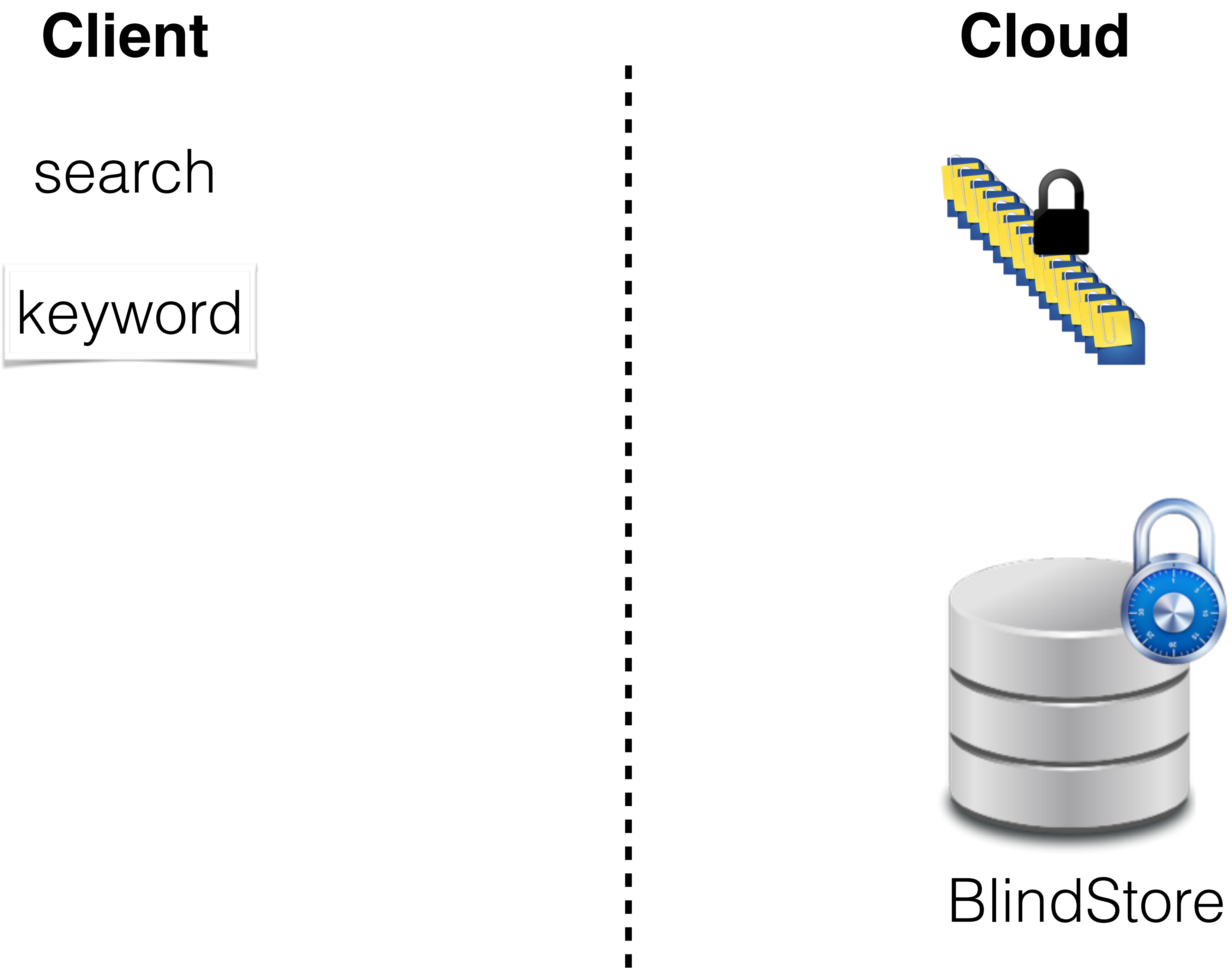
Search

Client

Cloud

BlindStore

Search



Client

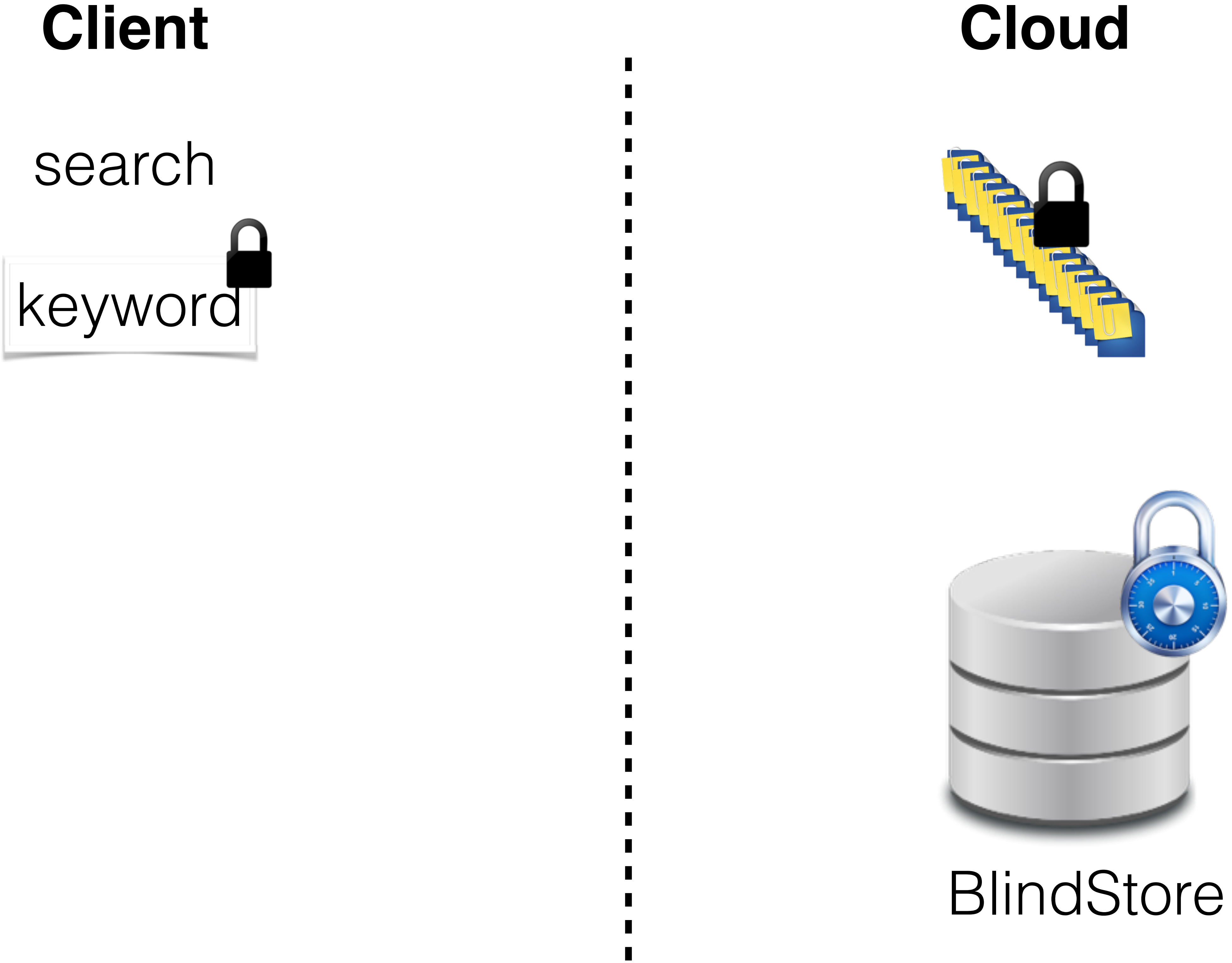
Cloud

search

keyword

BlindStore

Search



Client

search

keyword

Cloud

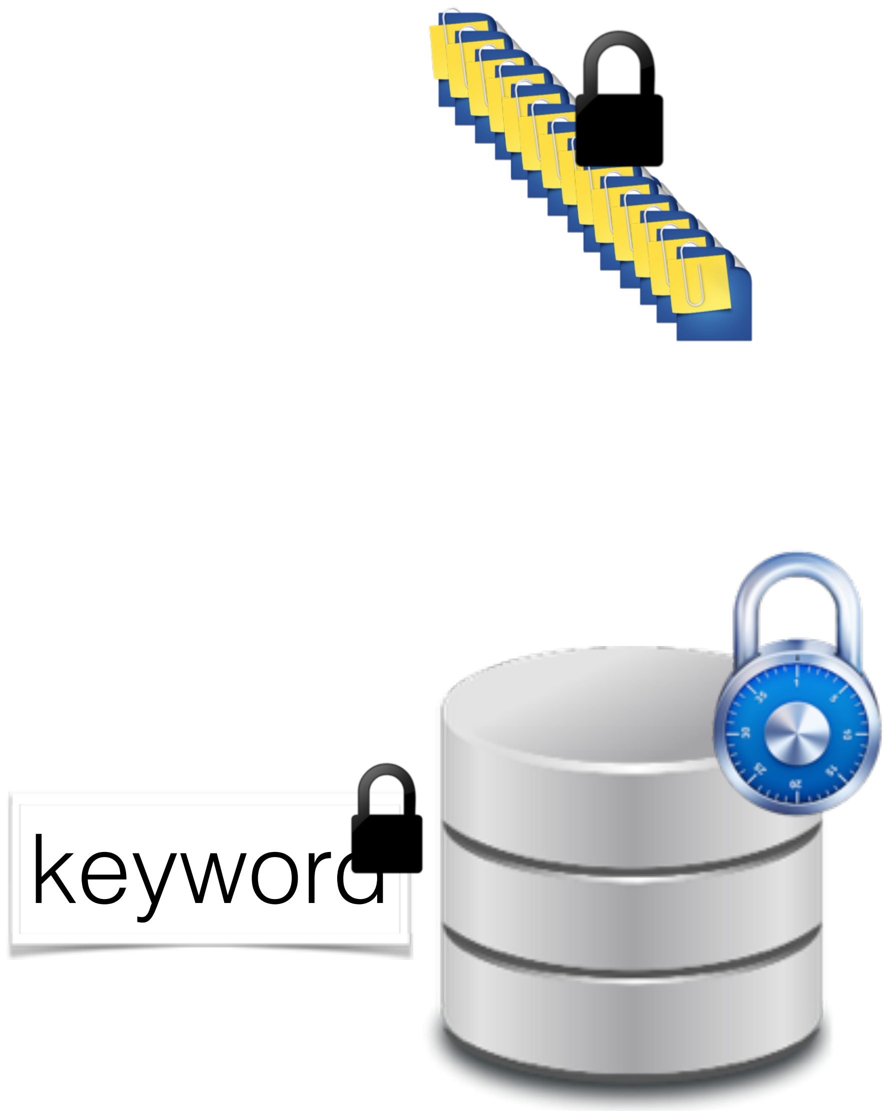
BlindStore

Search

Client

Cloud

search



keyword

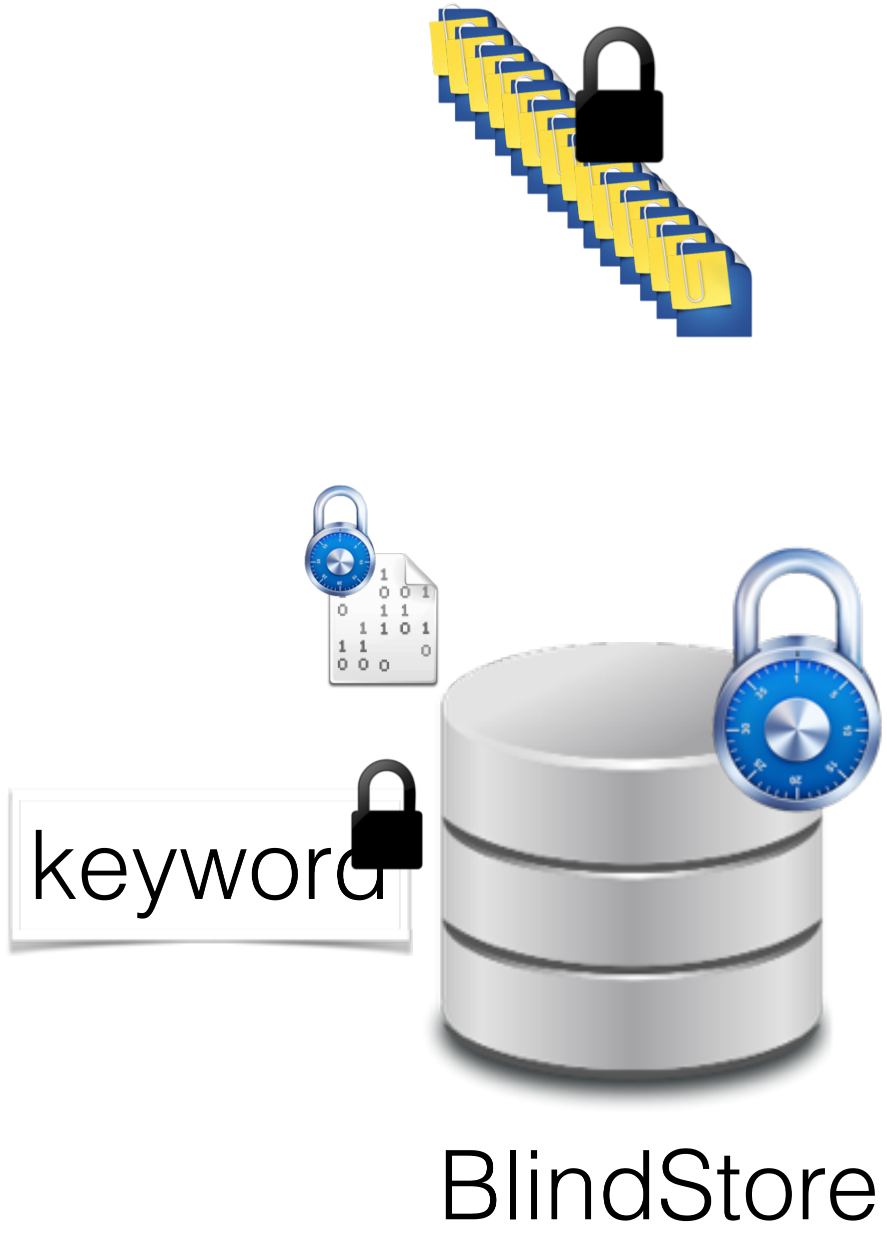
BlindStore

Search

Client

search

Cloud

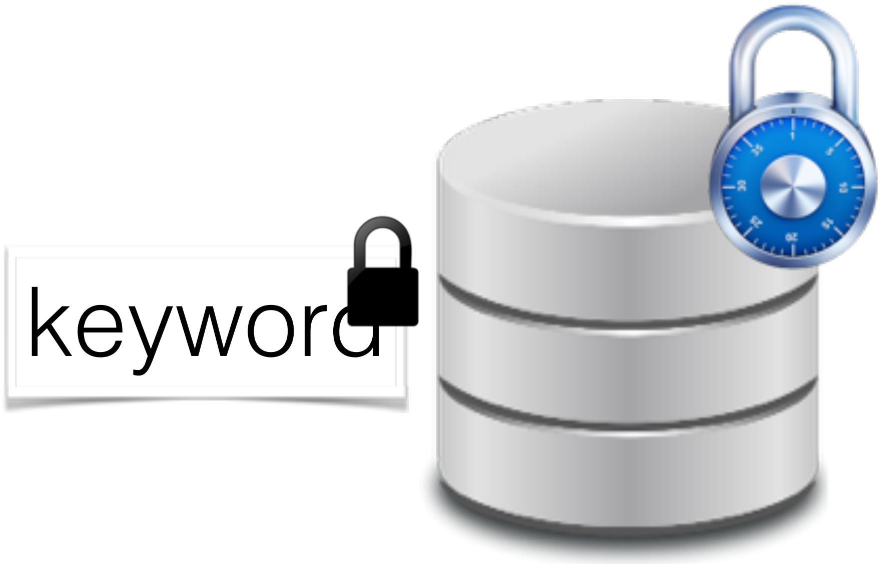


Search

Client

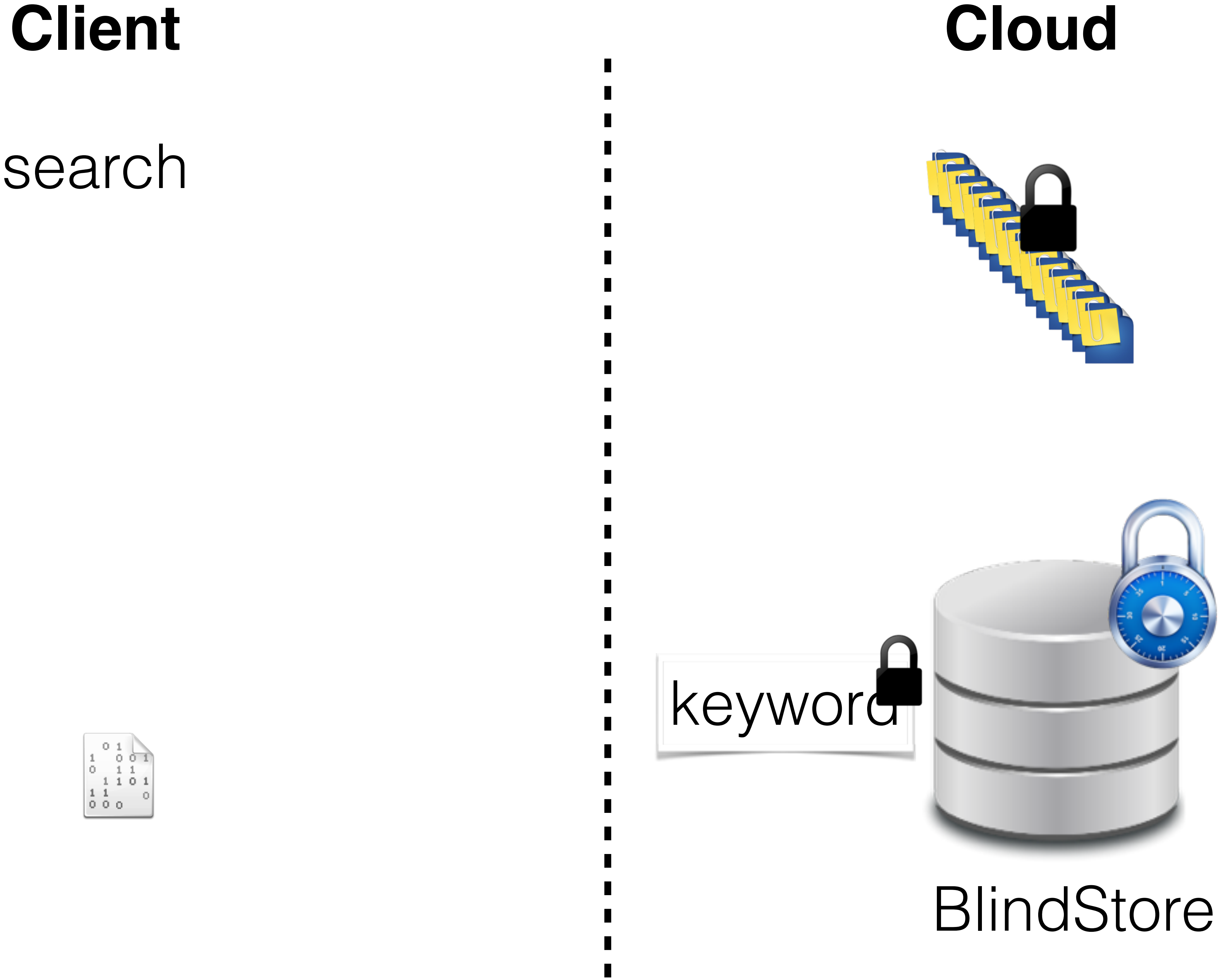
Cloud

search



BlindStore

Search



Client

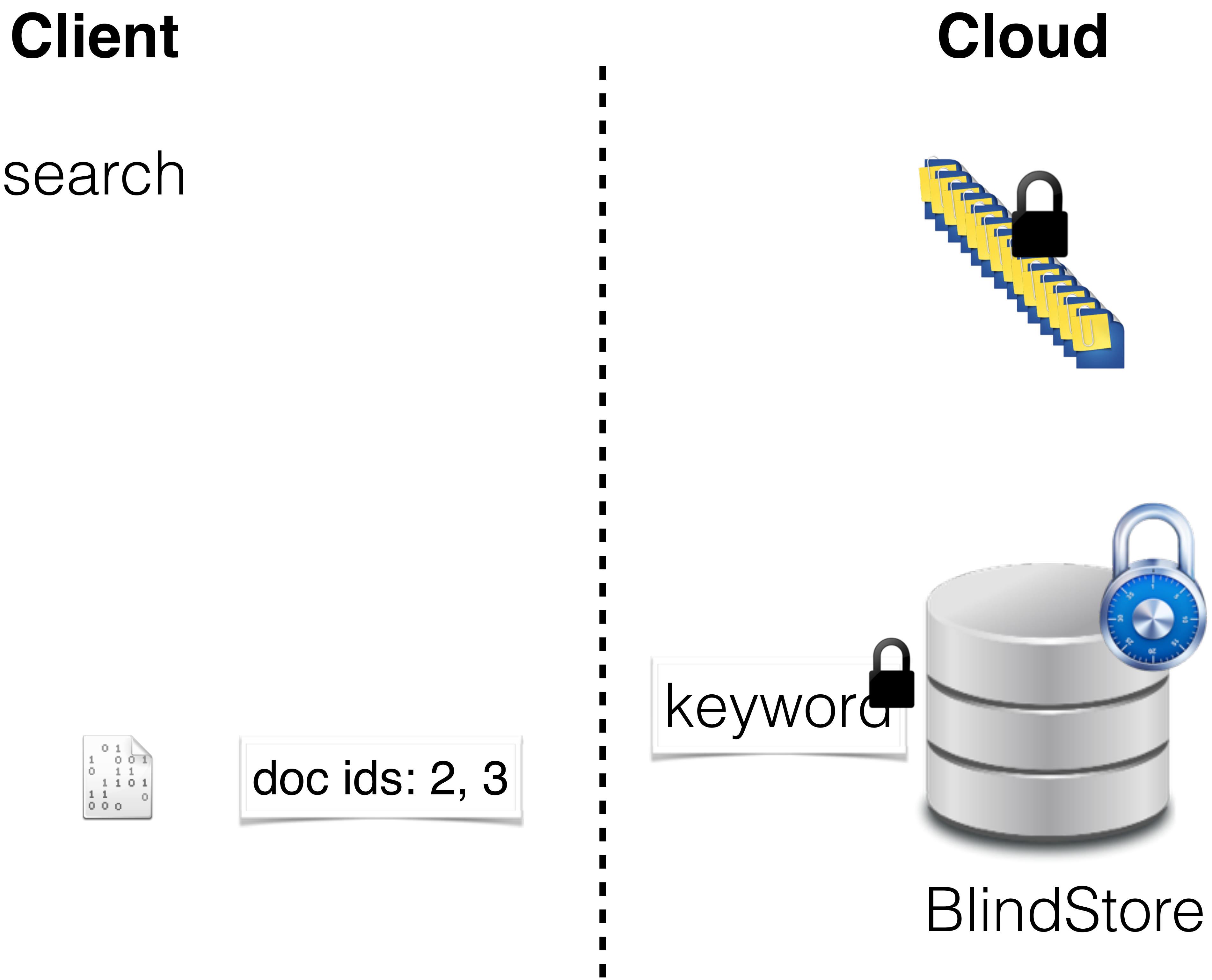
Cloud

search

keyword

BlindStore

Search



Client

Cloud

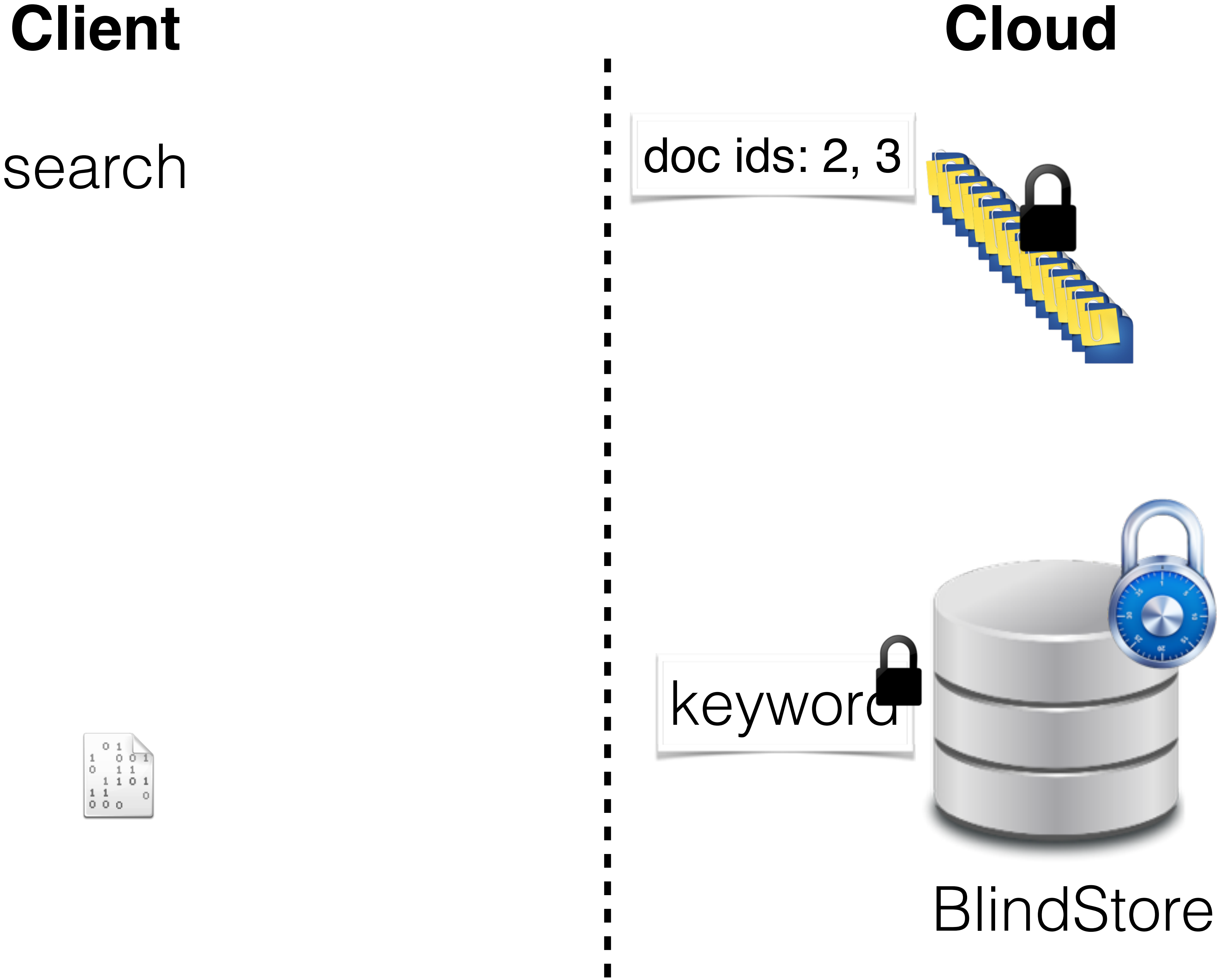
search

doc ids: 2, 3

keyword

BlindStore

Search



Client

Cloud

search

doc ids: 2, 3

keyword

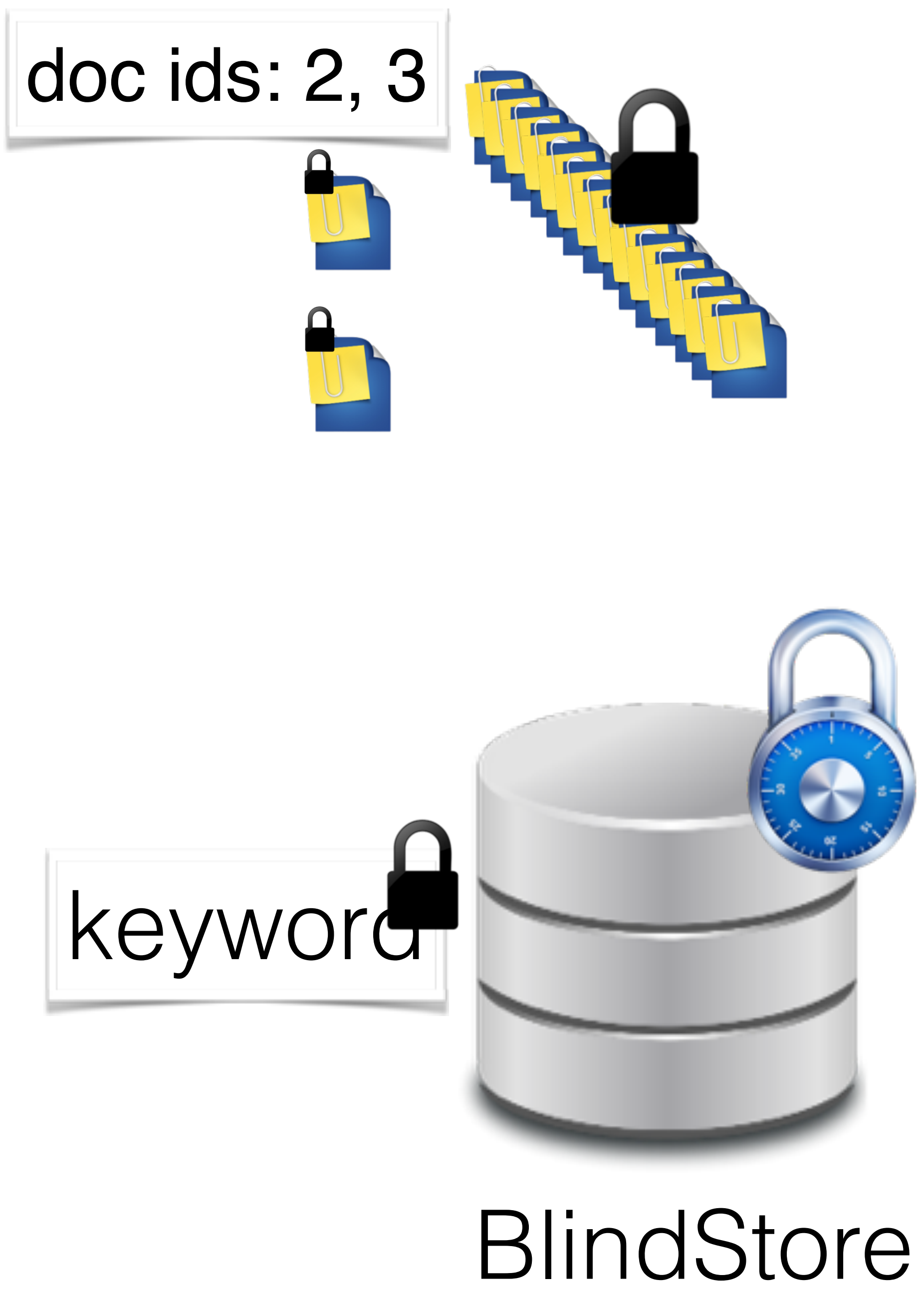
BlindStore

Search

Client

search

Cloud

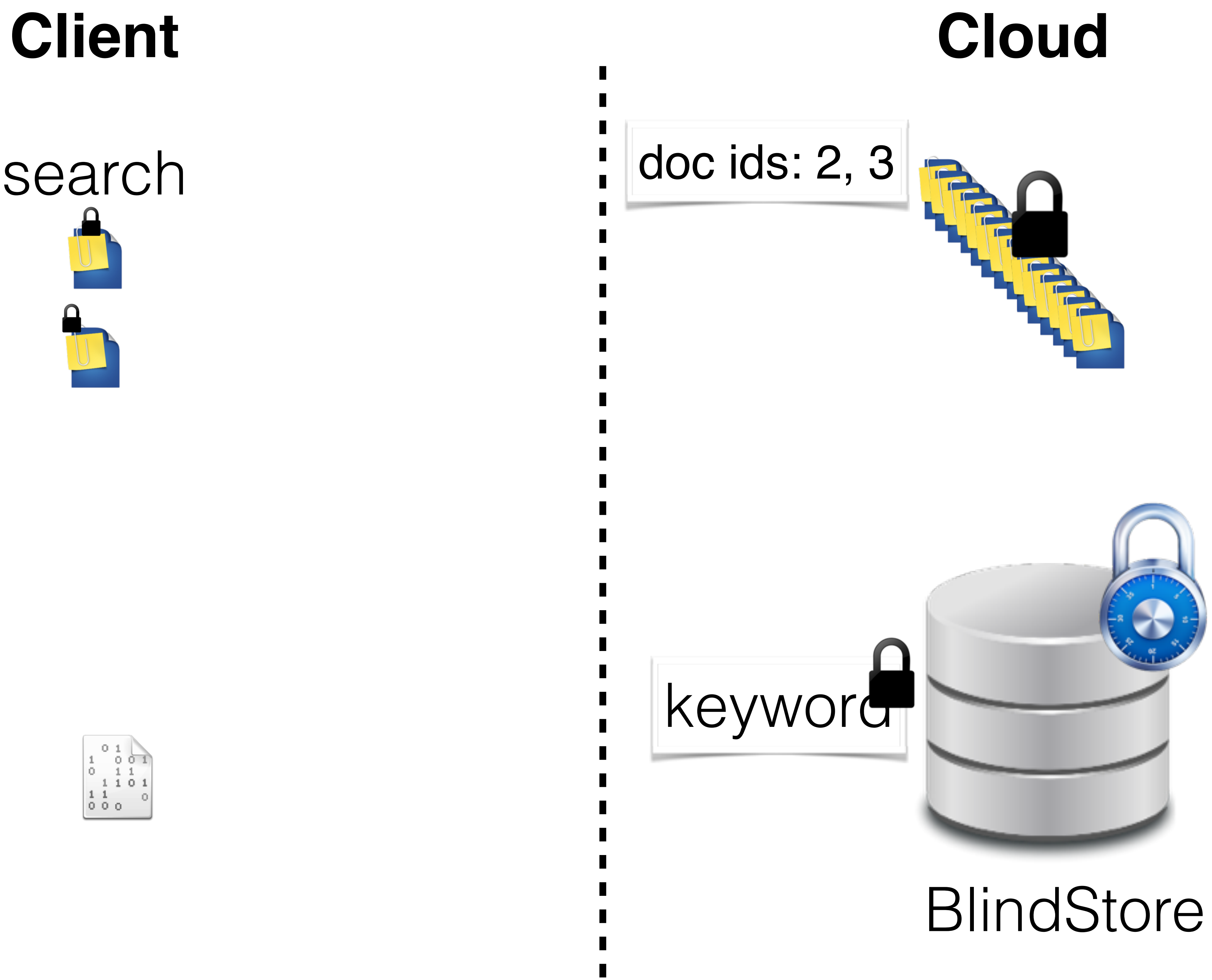


doc ids: 2, 3

keyword

BlindStore

Search



Client

Cloud

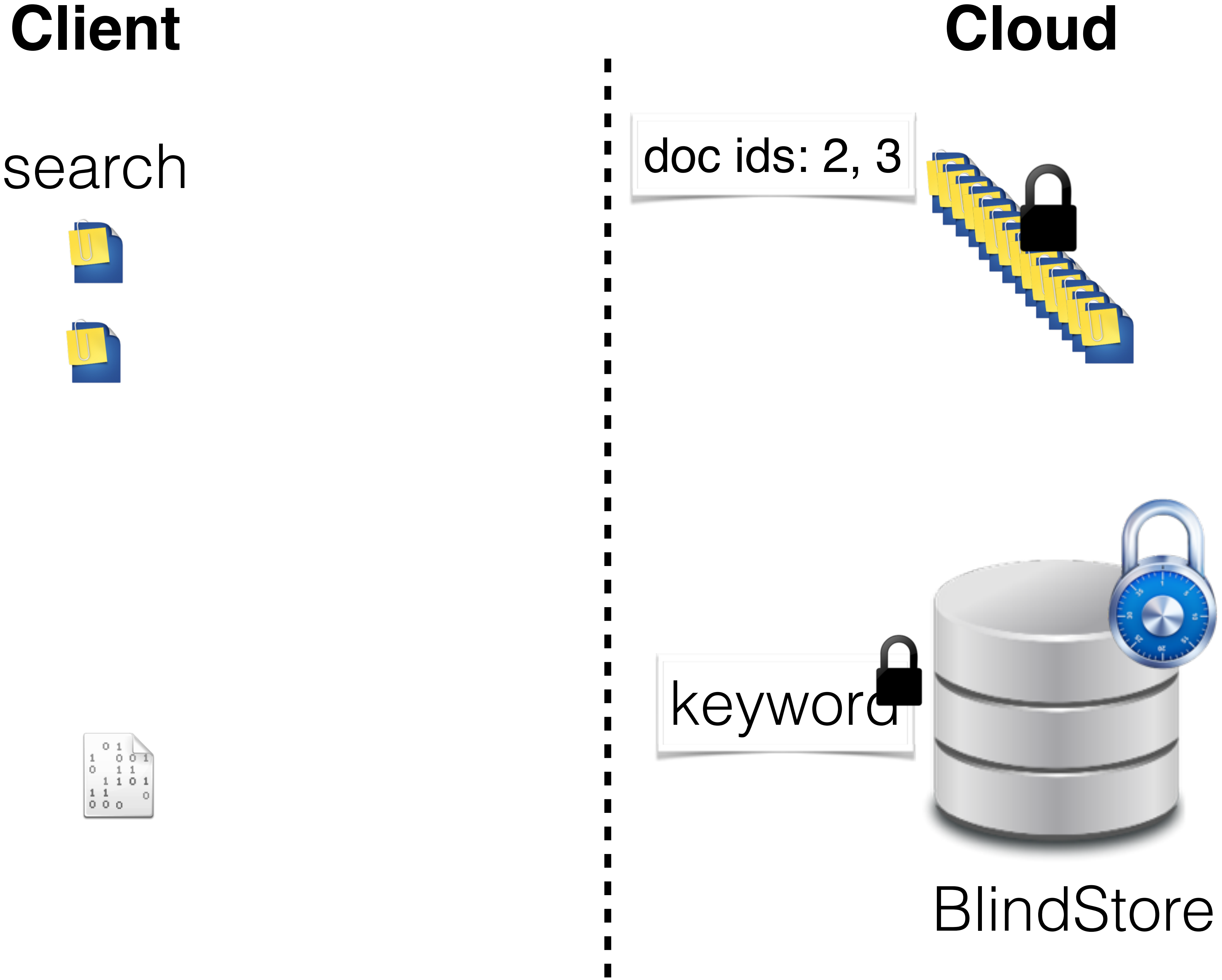
search

doc ids: 2, 3

keyword

BlindStore

Search



Client

Cloud

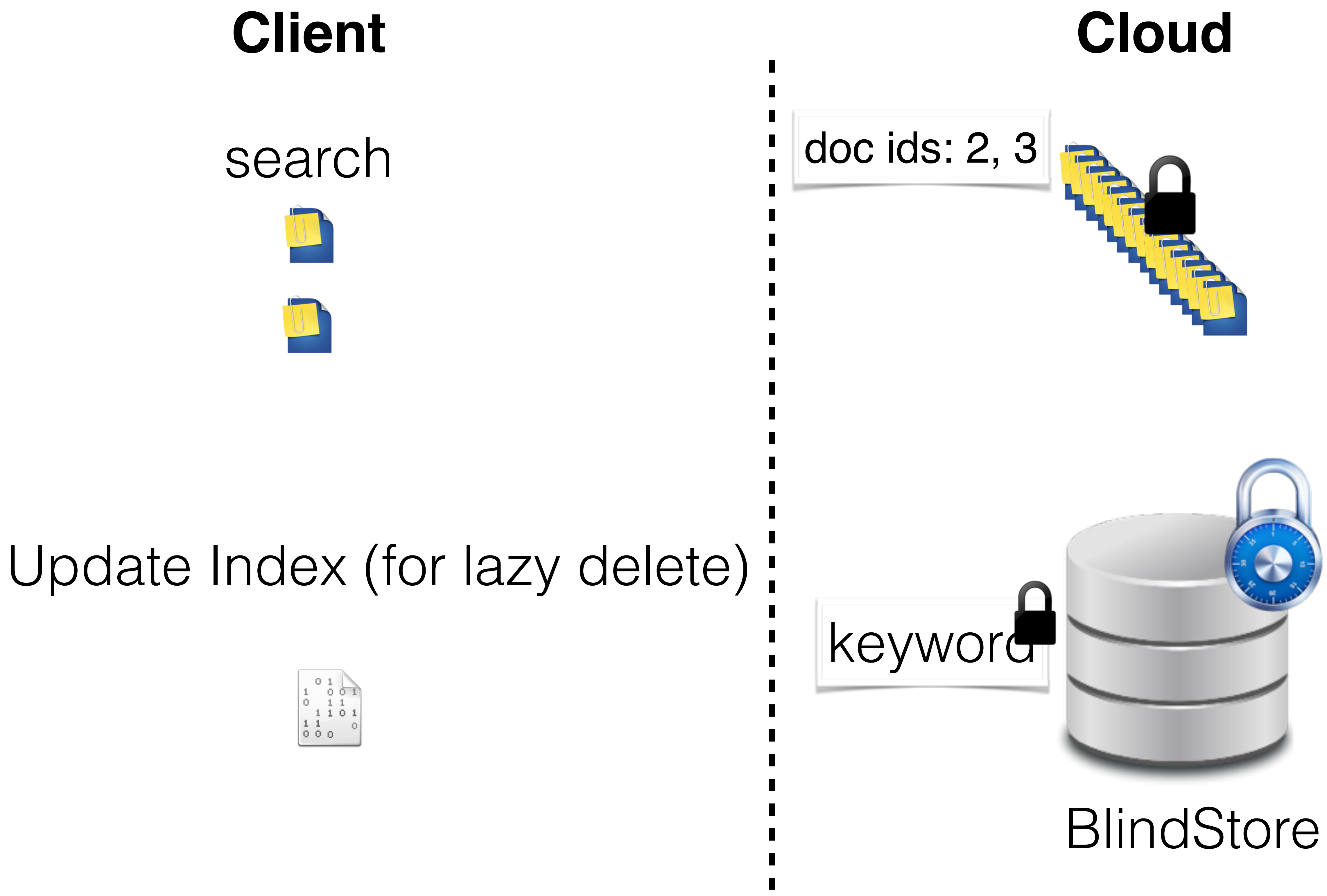
search

doc ids: 2, 3

keyword

BlindStore

Search



Client

Cloud

search

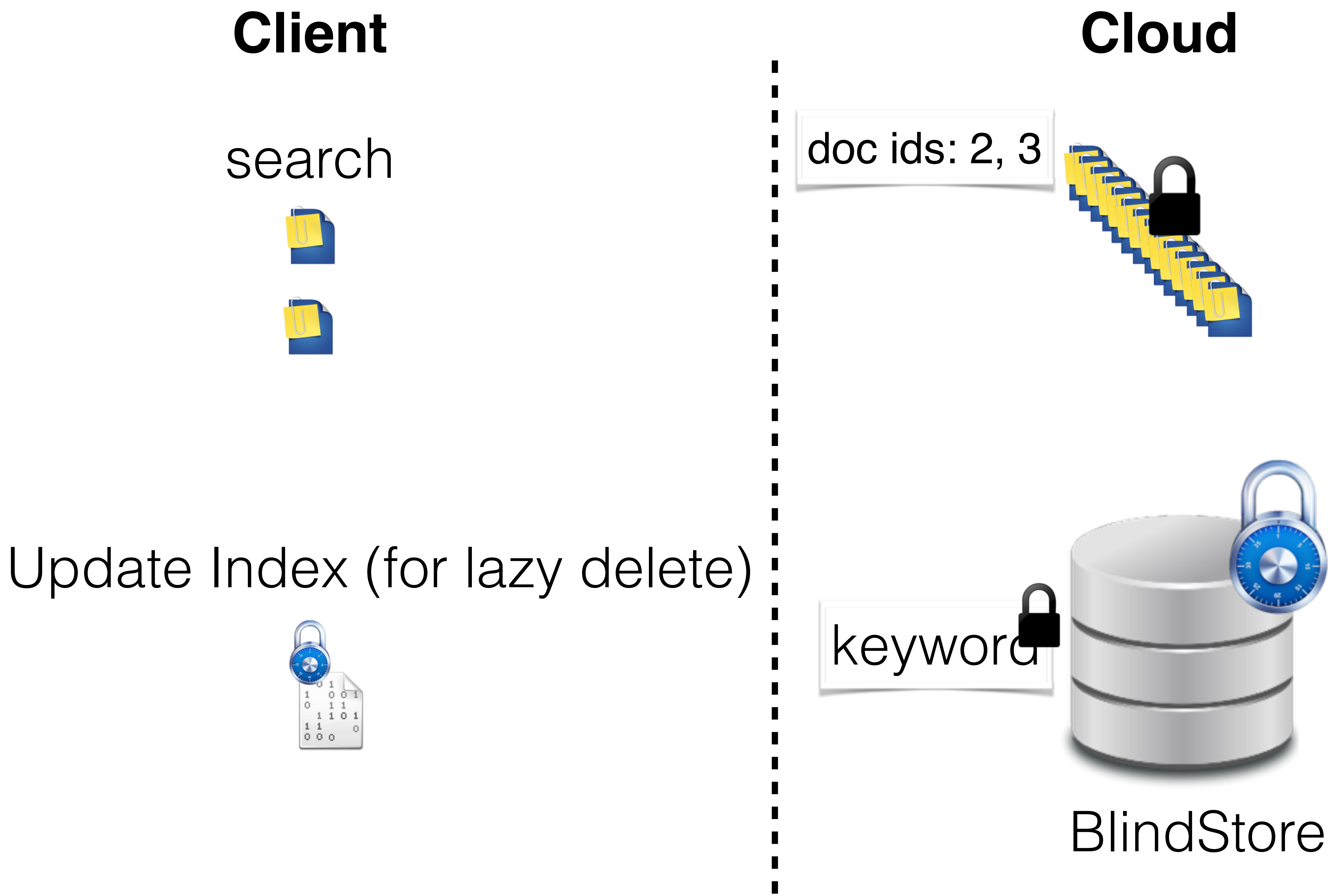
doc ids: 2, 3

Update Index (for lazy delete)

keyword

BlindStore

Search



Client

Cloud

search

doc ids: 2, 3

Update Index (for lazy delete)

keyword

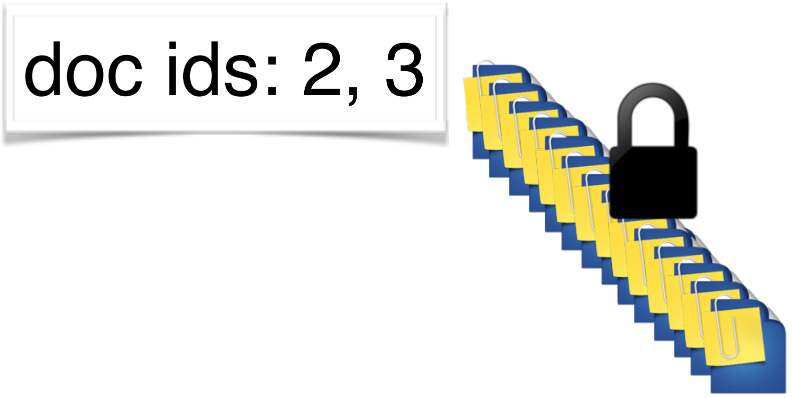
BlindStore

Search

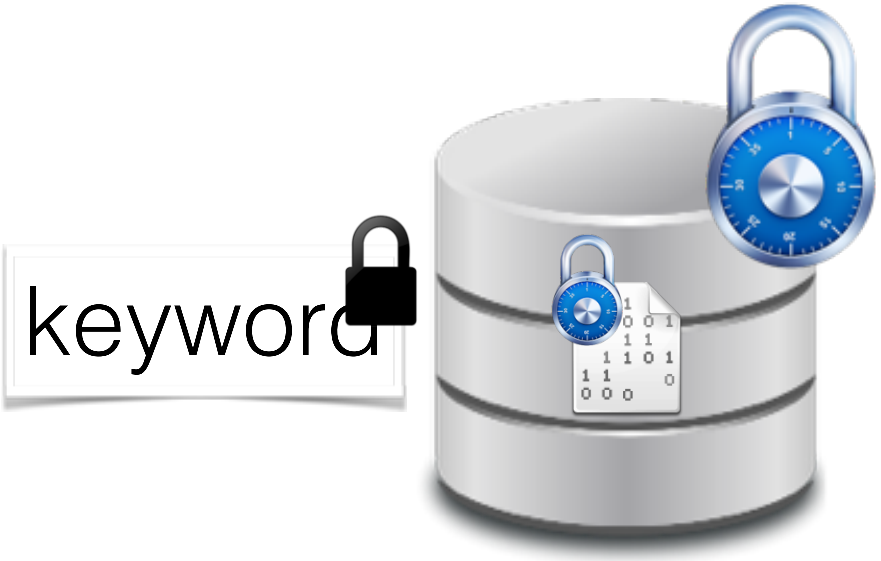
Client

Cloud

search



Update Index (for lazy delete)



BlindStore

Addition/Deletion

- All existing SSE schemes leak more during updates
  - Hashes of all the keywords in the new document are leaked
  - Presence of the same keyword in other documents
  - Delete leak even more

Addition/Deletion

- All existing SSE schemes leak more during updates
  - Hashes of all the keywords in the new document
  - Presence of the same keyword in other documents
  - Delete leak even more

BlindStorage is not required for the newly added documents

ClearStore

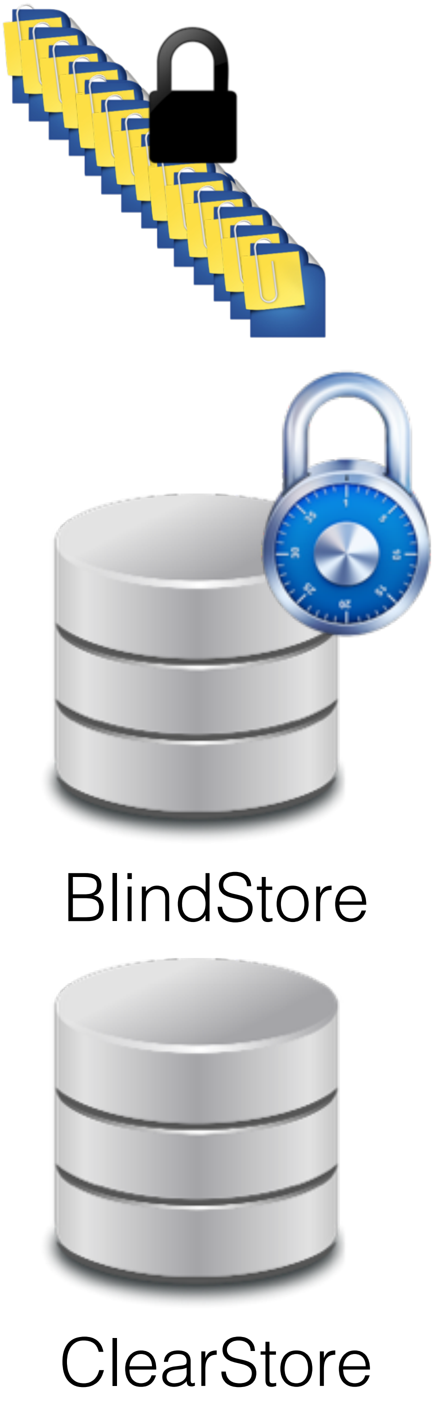
- New files are stored in ClearStore
- Store files unencrypted
- Supports constant time append operation
    - Requires downloading three blocks and uploading two blocks

ClearStore

Add

Client

Cloud



BlindStore

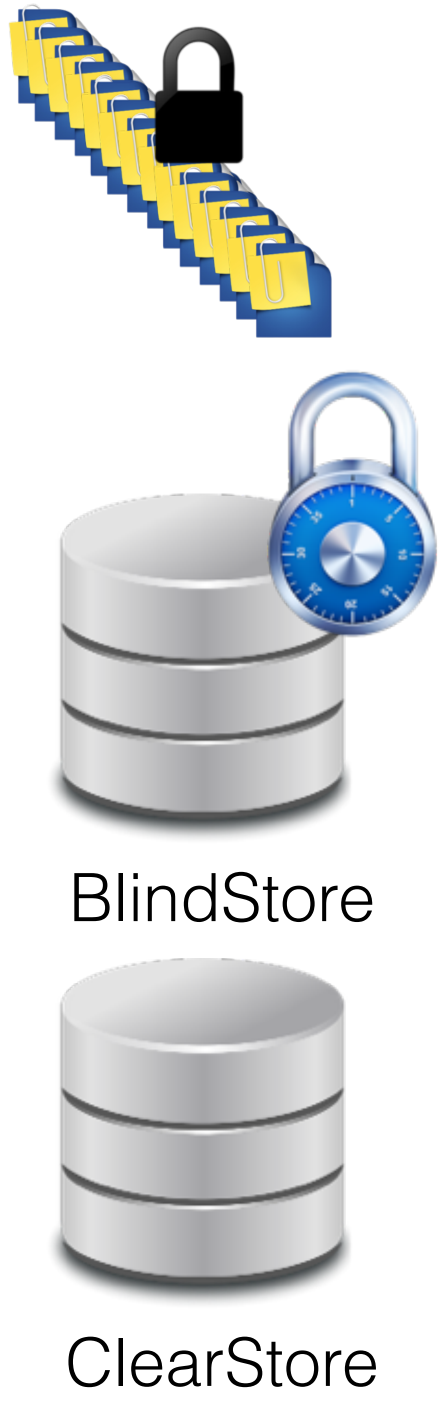
ClearStore

Add

Client

Cloud

add



Add

Client

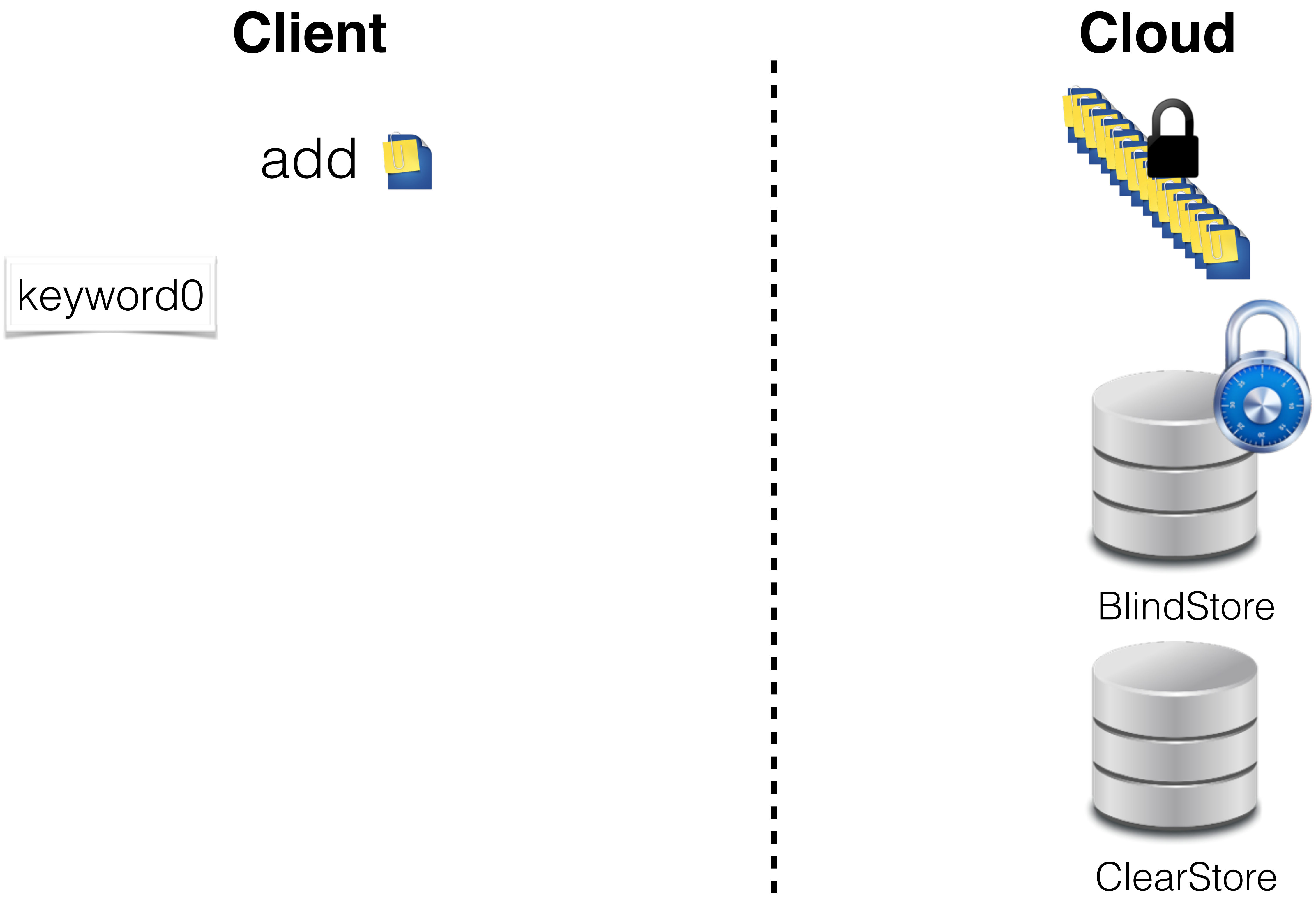
add

Cloud

BlindStore

ClearStore

Add



Client

Cloud

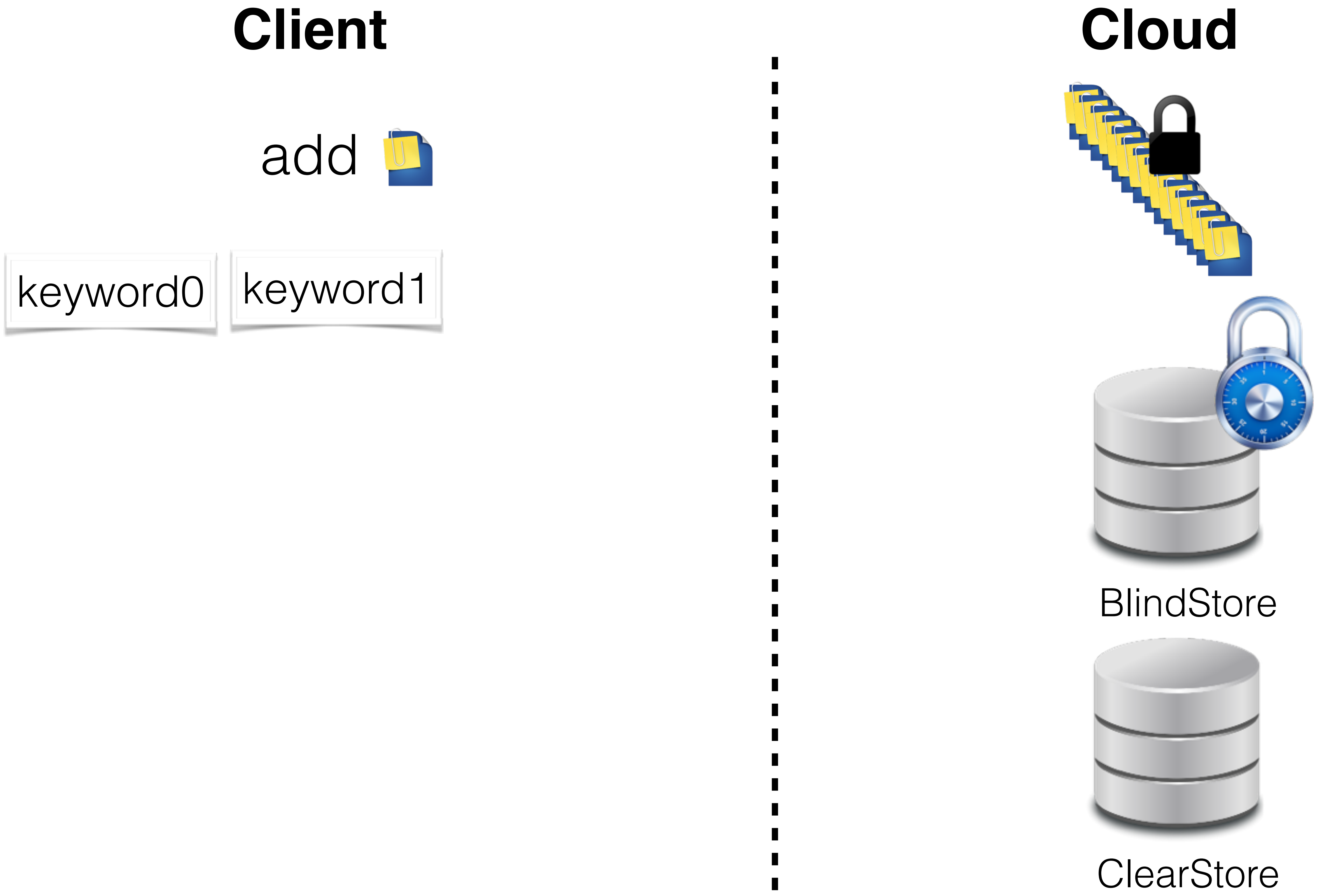
add

keyword0

BlindStore

ClearStore

Add



Client

add

keyword0 keyword1

Cloud

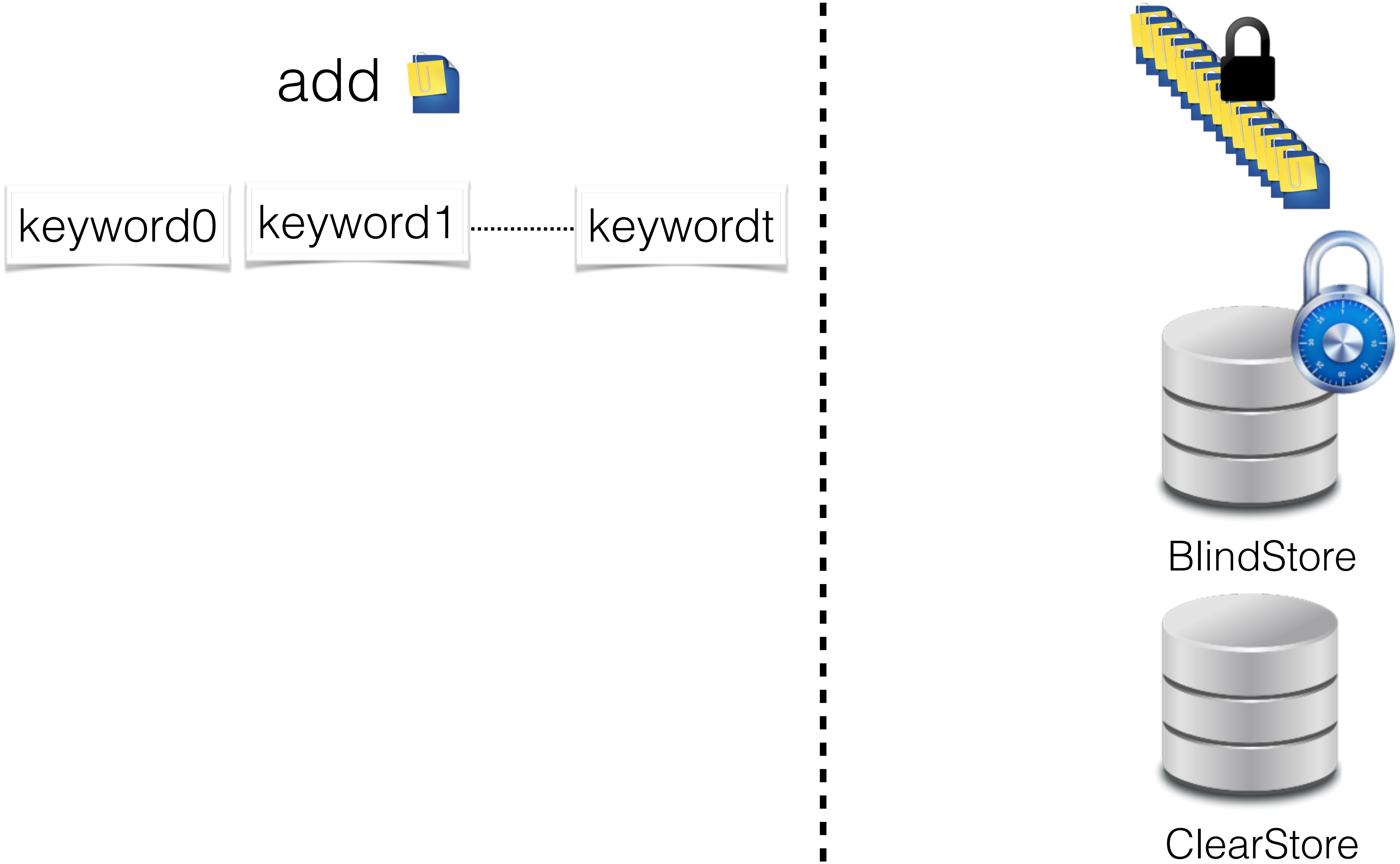
BlindStore

ClearStore

Add

Client

Cloud



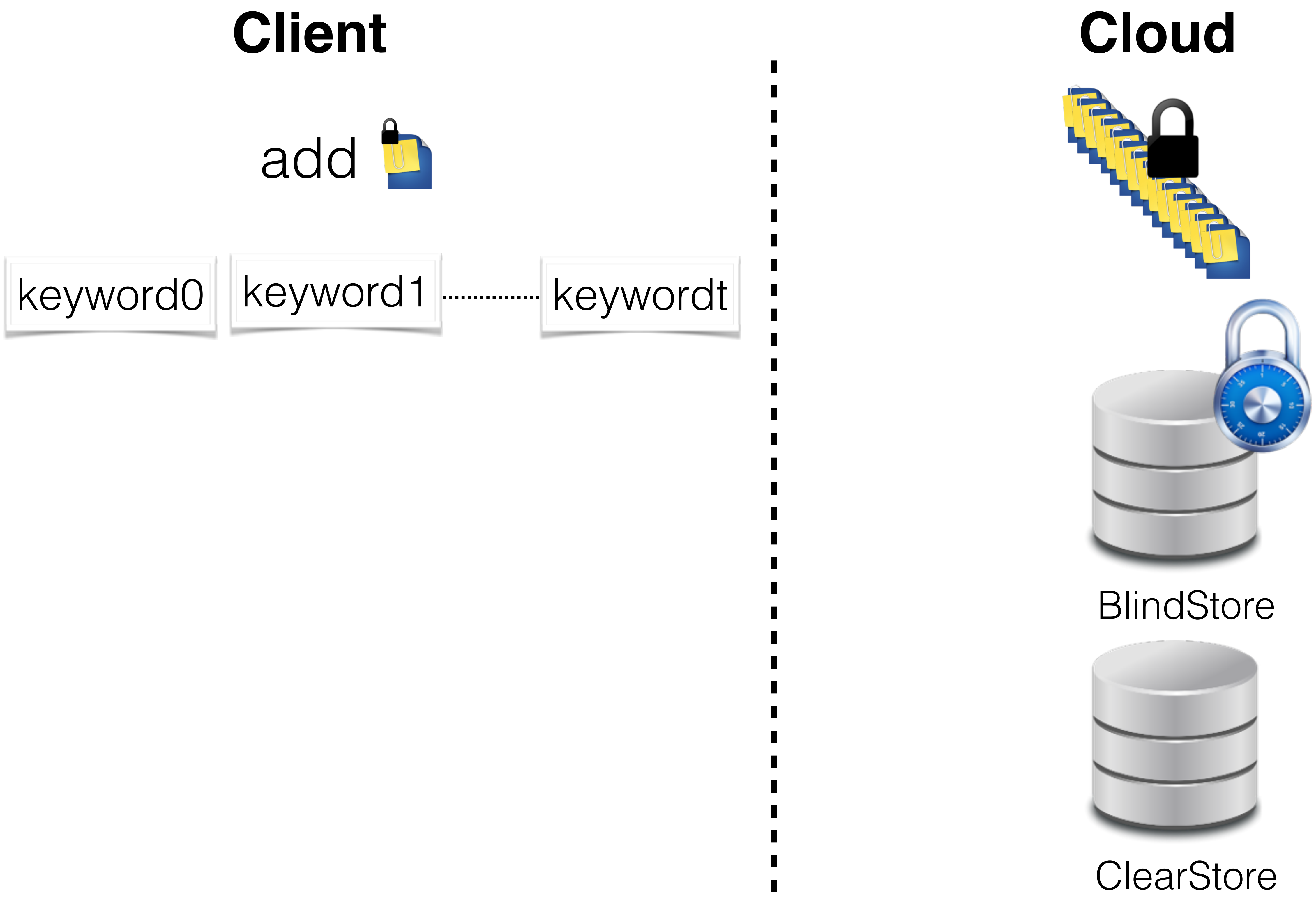
add

keyword0 keyword1 .... keywordt

BlindStore

ClearStore

Add



Client

Cloud

add

keyword0

keyword1

keywordt

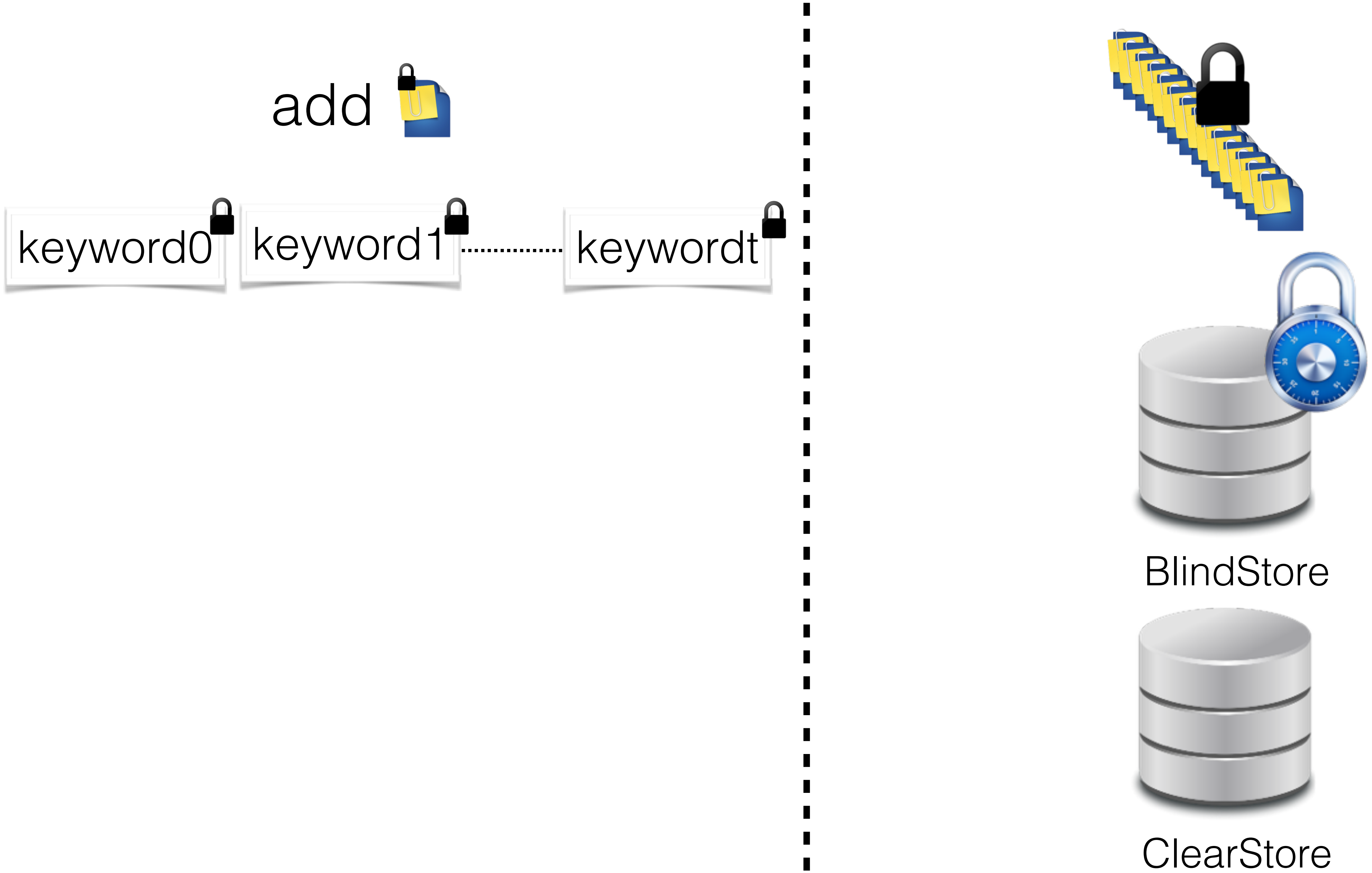
BlindStore

ClearStore

Add

Client

Cloud



add

keyword0 keyword1 keywordt

BlindStore

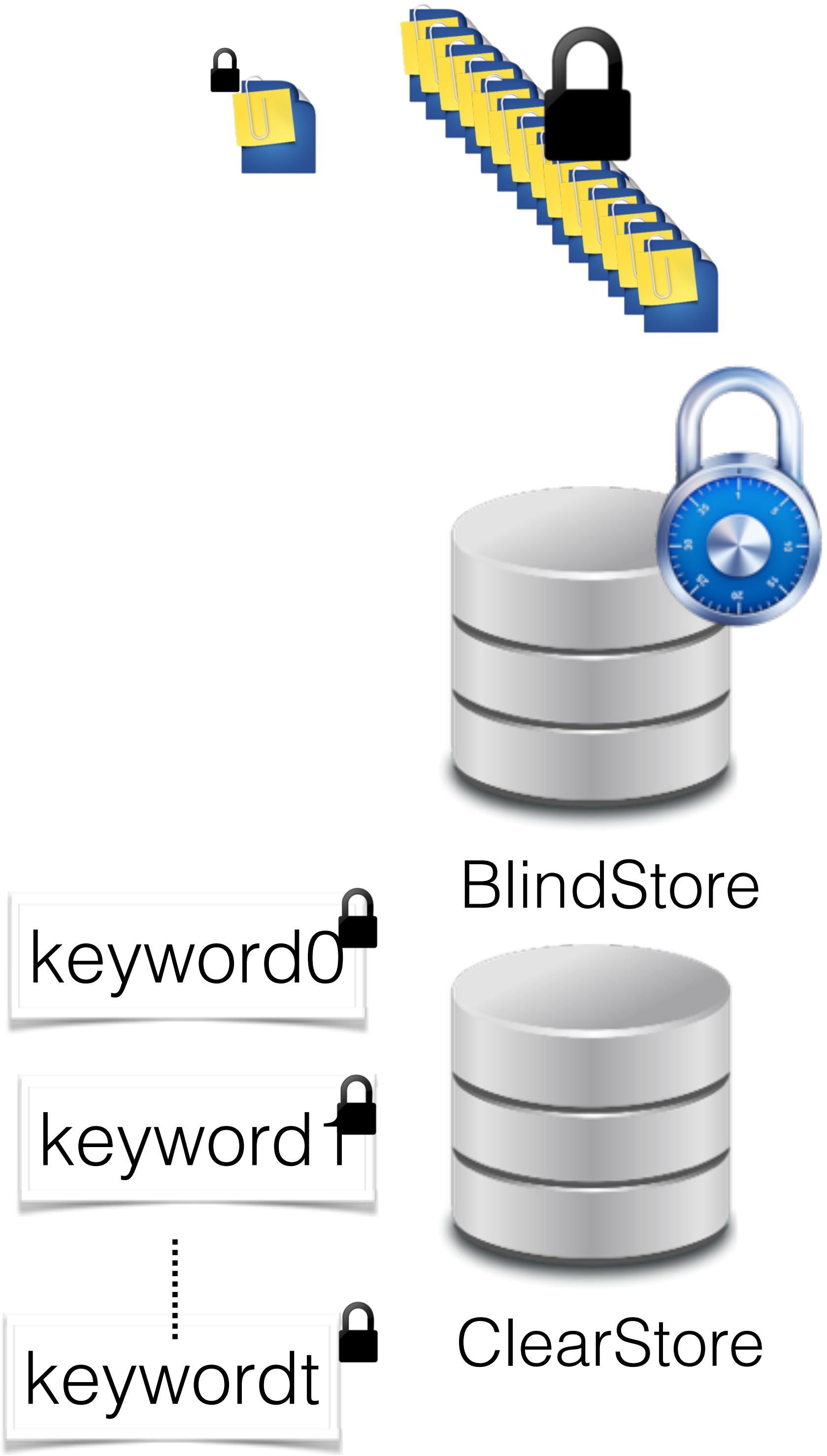
ClearStore

Add

Client

add

Cloud

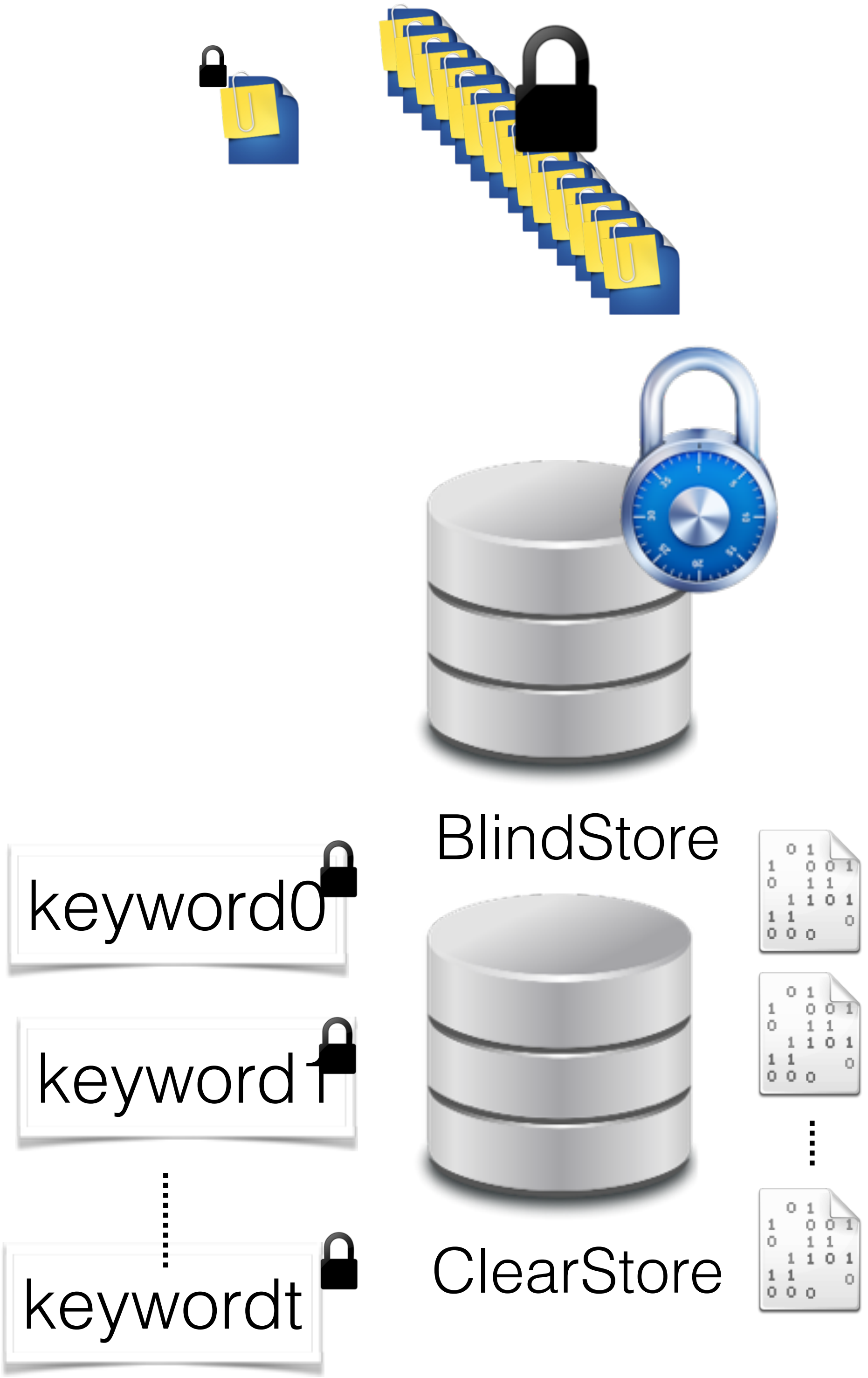


Add

Client

add

Cloud



keyword0

keyword1

keywordt

BlindStore

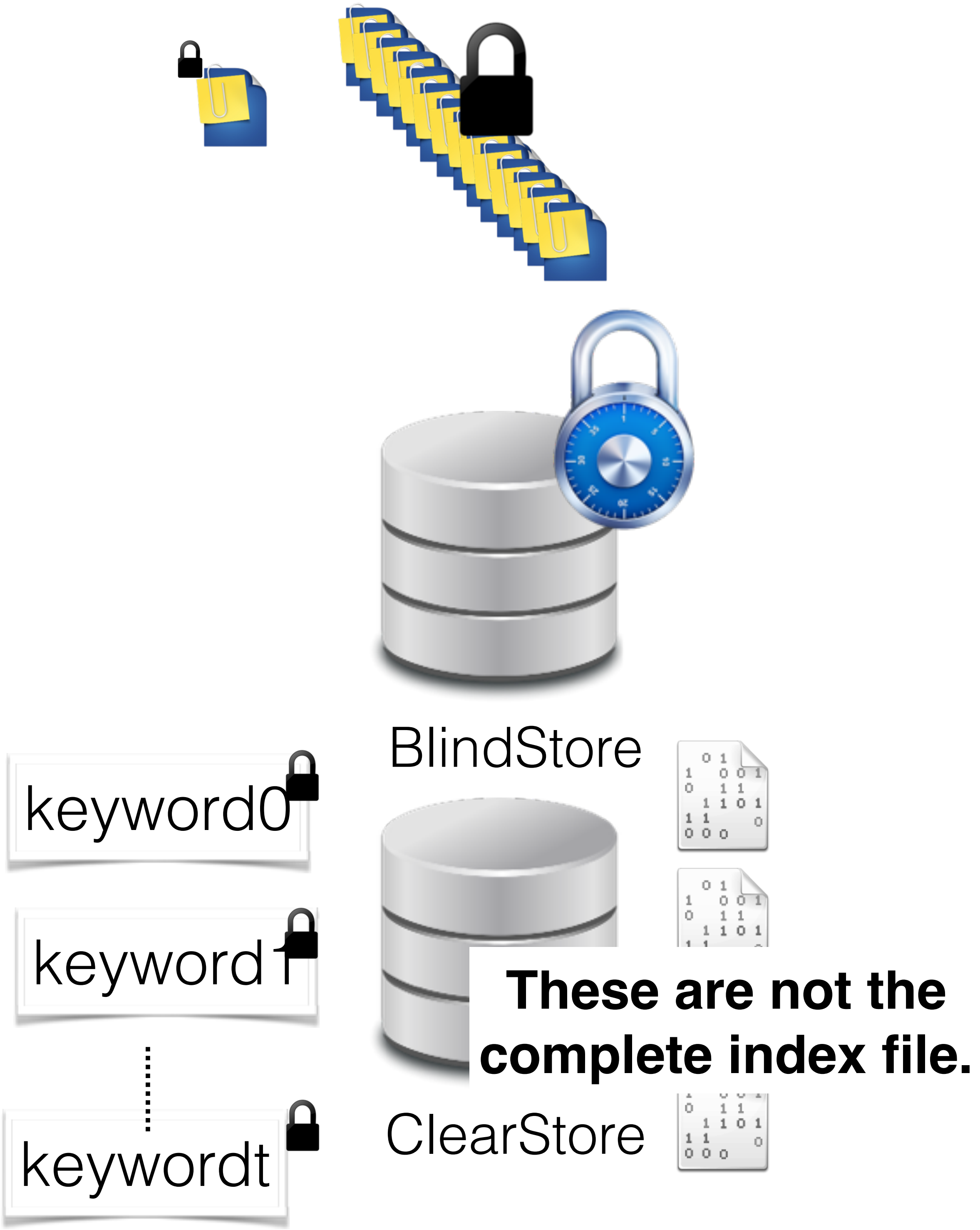
ClearStore

Add

Client

Cloud

add



keyword0

keyword1

keywordt

BlindStore

ClearStore

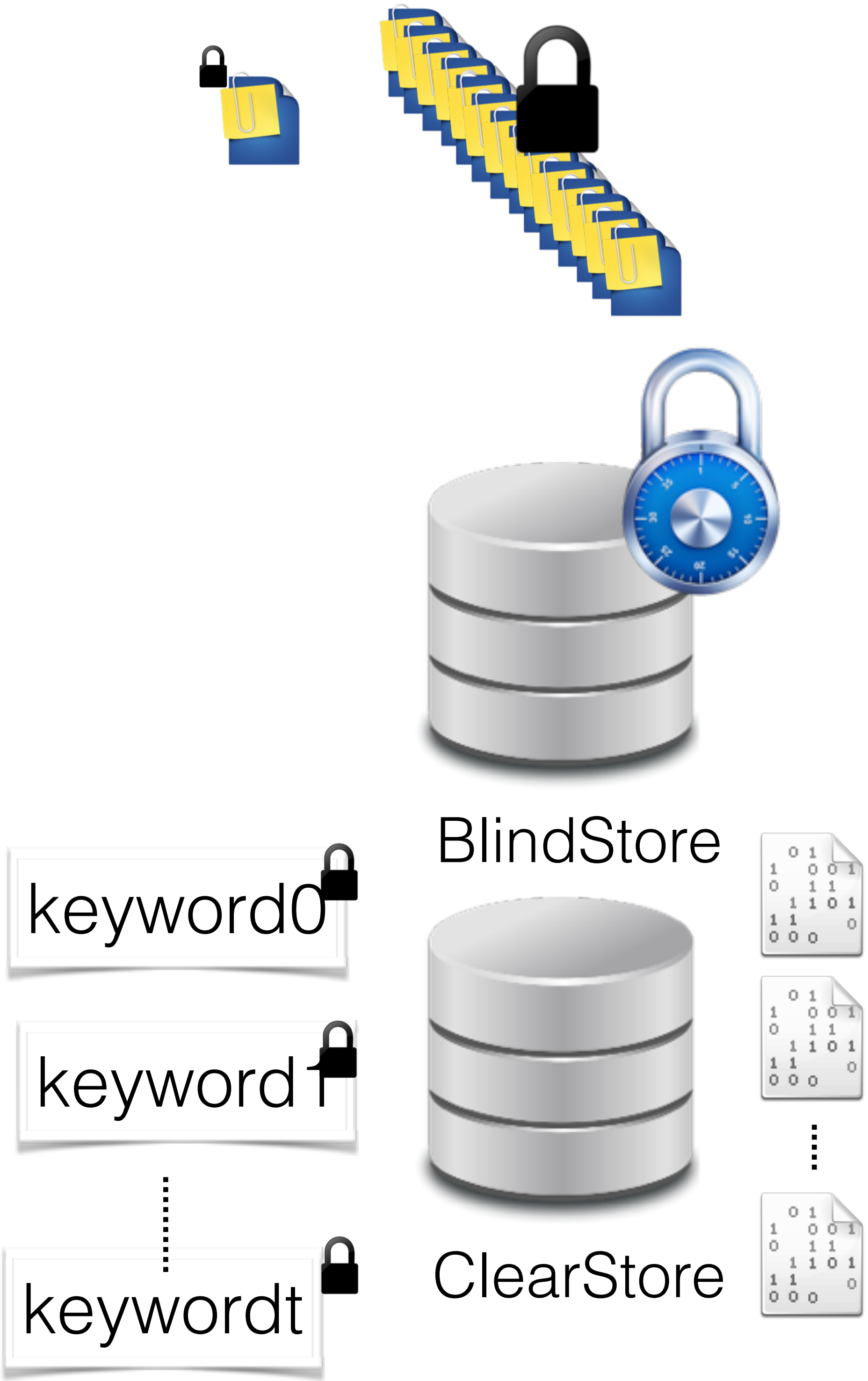
These are not the complete index file.

Add

Client

add

Cloud



BlindStore

keyword0

keyword1

keywordt

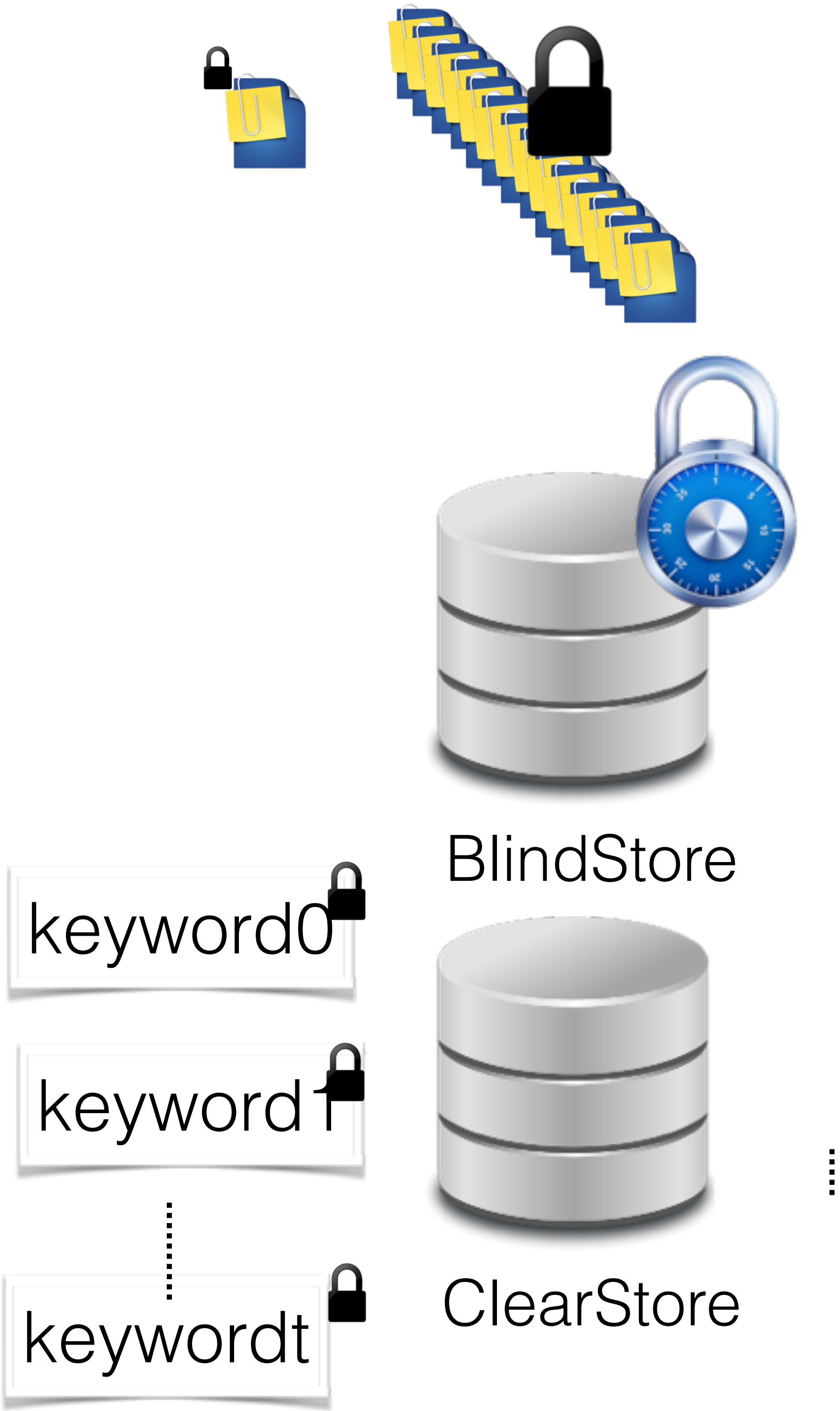
ClearStore

Add

Client

Cloud

add



BlindStore

ClearStore

keyword0

keyword1

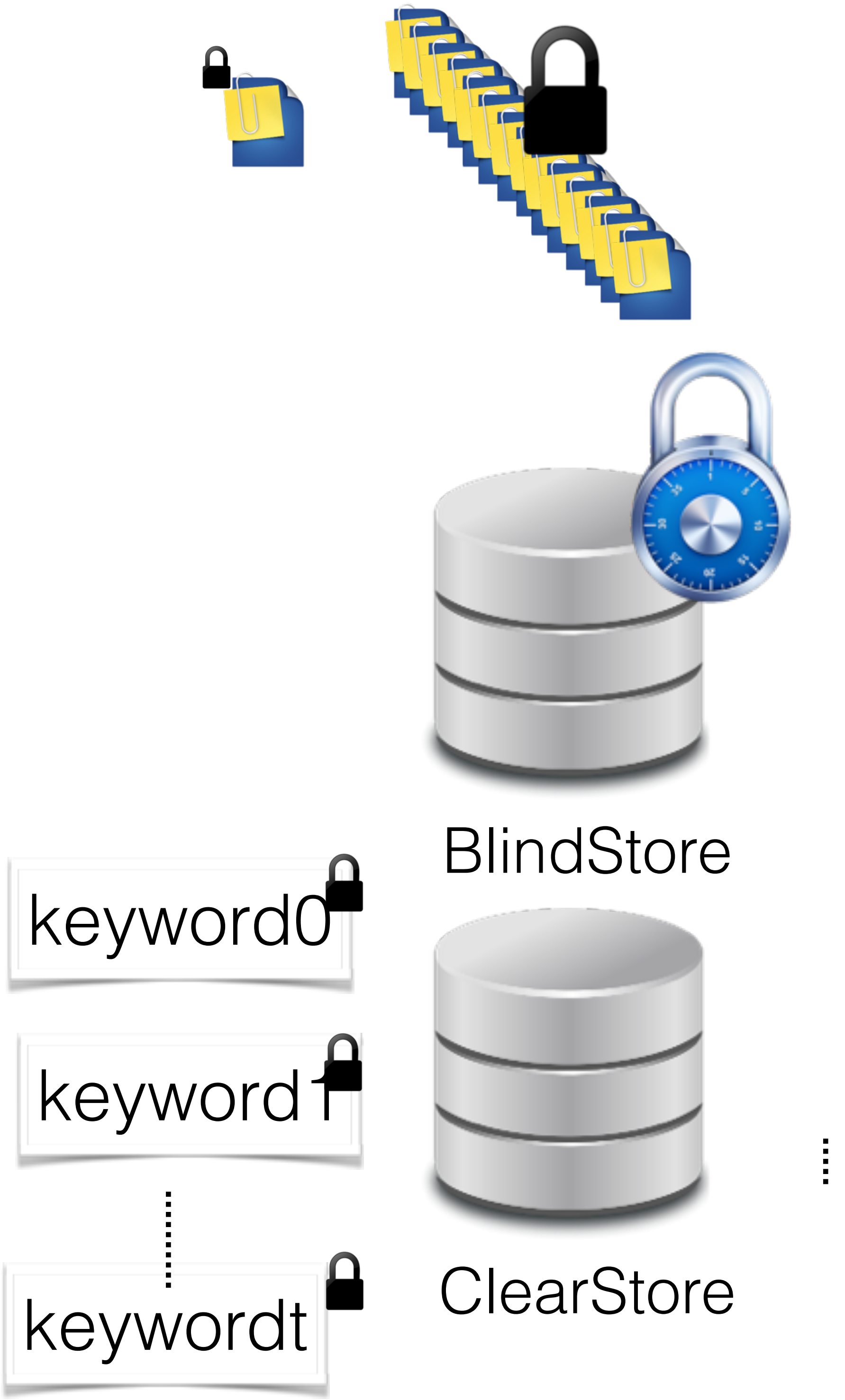
keywordt

Add

Client

Cloud

add



keyword0

keyword1

keywordt

BlindStore

ClearStore

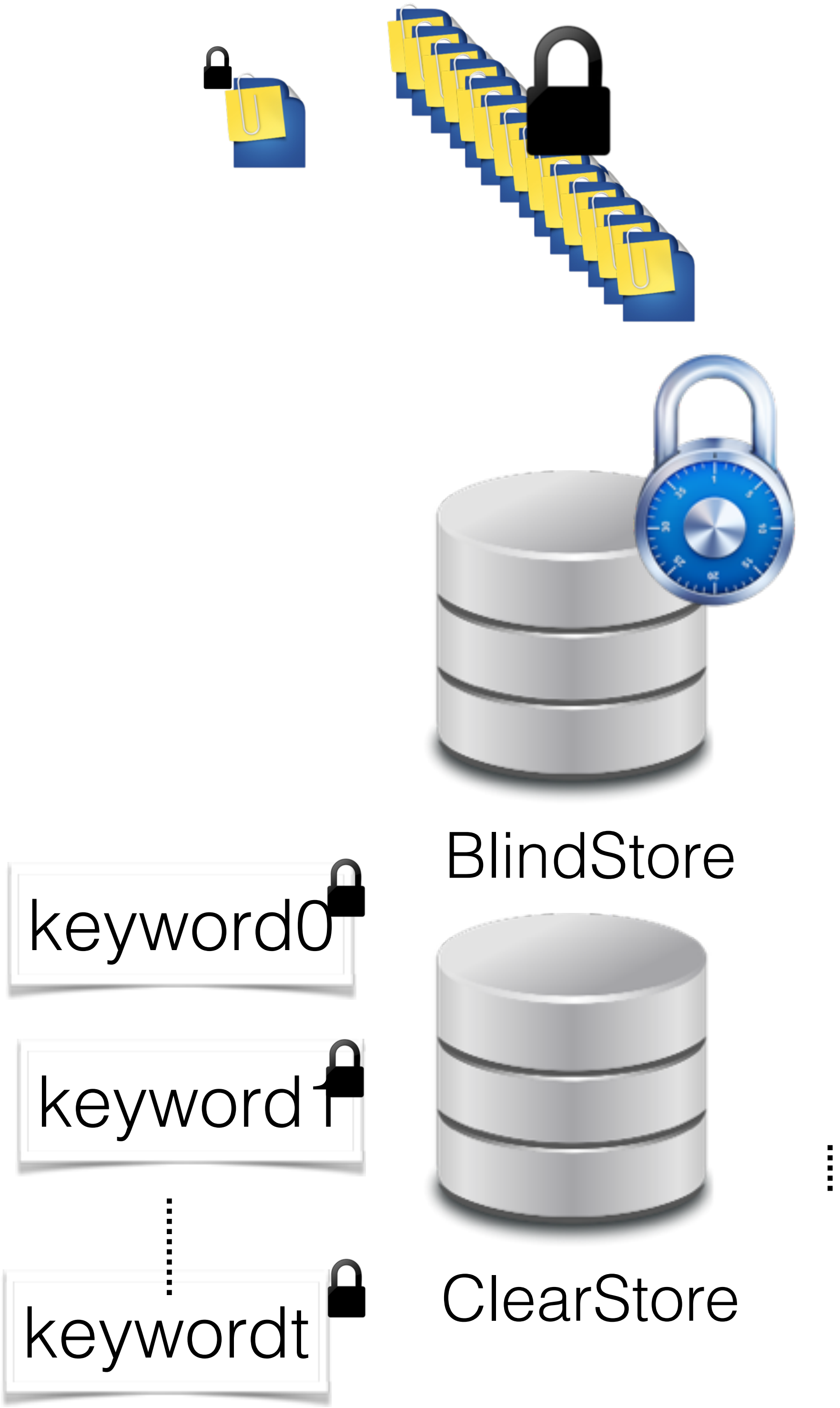
Add id of the new document

Add

Client

Cloud

add



keyword0

keyword1

keywordt

BlindStore

ClearStore

Add id of the new document

Delete is free

Client

Cloud

Blind Virtual Disk

Delete is free

Client

delete

Cloud

doc ID

Blind Virtual Disk

Delete is free

Client

delete

Cloud

doc ID

Blind Virtual Disk

Delete is free

Client

Cloud

delete

doc ID

Blind Virtual Disk

Lazy Delete Strategy

Client

Cloud

BlindStore

Lazy Delete Strategy

Client

search

keyword

Cloud

BlindStore

Lazy Delete Strategy

Client

Cloud

search

keyword

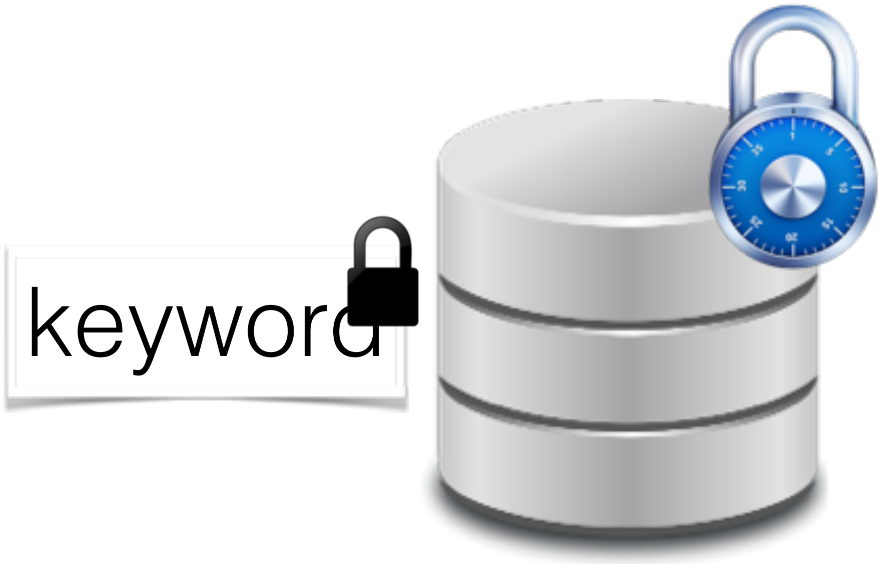
BlindStore

Lazy Delete Strategy

Client

Cloud

search



keyword

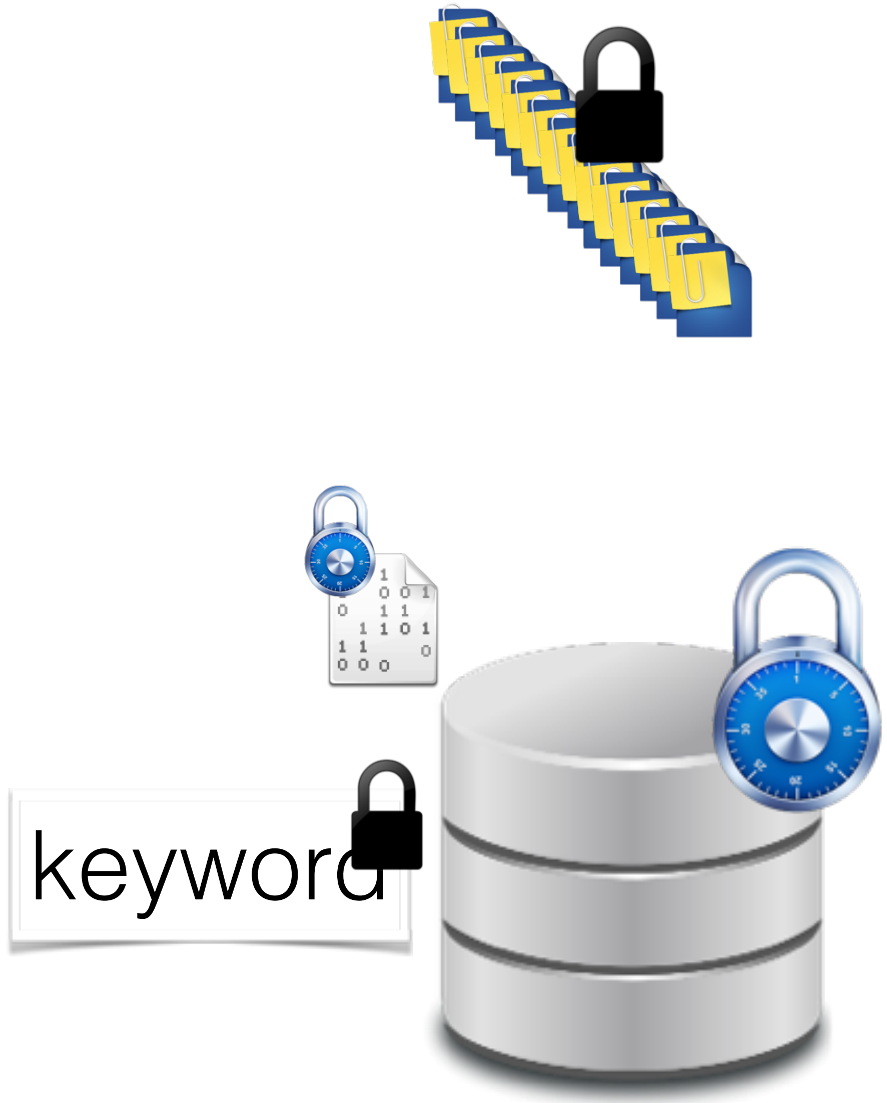
BlindStore

Lazy Delete Strategy

Client

Cloud

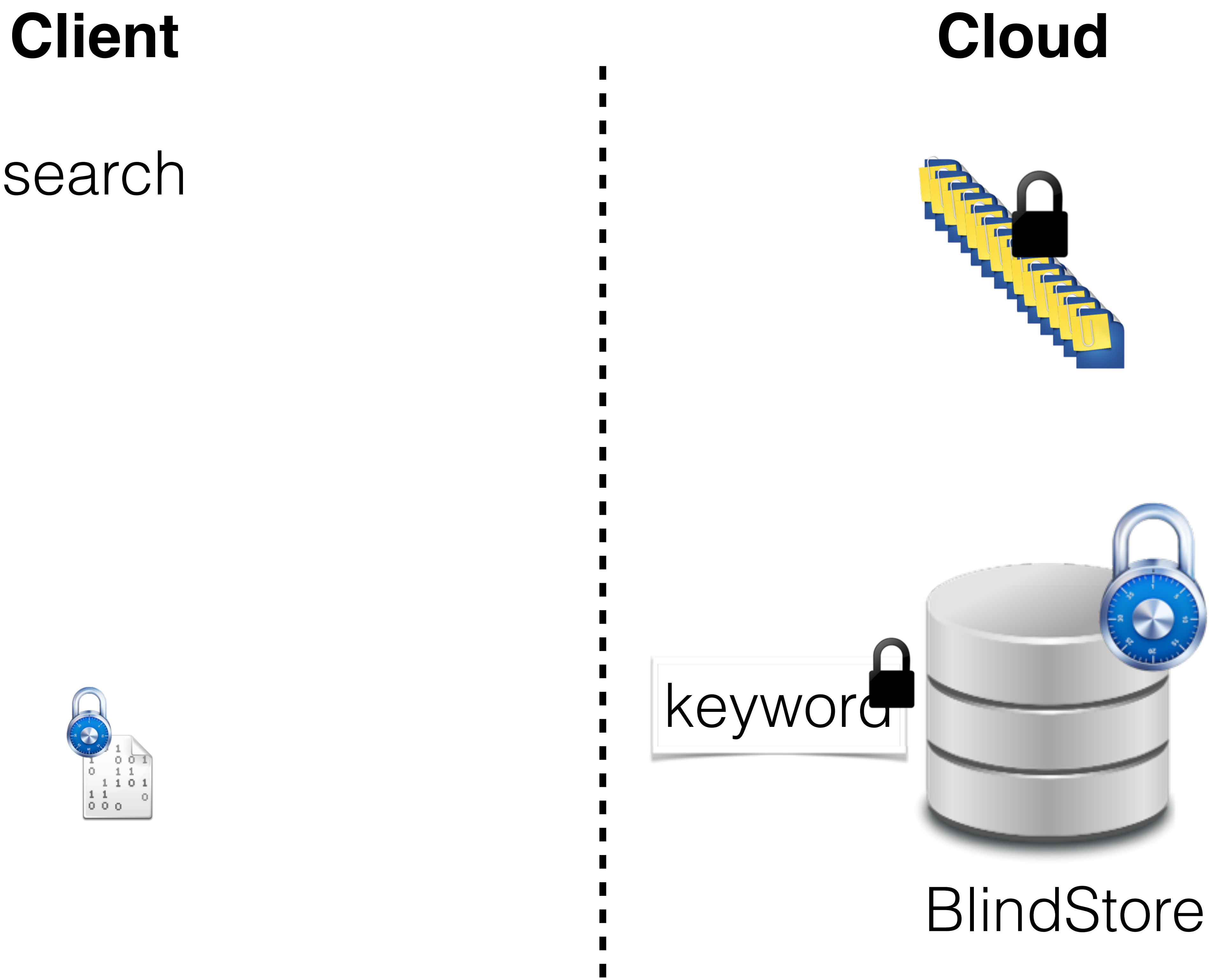
search



keyword

BlindStore

Lazy Delete Strategy



Client

Cloud

search

keyword

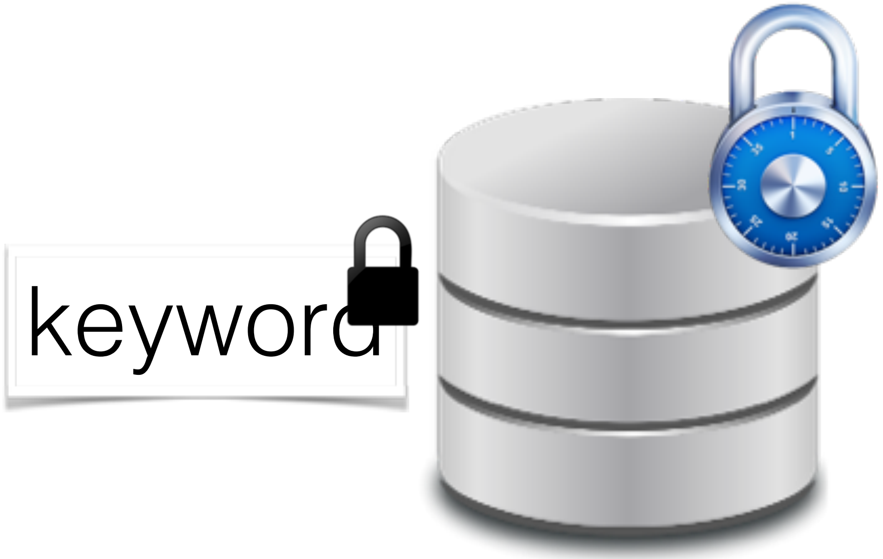
BlindStore

Lazy Delete Strategy

Client

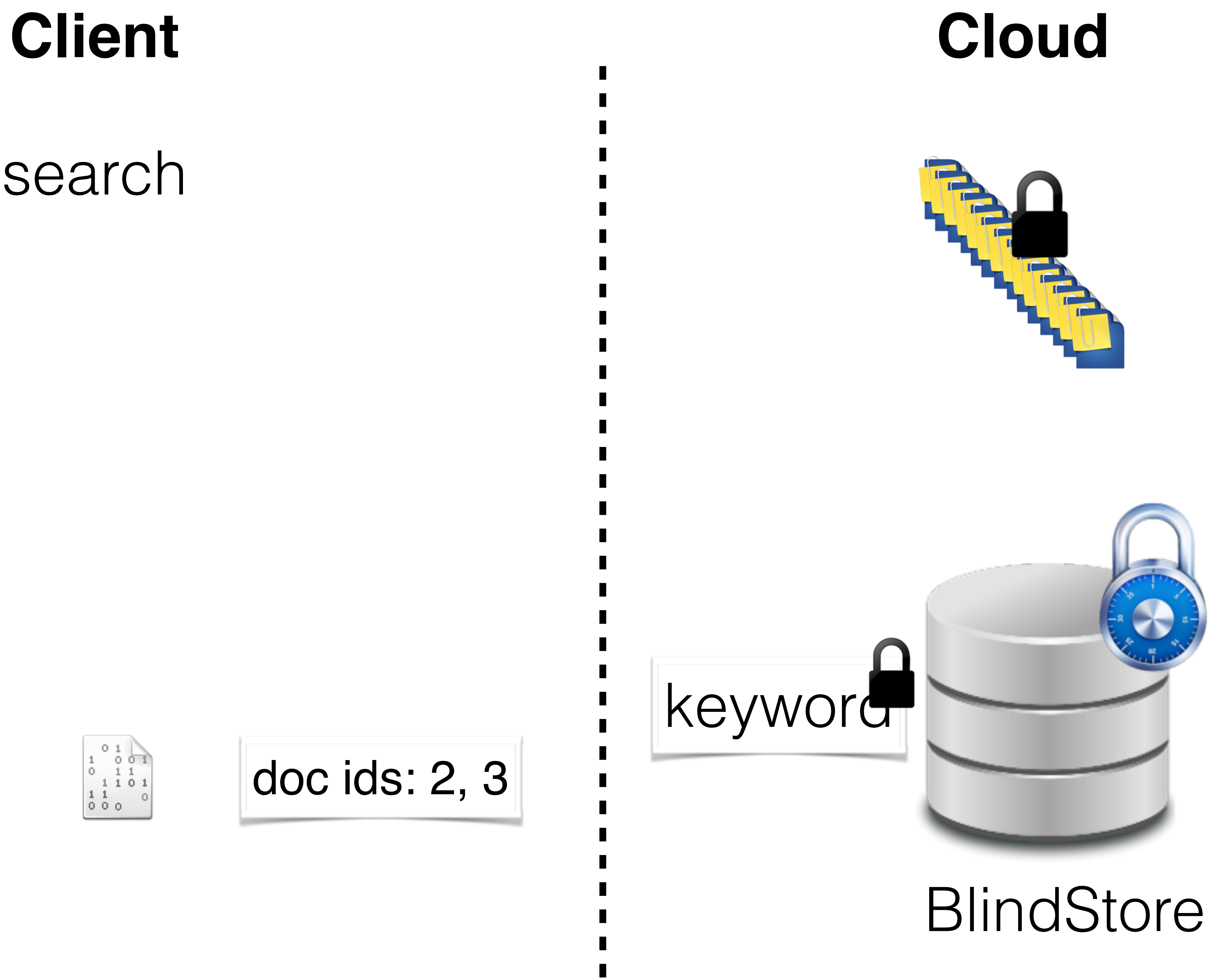
Cloud

search



BlindStore

Lazy Delete Strategy



Client

Cloud

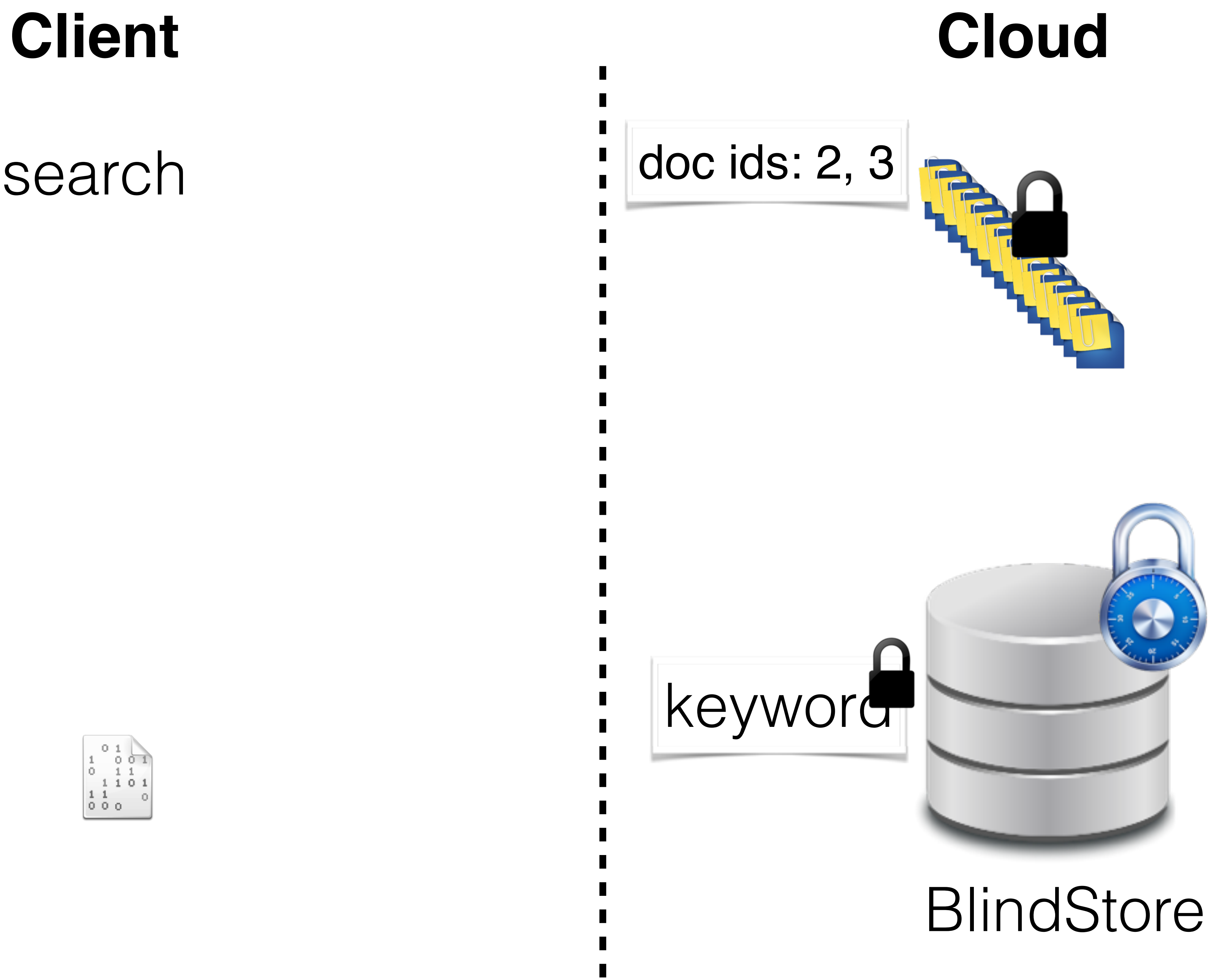
search

doc ids: 2, 3

keyword

BlindStore

Lazy Delete Strategy



Client

Cloud

search

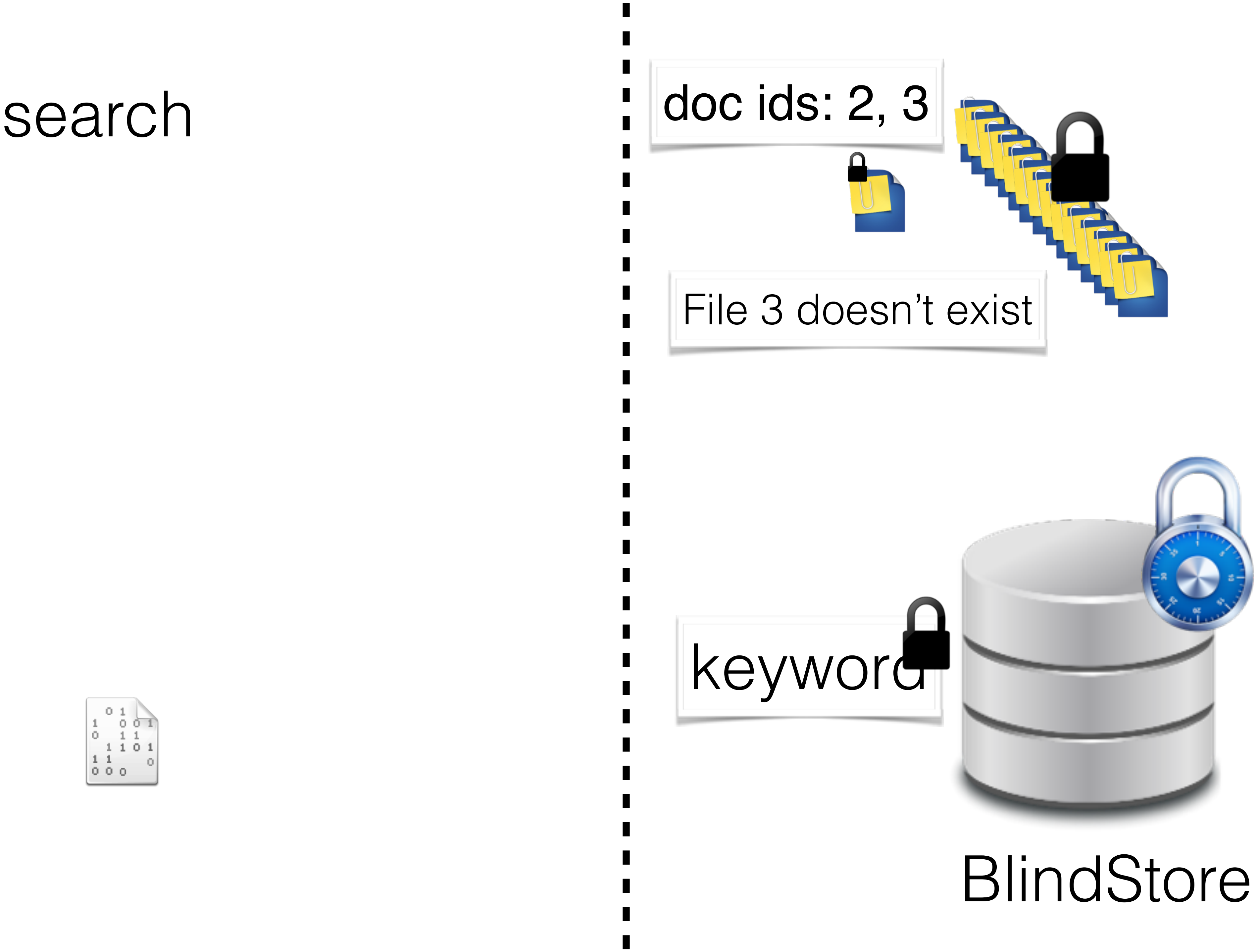
doc ids: 2, 3

keyword

BlindStore

Lazy Delete Strategy

Client **Cloud**



search

doc ids: 2, 3

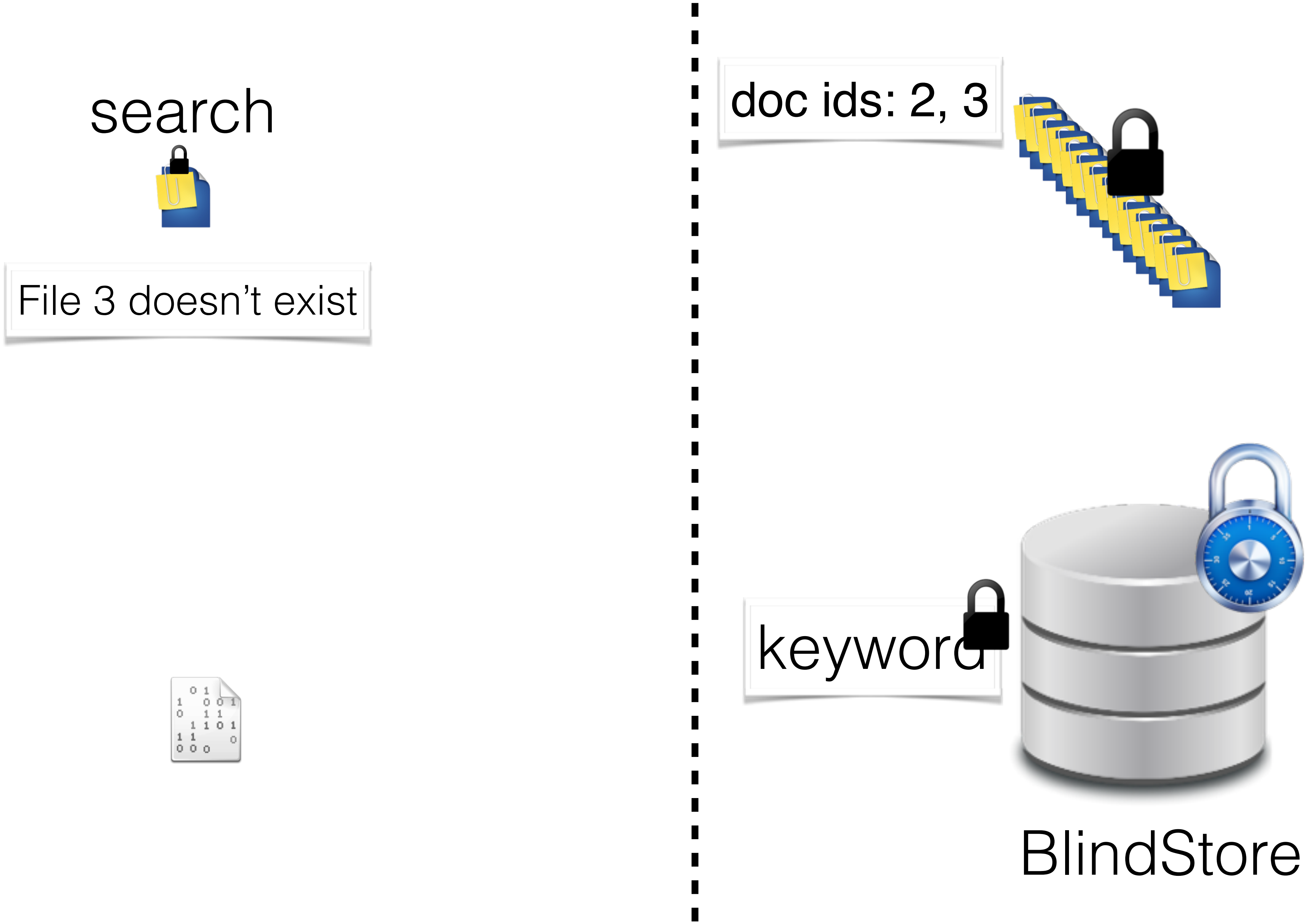
File 3 doesn’t exist

keyword

BlindStore

Lazy Delete Strategy

Client **Cloud**



search

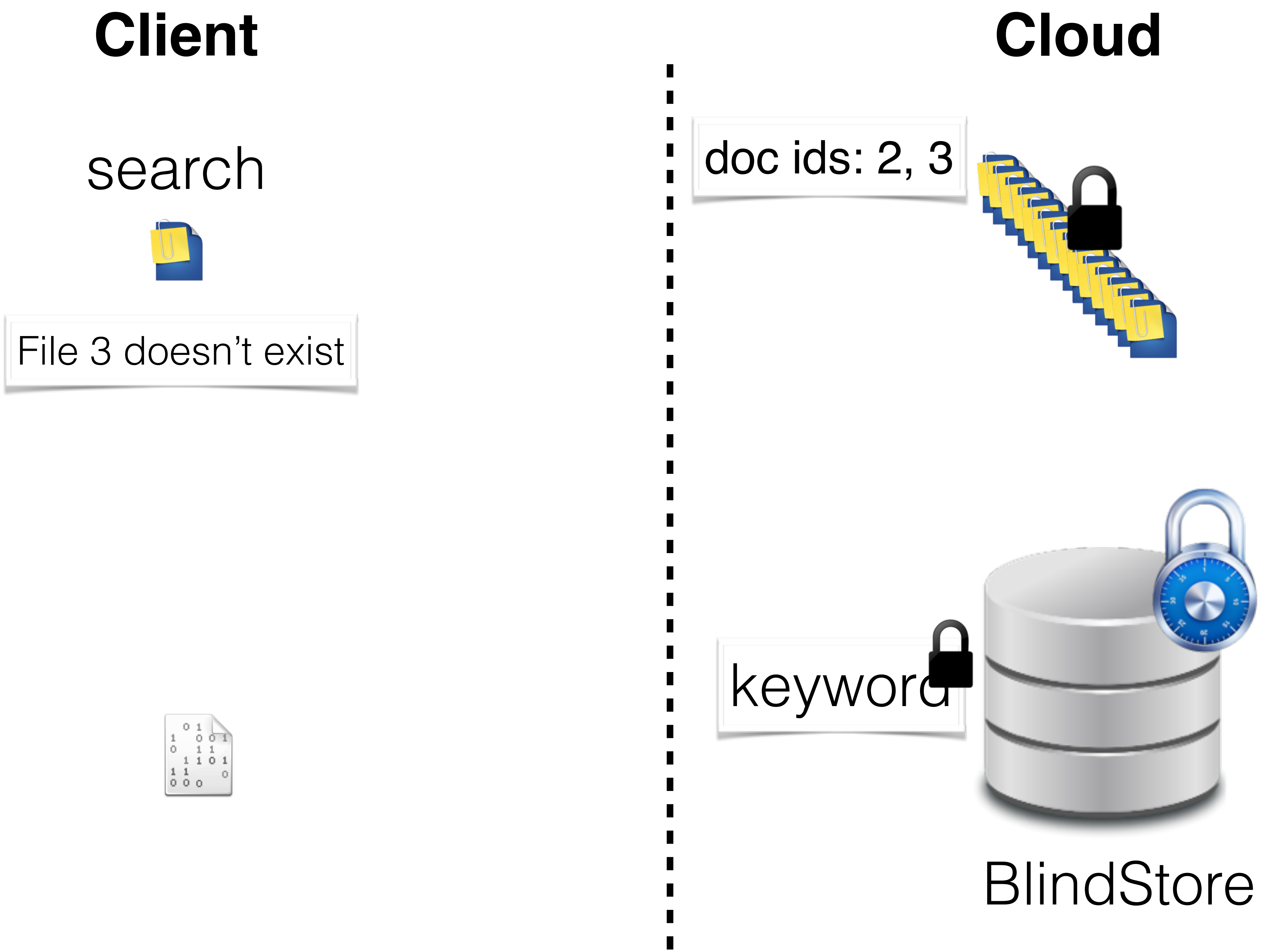
File 3 doesn’t exist

doc ids: 2, 3

keyword

BlindStore

Lazy Delete Strategy



Client

Cloud

search

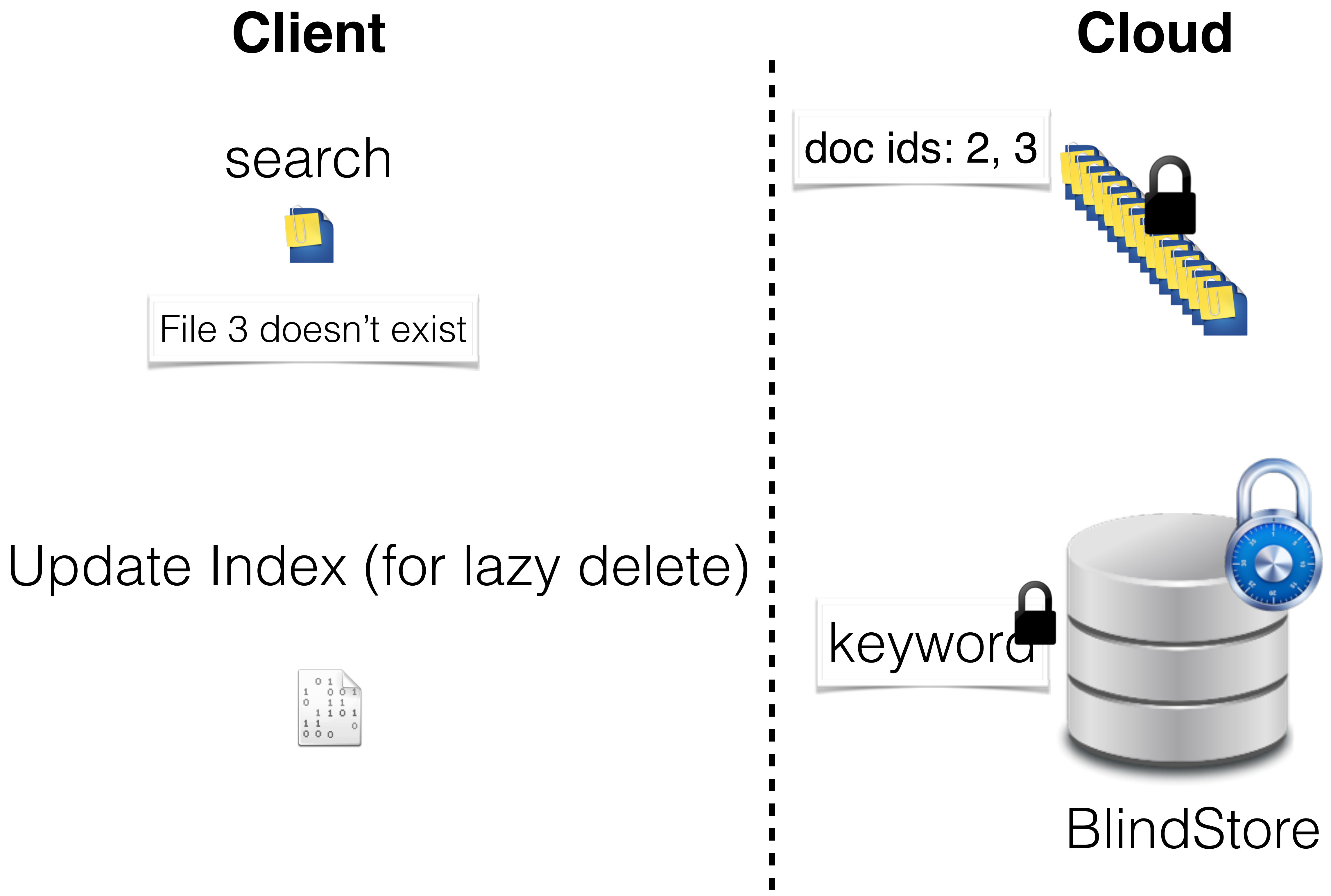
doc ids: 2, 3

File 3 doesn't exist

keyword

BlindStore

Lazy Delete Strategy



Client

Cloud

search

doc ids: 2, 3

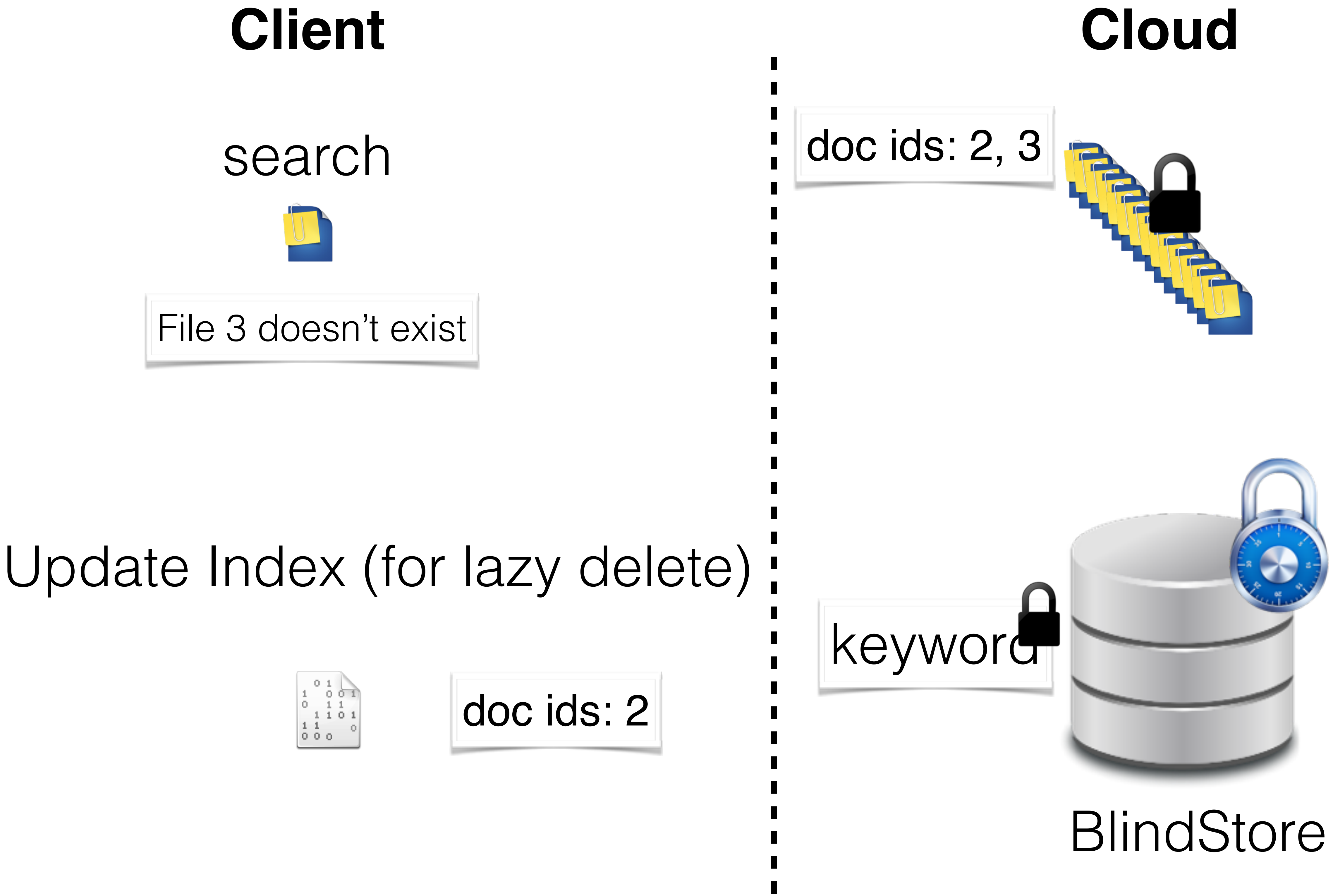
File 3 doesn't exist

Update Index (for lazy delete)

keyword

BlindStore

Lazy Delete Strategy



Client

Cloud

search

File 3 doesn't exist

Update Index (for lazy delete)

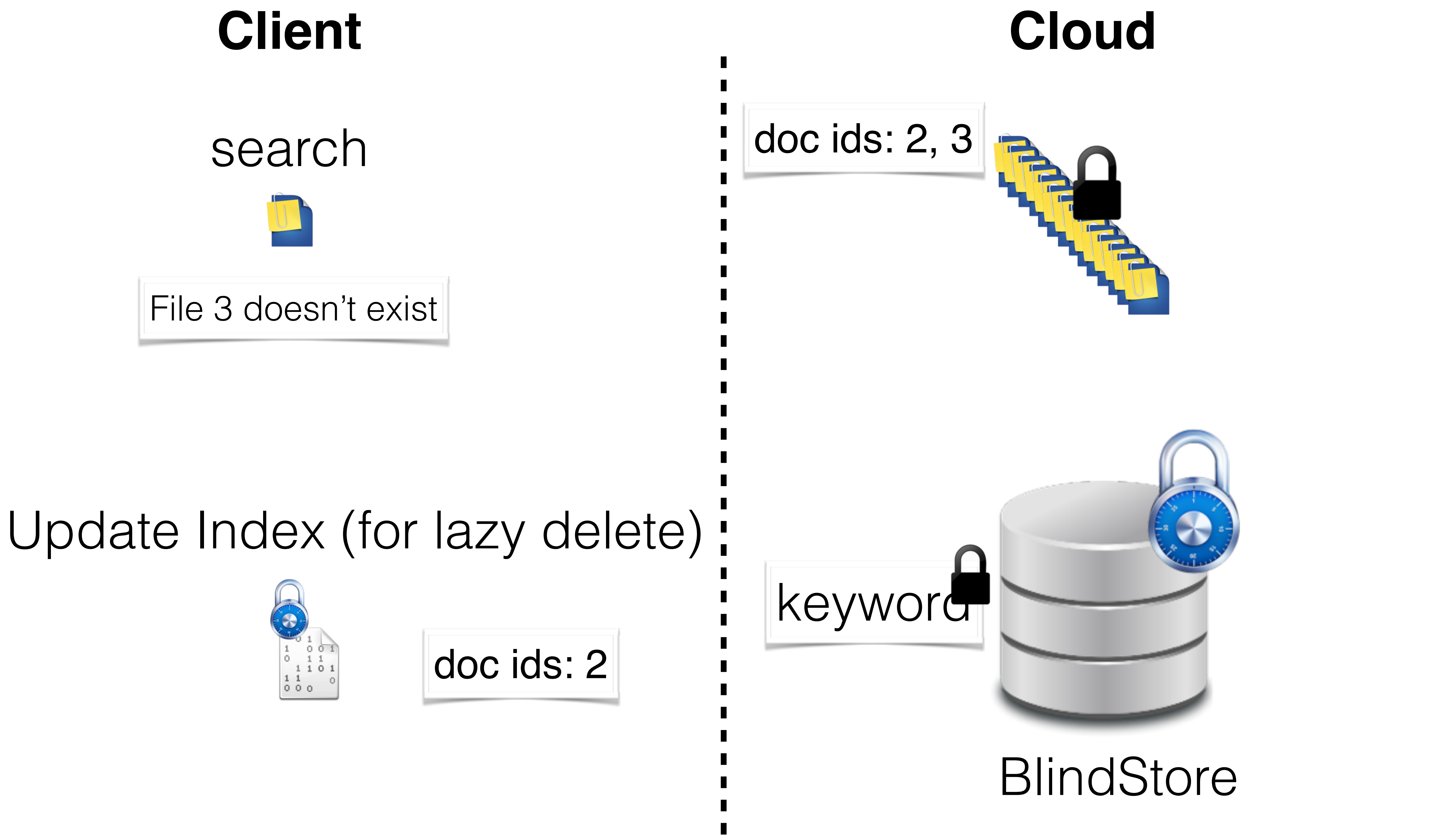
doc ids: 2

doc ids: 2, 3

keyword

BlindStore

Lazy Delete Strategy



Client

Cloud

search

File 3 doesn't exist

Update Index (for lazy delete)

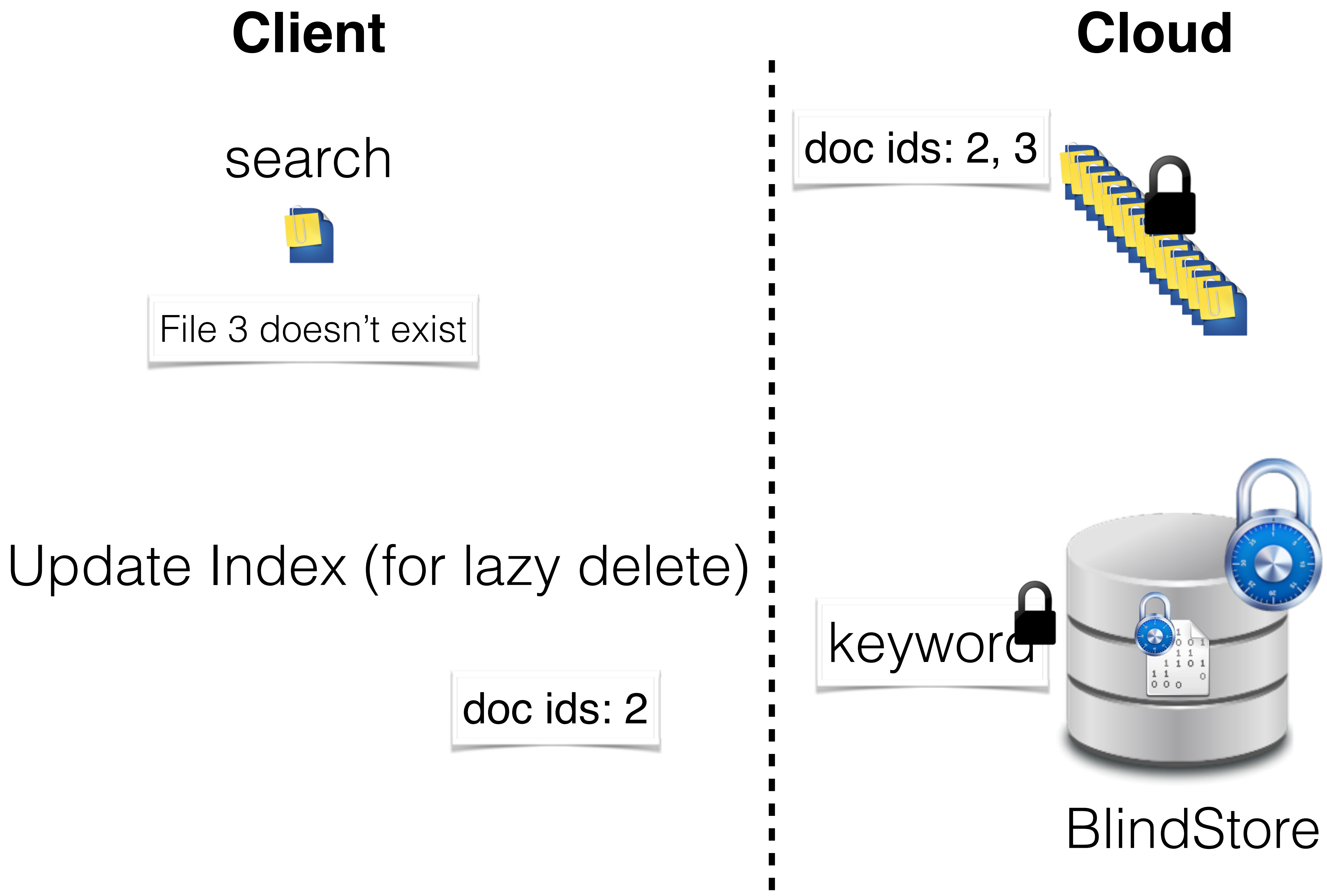
doc ids: 2

doc ids: 2, 3

keyword

BlindStore

Lazy Delete Strategy



Client

Cloud

search

File 3 doesn’t exist

Update Index (for lazy delete)

doc ids: 2

doc ids: 2, 3

keyword

BlindStore

Leakage

- Leaks Access and Search Pattern
- Leak nothing when file is deleted, slowly reveal keywords contained in deleted files
- Updates: Leaks strictly less than prior schemes except Stefanov et. al. NDSS 2014 scheme
  - They have polylograithmic overhead on top of other schemes (including ours)

We achieve adaptive security through **one extra round of interaction**.

Performance

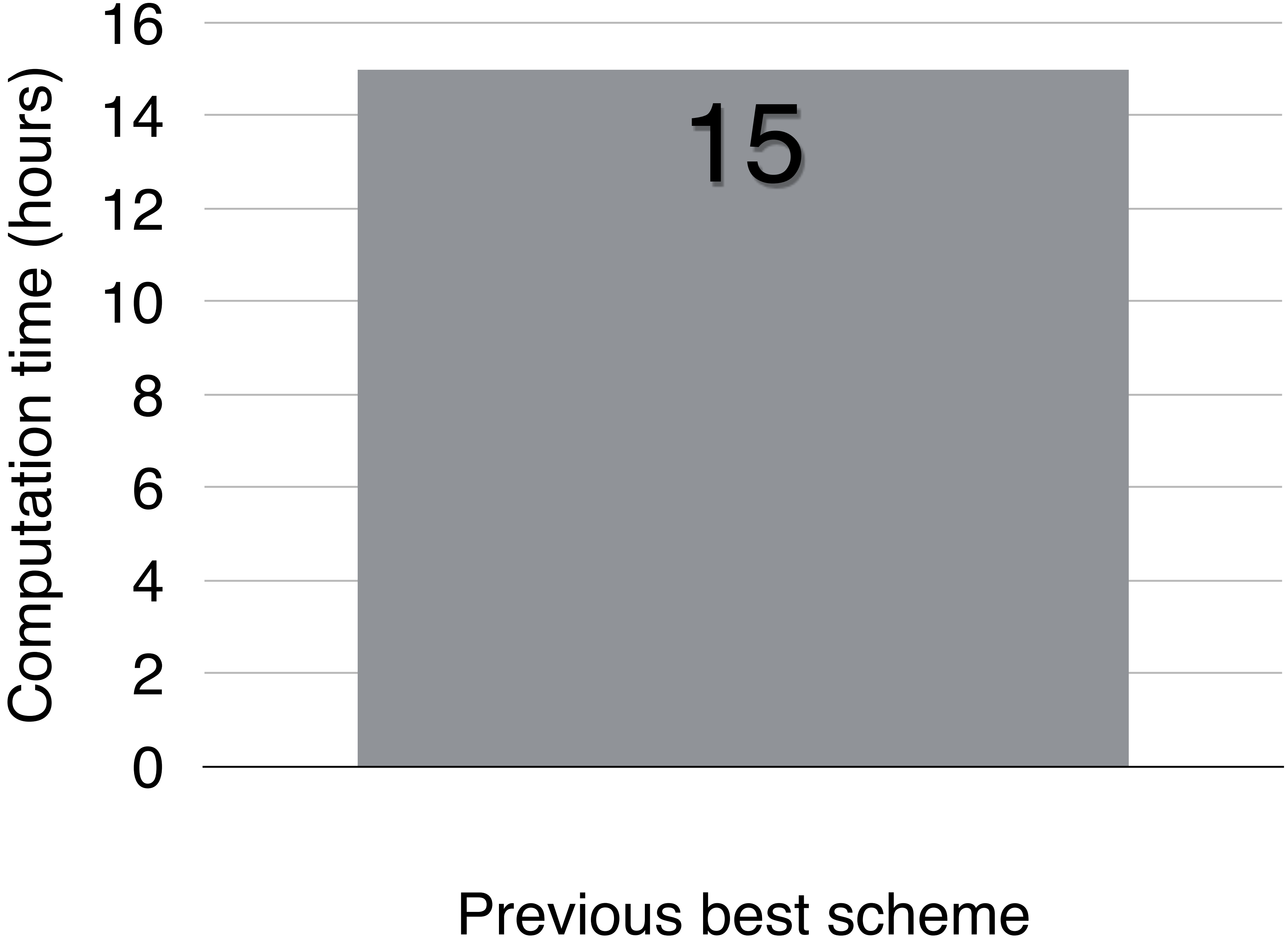
4X AES cost to encrypt the index

Evaluation

- Datasets
  - Emails: Subset of Enron email dataset
  - Documents: We collected 1GB doc, ppt, xls and pdf document using Google
- Operations
  - Setup (Preprocessing)
  - Search (for the most frequent word “the”)
  - Add
  - Delete
- Laptop machine was used for experiments

Setup cost

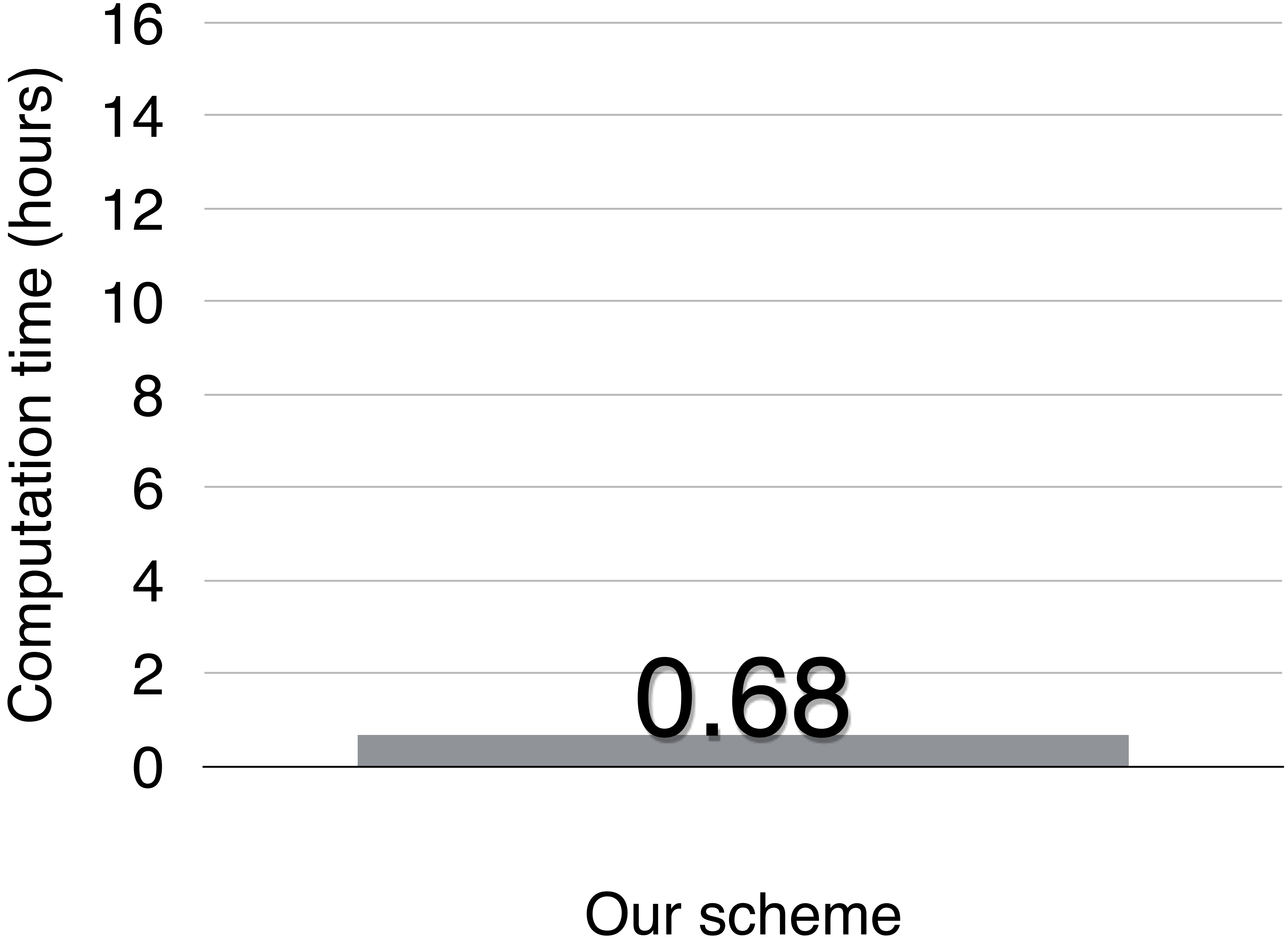
for 16GB Enron Emails (Extrapolated)



Prior work used Xeon server while we used a laptop

Setup cost

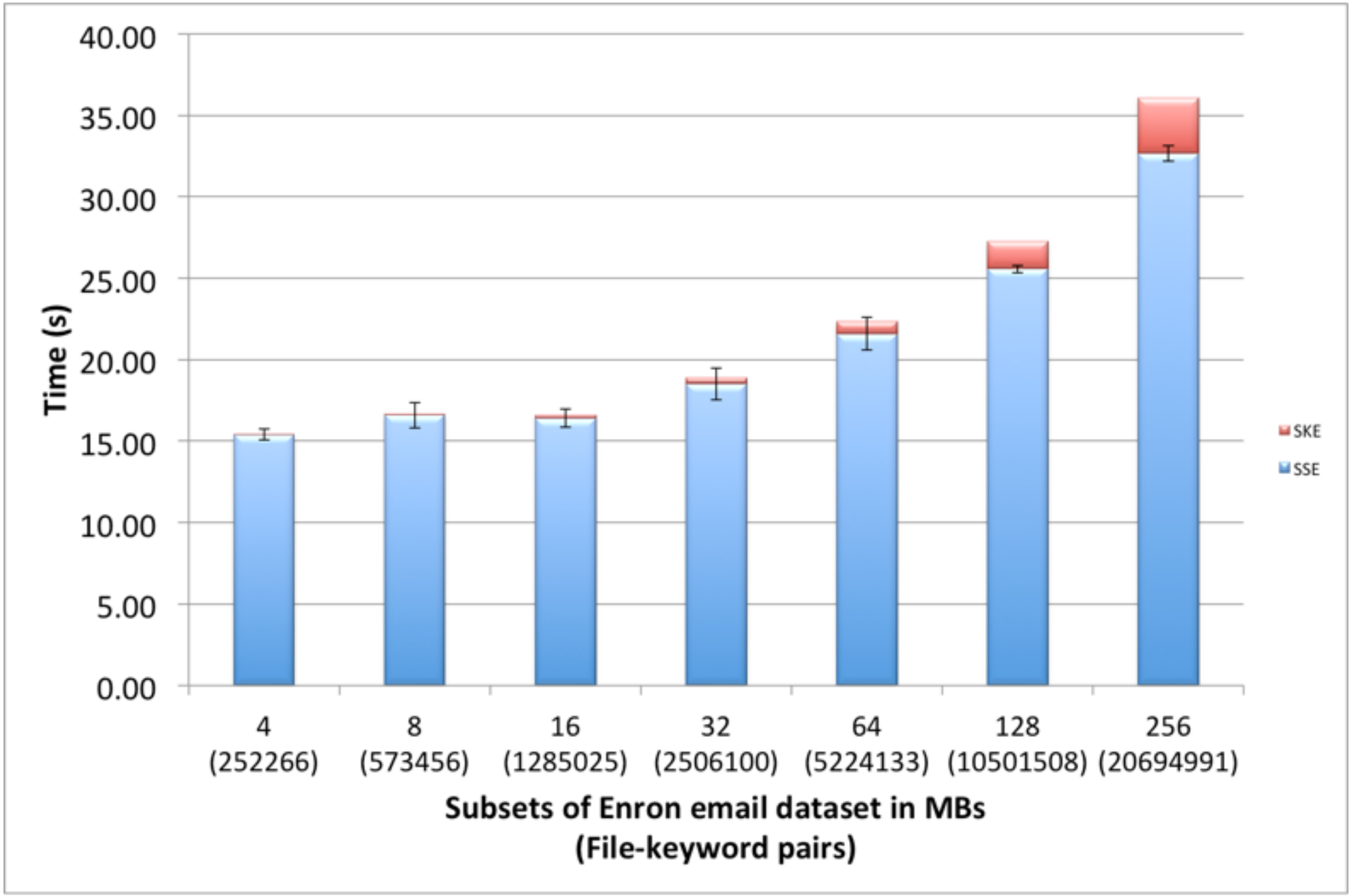
for 16GB Enron Emails (Extrapolated)



Prior work used Xeon server while we used a laptop

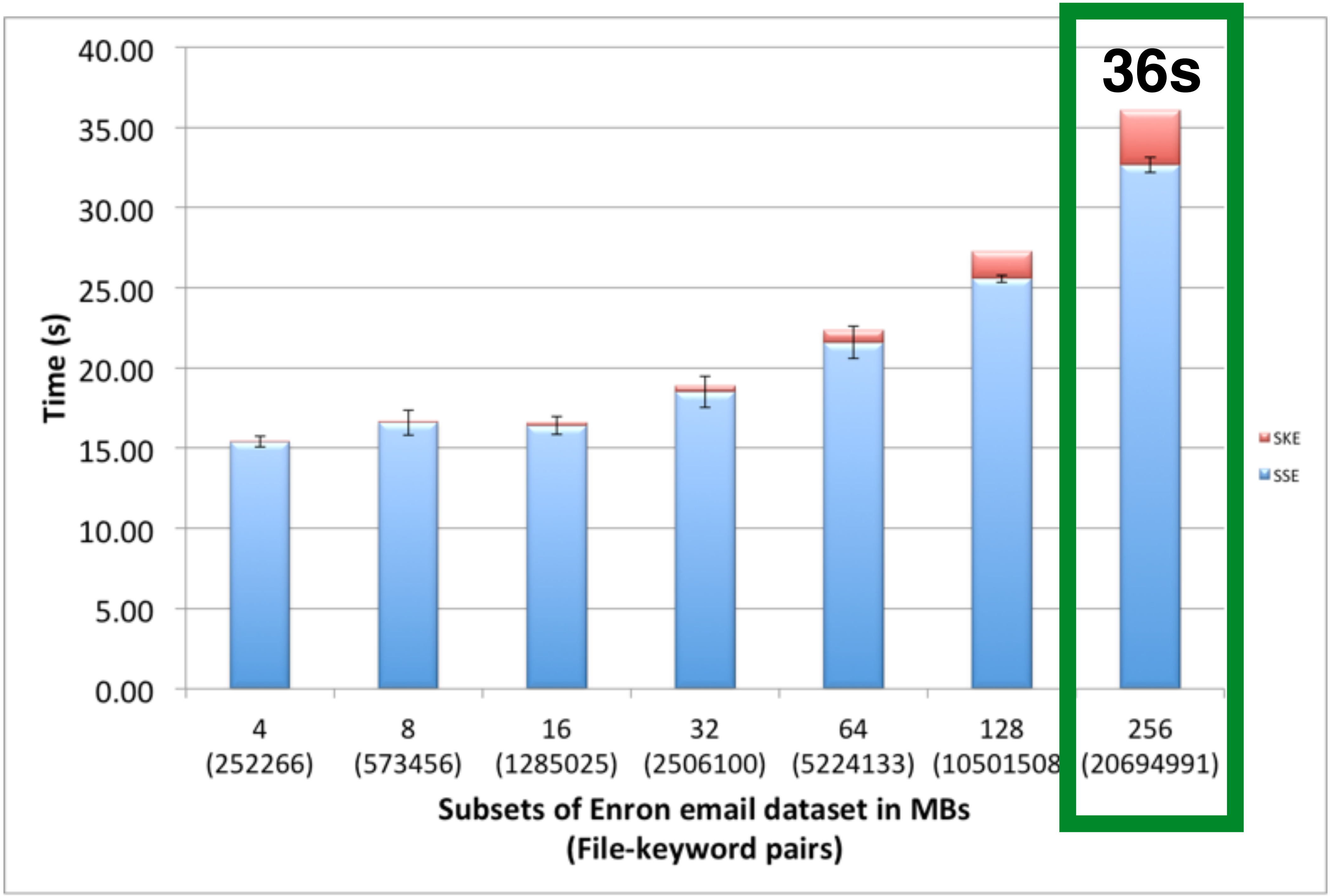
Evaluation on
Enron Email dataset

Setup

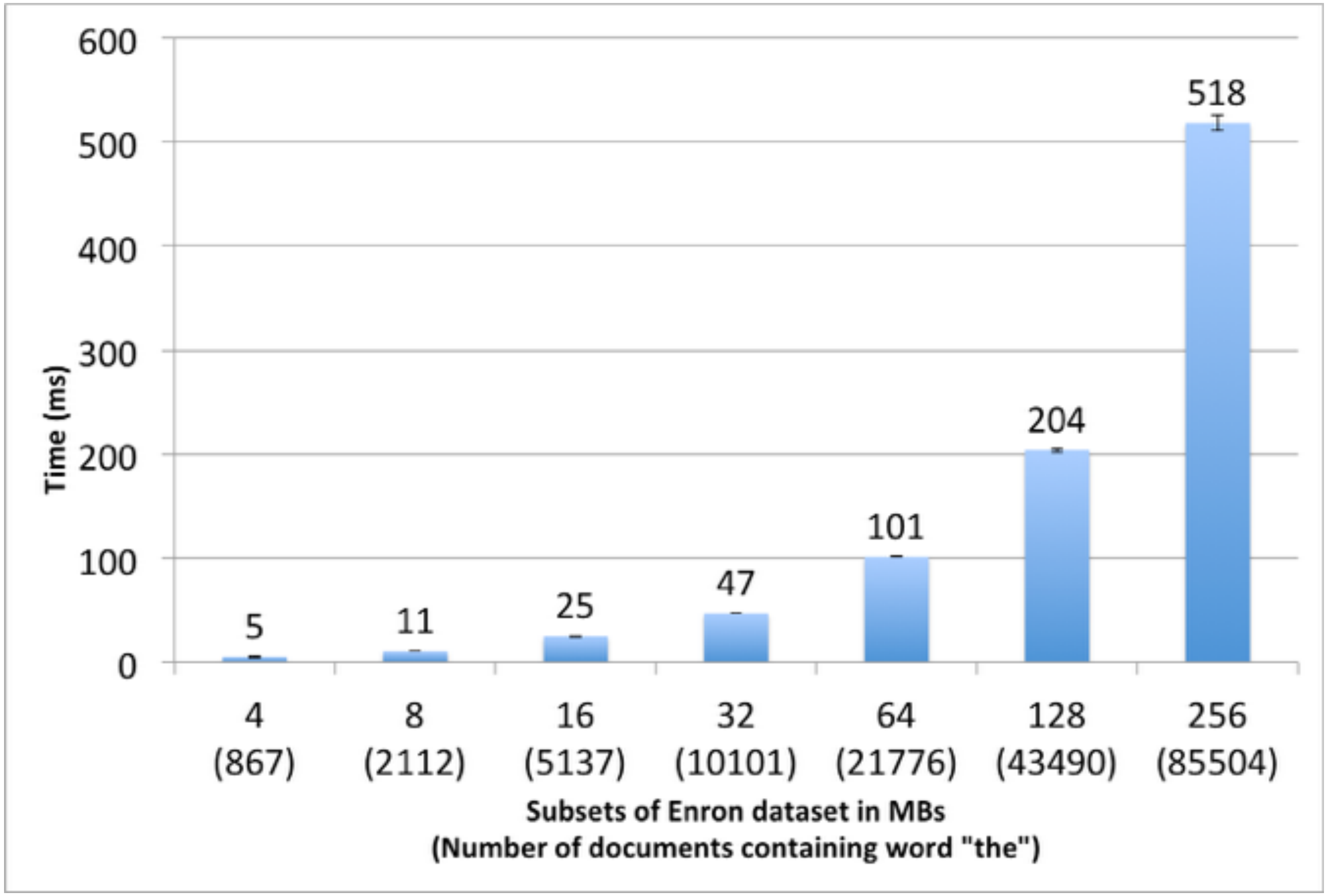


40.00
35.00
30.00
25.00
20.00
15.00
10.00
5.00
0.00
Time (s)
4
(252266)
8
(573456)
16
(1285025)
32
(2506100)
64
(5224133)
128
(10501508)
256
(20694991)
Subsets of Enron email dataset in MBs
(File-keyword pairs)
SKE
SSE

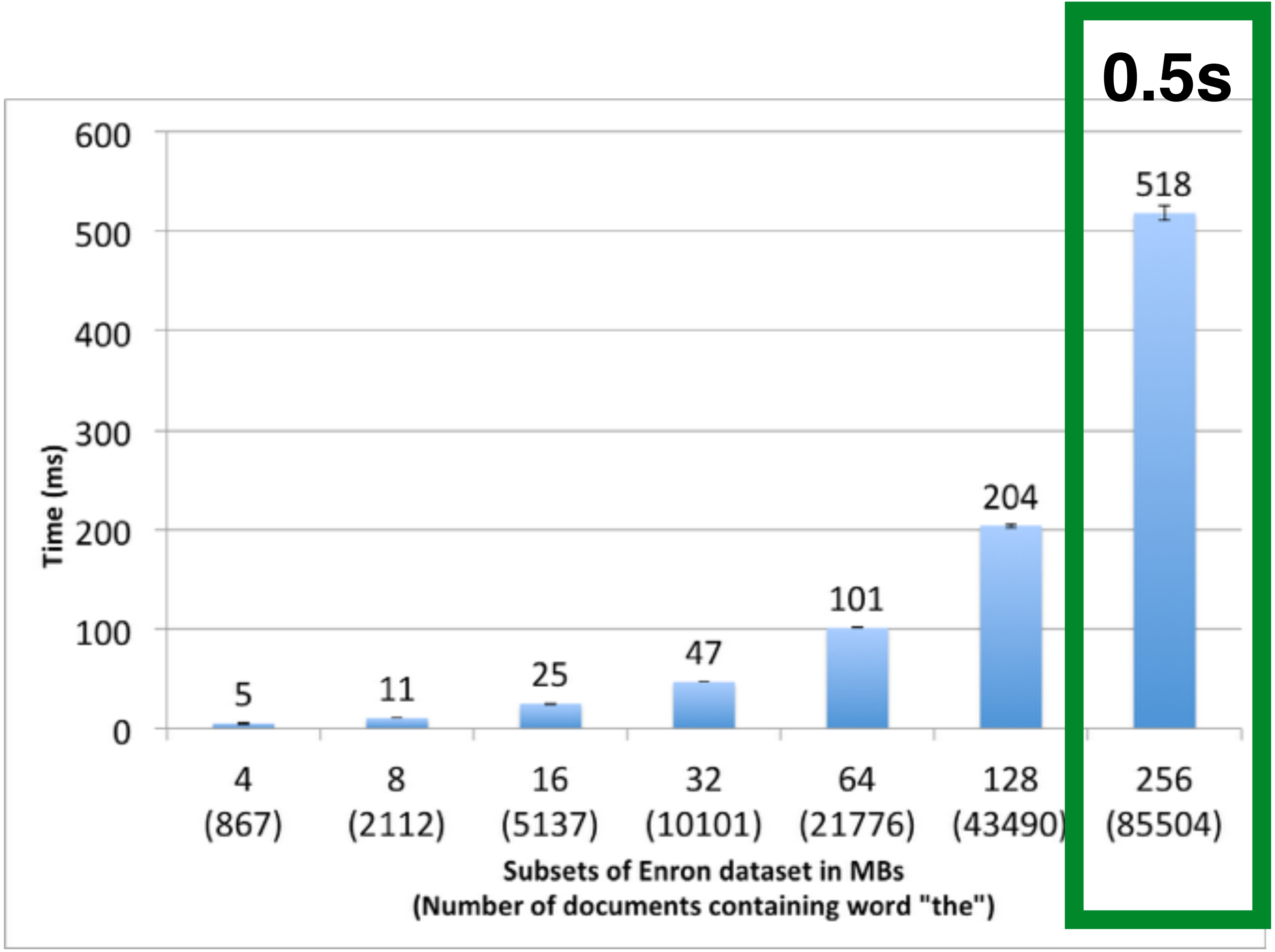
Setup


36s
Time (s)
40.00
35.00
30.00
25.00
20.00
15.00
10.00
5.00
0.00
4
(252266)
8
(573456)
16
(1285025)
32
(2506100)
64
(5224133)
128
(10501508
256
(20694991)
Subsets of Enron email dataset in MBs
(File-keyword pairs)
SKE
SSE

Search

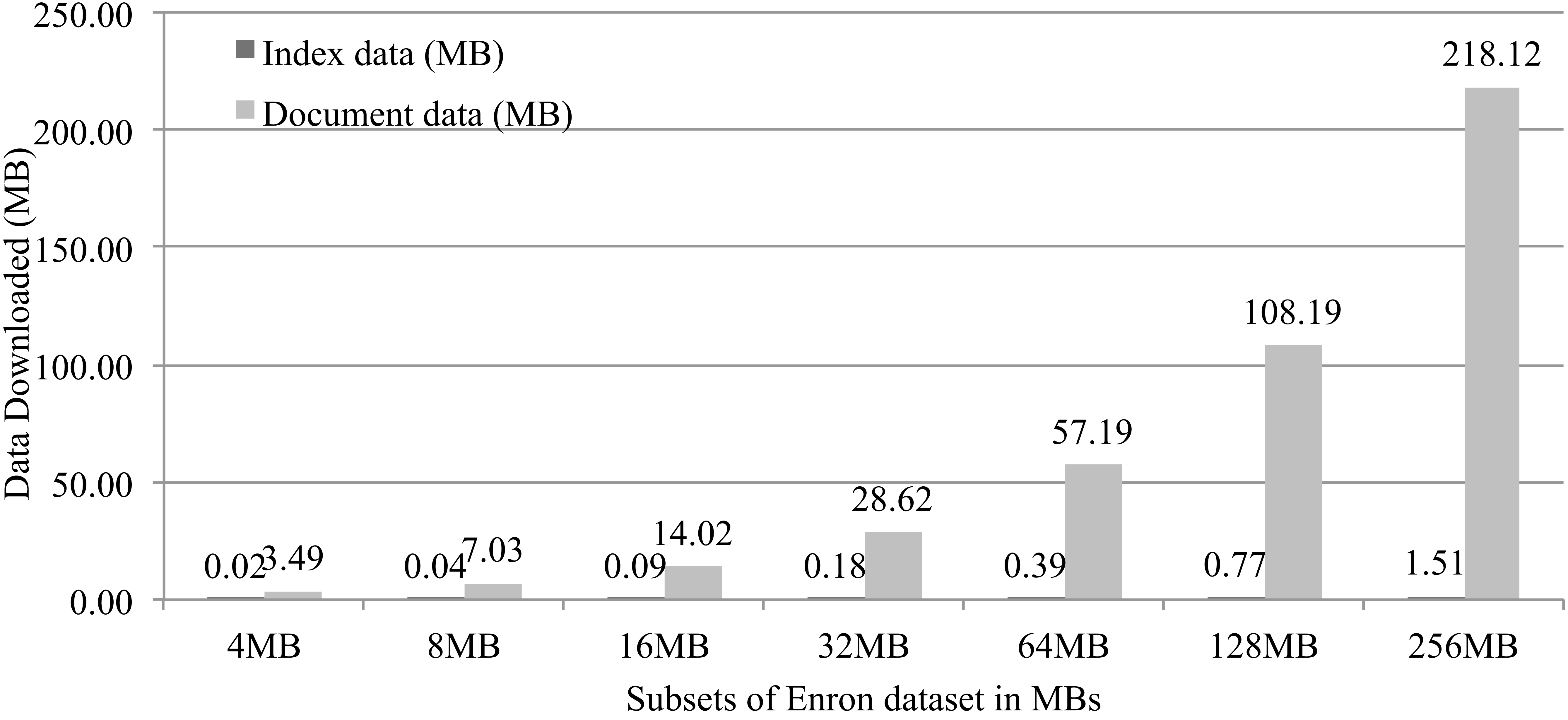

600
500
400
300
200
100
0
Time (ms)
5
11
25
47
101
204
518
4 (867)
8 (2112)
16 (5137)
32 (10101)
64 (21776)
128 (43490)
256 (85504)
Subsets of Enron dataset in MBs
(Number of documents containing word "the")

Search

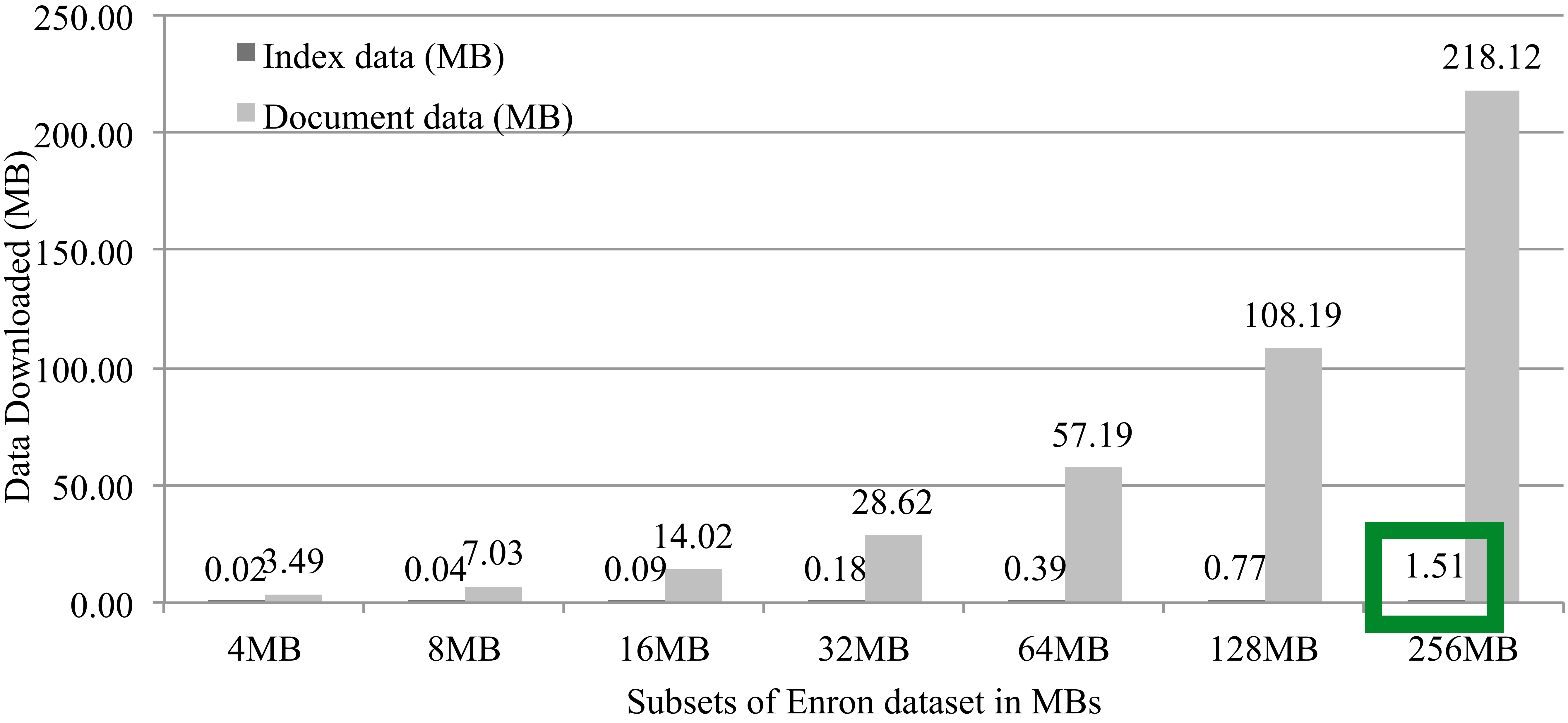

600
500
400
300
200
100
0
Time (ms)
5
11
25
47
101
204
518
4
(867)
8
(2112)
16
(5137)
32
(10101)
64
(21776)
128
(43490)
256
(85504)
Subsets of Enron dataset in MBs
(Number of documents containing word "the")

0.5s

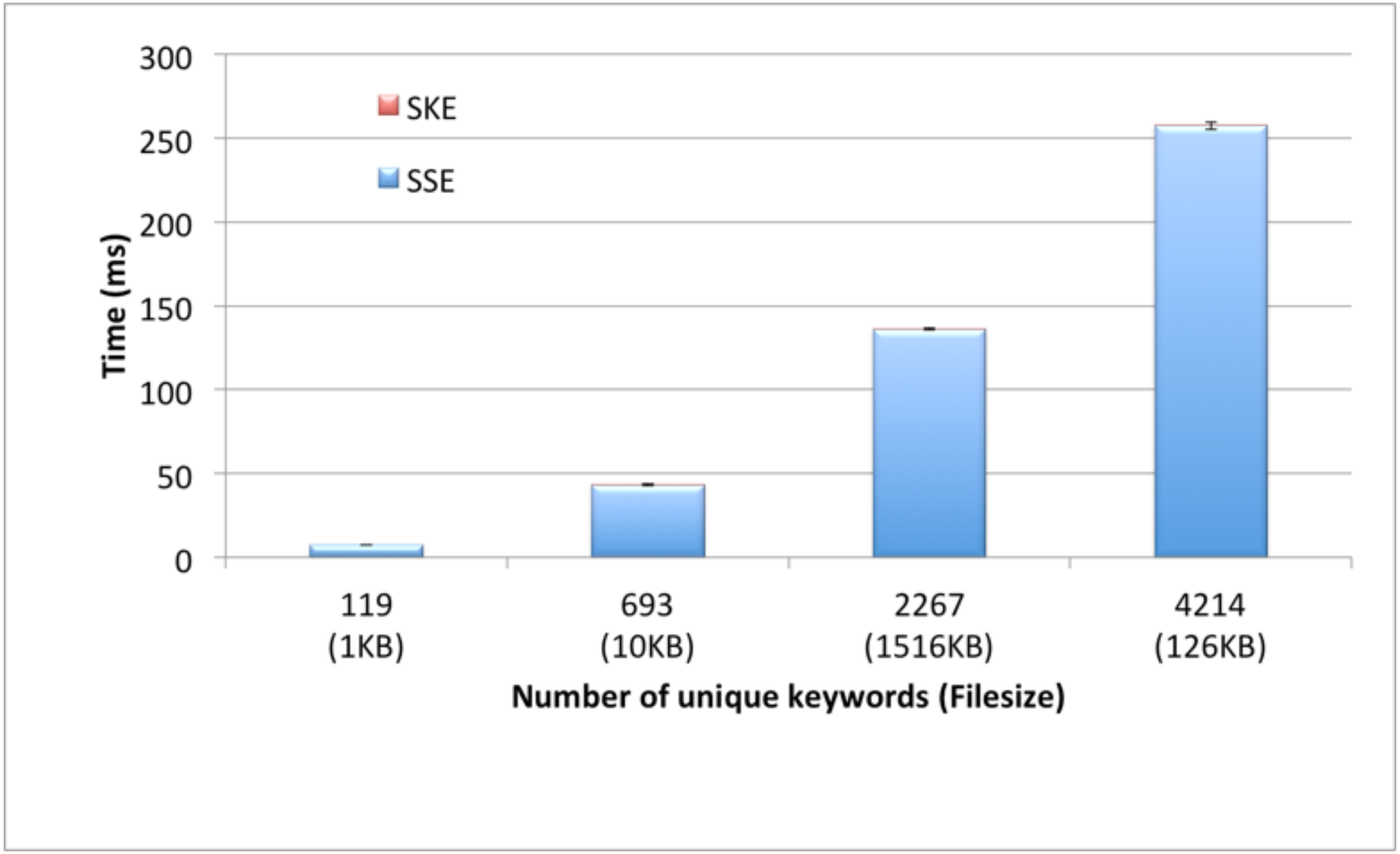
Communication Overhead



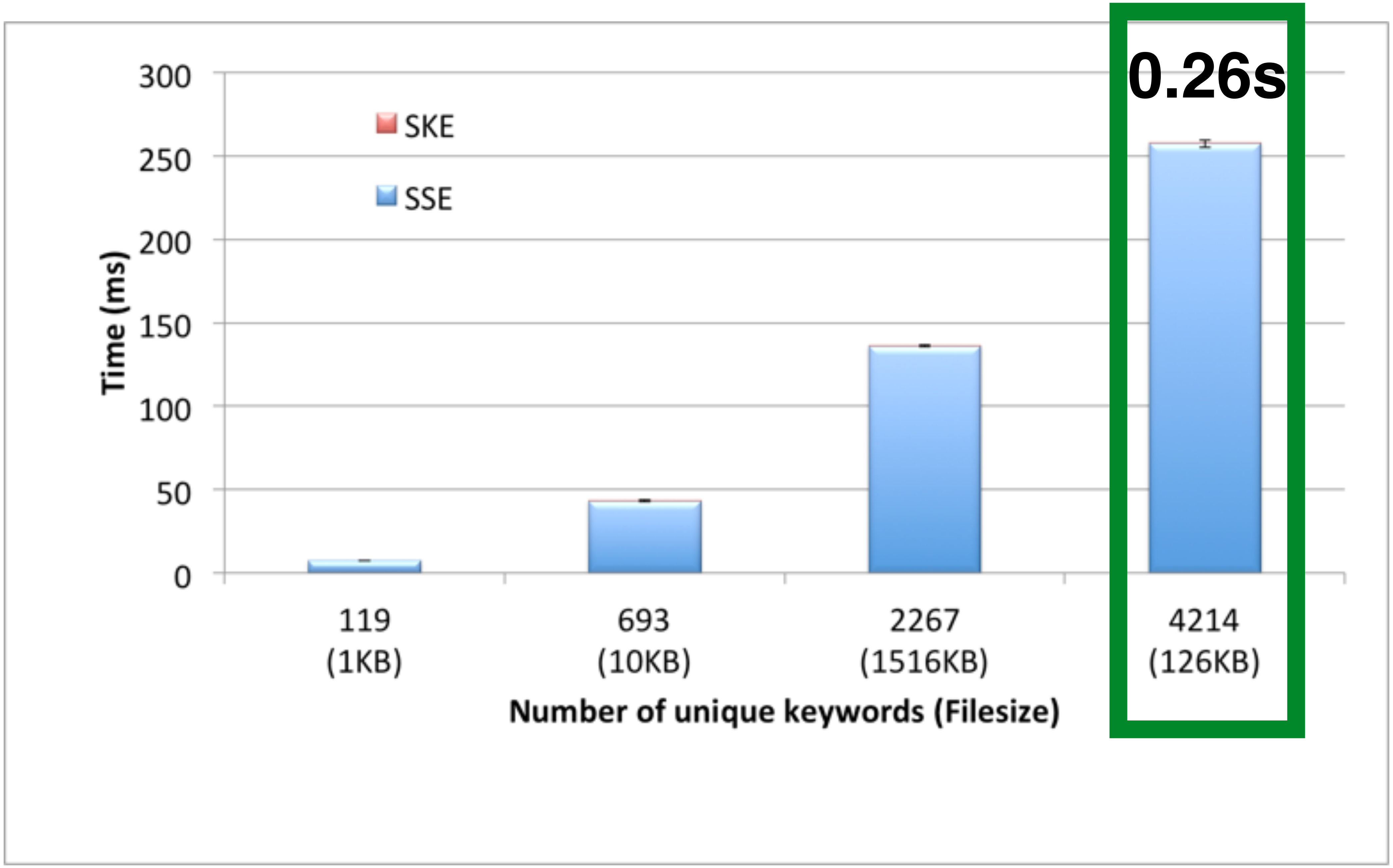
Communication Overhead



Add


300
250
200
150
100
50
0
Time (ms)
SKE
SSE
119
(1KB)
693
(10KB)
2267
(1516KB)
4214
(126KB)
Number of unique keywords (Filesize)

Add


300
250
200
150
100
50
0
Time (ms)
SKE
SSE
119
(1KB)
693
(10KB)
2267
(1516KB)
4214
(126KB)
Number of unique keywords (Filesize)

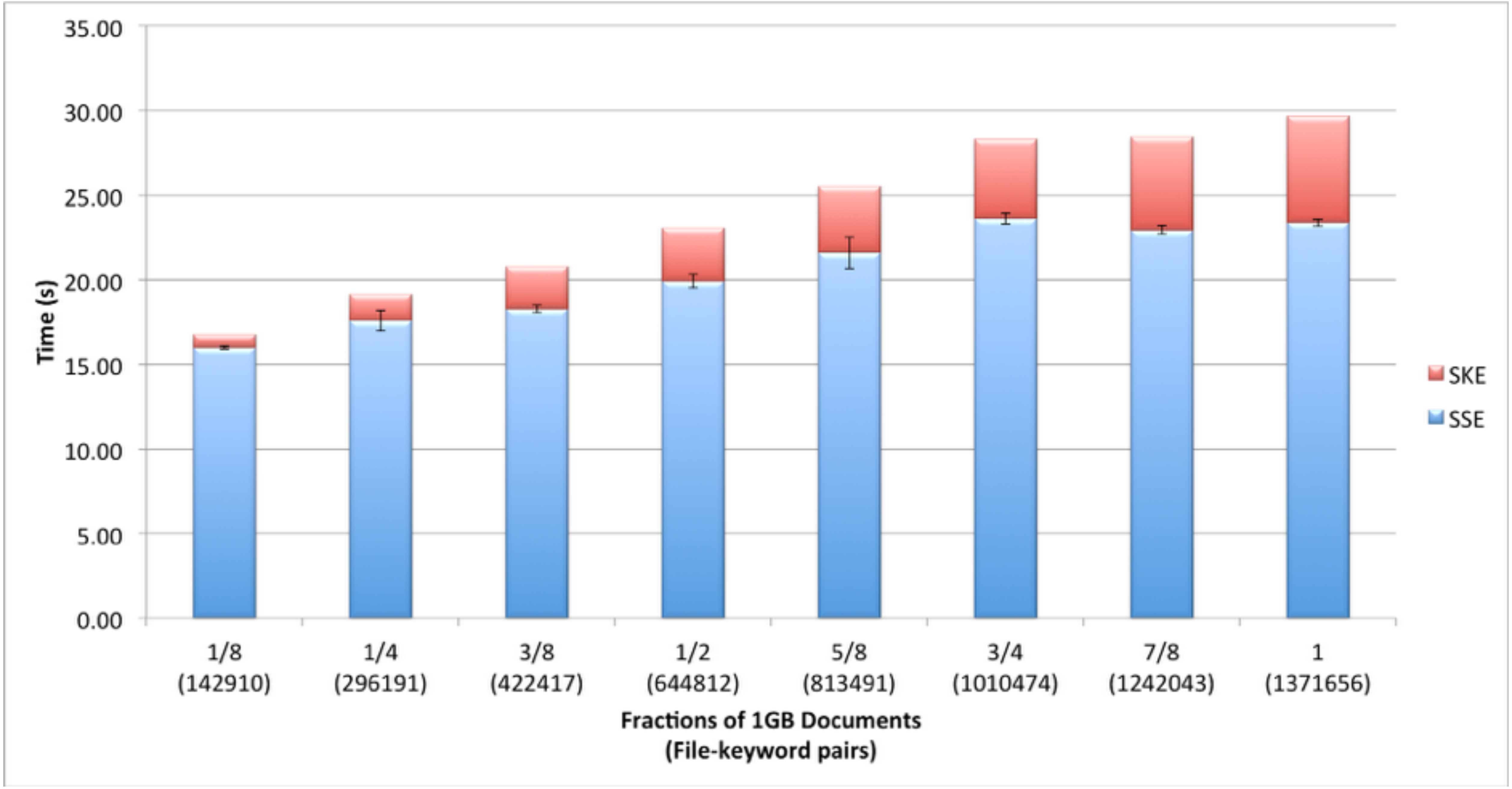
0.26s

Evaluation on Documents dataset

Data collection

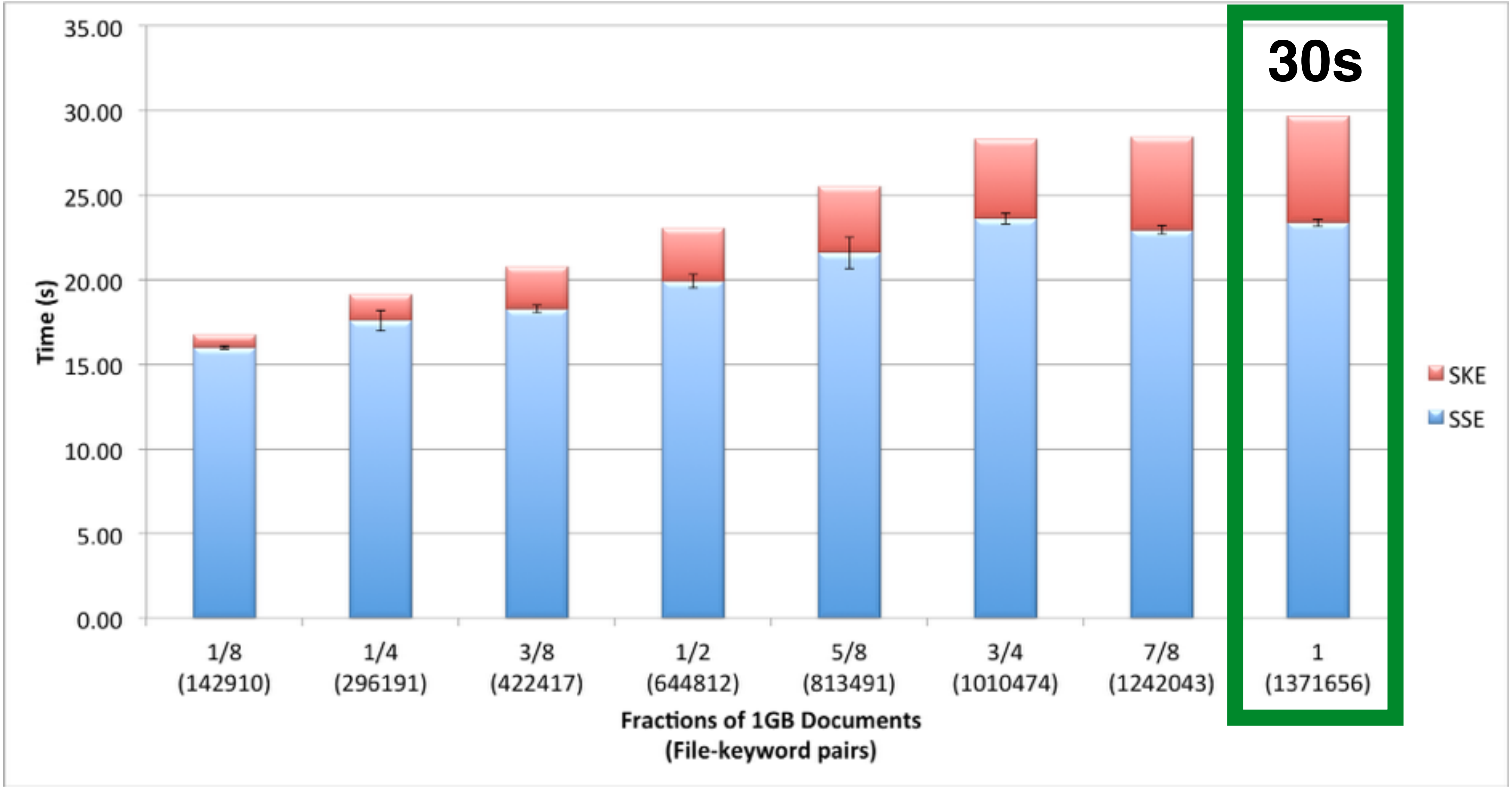
- We collected 1GB doc, ppt, xls and pdf document using Google
- All documents in the dataset are in English

Setup

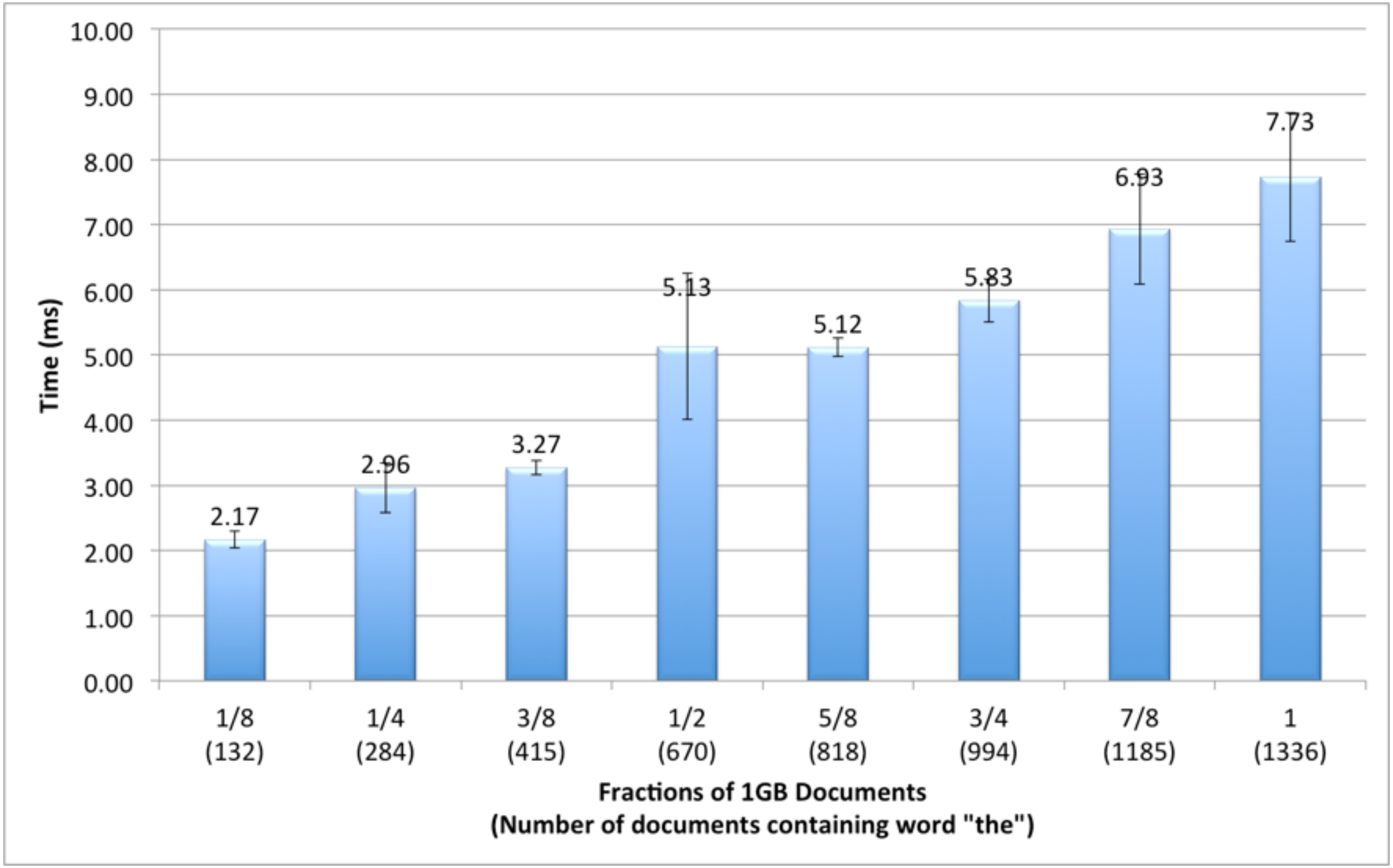


35.00
30.00
25.00
20.00
15.00
10.00
5.00
0.00
Time (s)
SKE
SSE
1/8 (142910)
1/4 (296191)
3/8 (422417)
1/2 (644812)
5/8 (813491)
3/4 (1010474)
7/8 (1242043)
1 (1371656)
Fractions of 1GB Documents (File-keyword pairs)

Setup

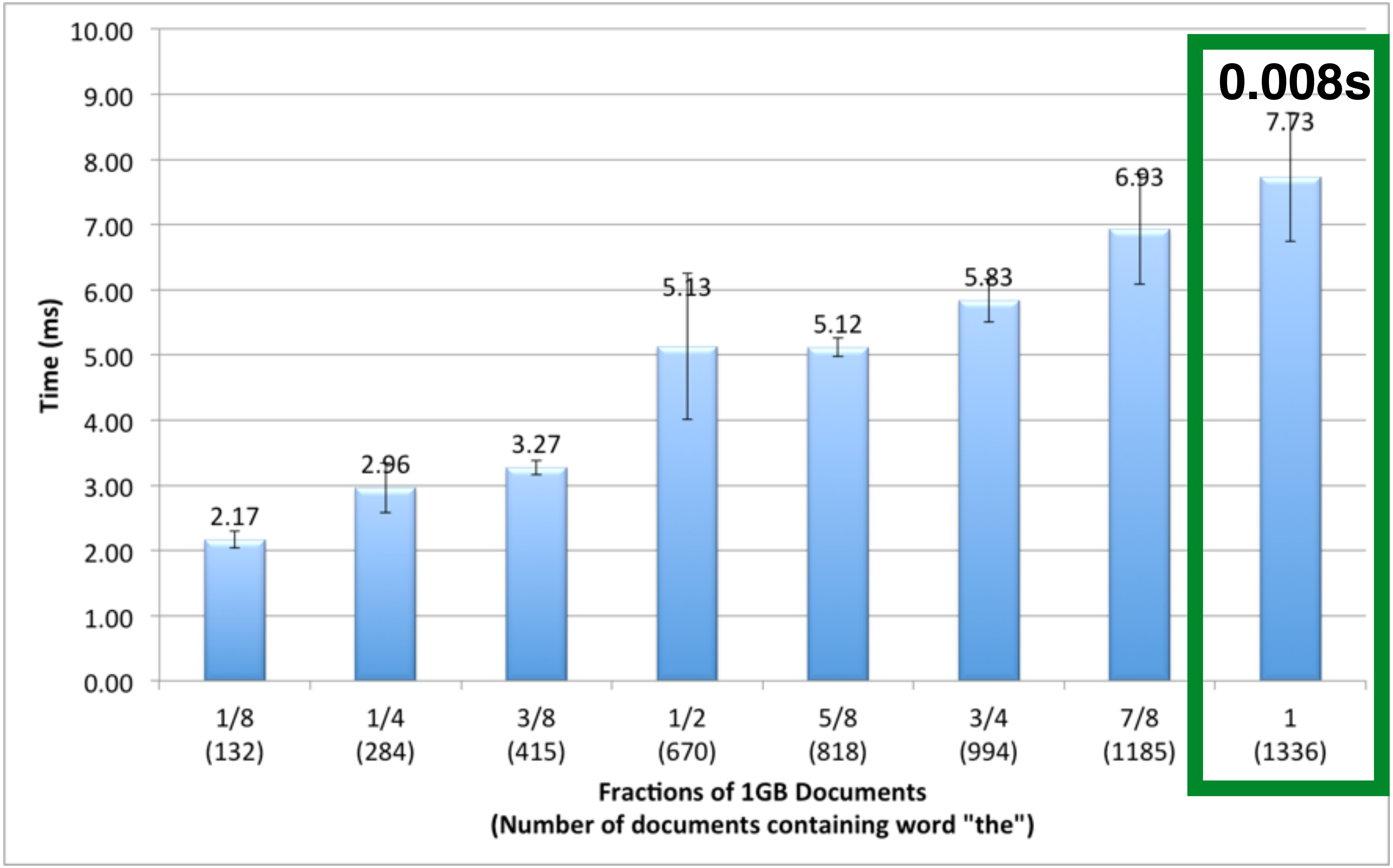

30s
Time (s)
35.00
30.00
25.00
20.00
15.00
10.00
5.00
0.00
1/8 (142910)
1/4 (296191)
3/8 (422417)
1/2 (644812)
5/8 (813491)
3/4 (1010474)
7/8 (1242043)
1 (1371656)
Fractions of 1GB Documents (File-keyword pairs)
SKE
SSE

Search

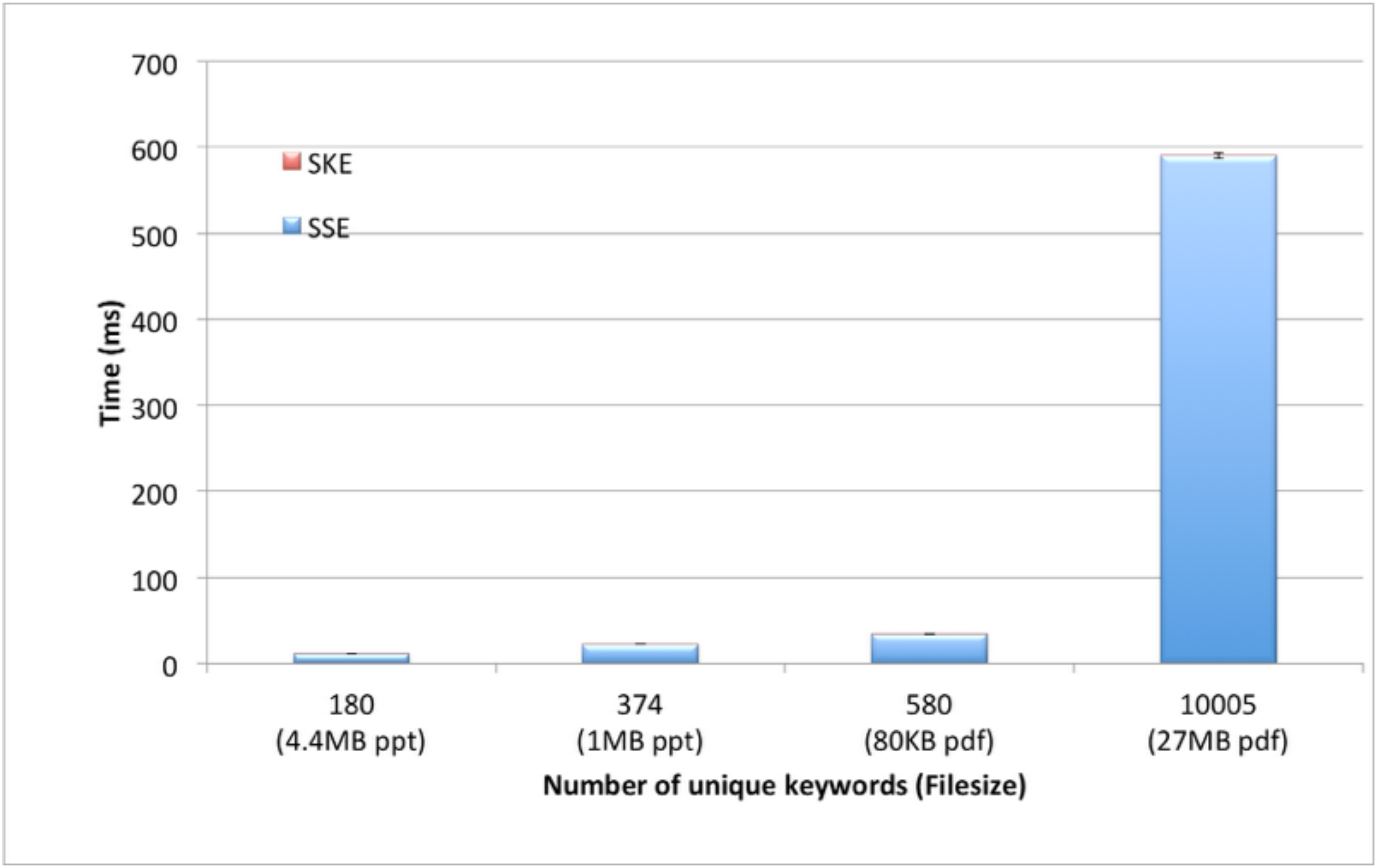


10.00
9.00
8.00
7.00
6.00
5.00
4.00
3.00
2.00
1.00
0.00
Time (ms)
2.17
2.96
3.27
5.13
5.12
5.83
6.93
7.73
1/8 (132)
1/4 (284)
3/8 (415)
1/2 (670)
5/8 (818)
3/4 (994)
7/8 (1185)
1 (1336)
Fractions of 1GB Documents
(Number of documents containing word "the")

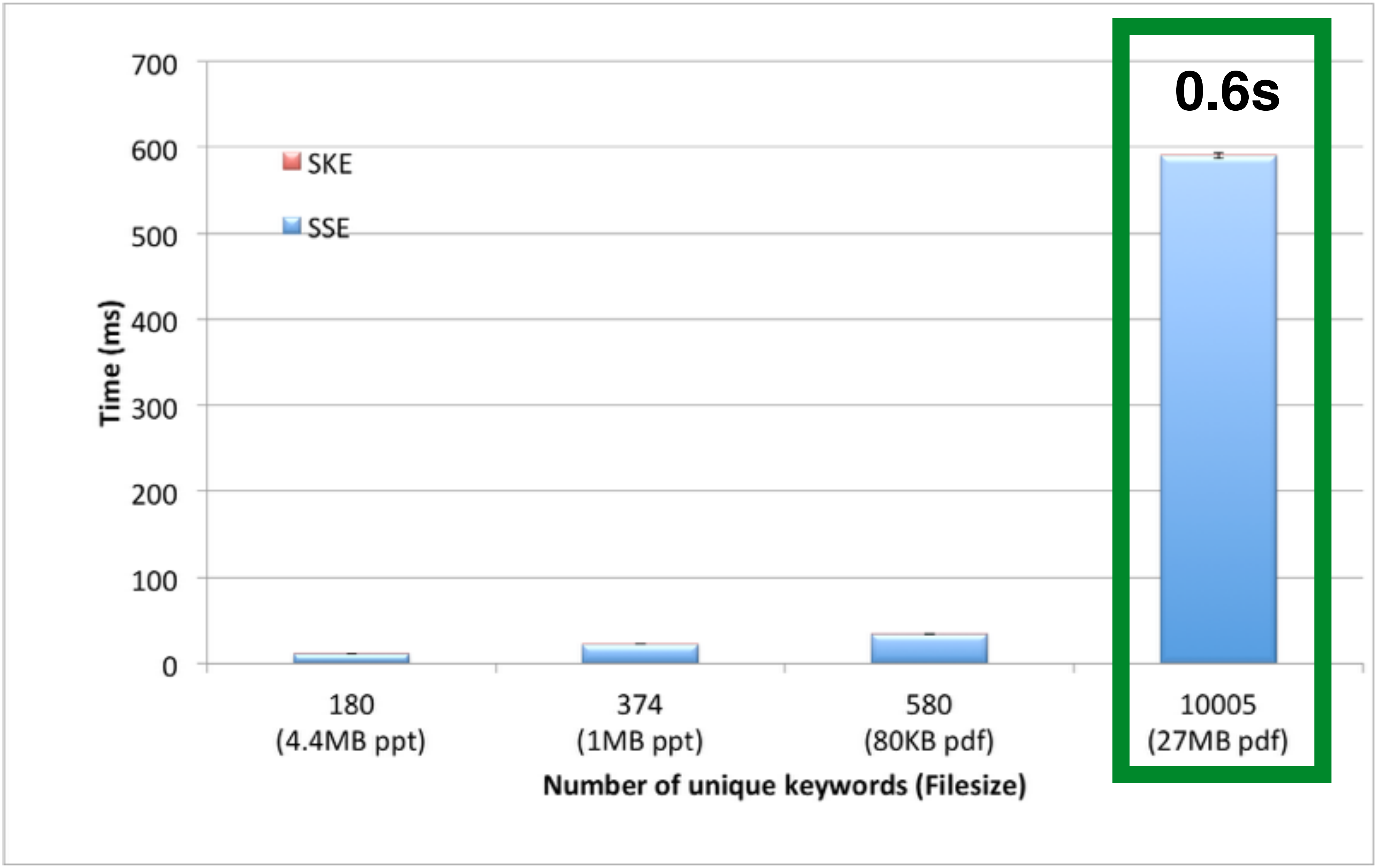
Search


0.008s
Time (ms)
10.00
9.00
8.00
7.00
6.00
5.00
4.00
3.00
2.00
1.00
0.00
2.17
2.96
3.27
5.13
5.12
5.83
6.93
7.73
1/8 (132)
1/4 (284)
3/8 (415)
1/2 (670)
5/8 (818)
3/4 (994)
7/8 (1185)
1 (1336)
Fractions of 1GB Documents
(Number of documents containing word "the")

Add


700
600
500
400
300
200
100
0
Time (ms)
🟥 SKE
🟦 SSE
180
(4.4MB ppt)
374
(1MB ppt)
580
(80KB pdf)
10005
(27MB pdf)
Number of unique keywords (Filesize)

Add


0.6s
700
600
500
400
300
200
100
0
Time (ms)
SKE
SSE
180
(4.4MB ppt)
374
(1MB ppt)
580
(80KB pdf)
10005
(27MB pdf)
Number of unique keywords (Filesize)

Delete is free

Because of our **lazy delete strategy**

Conclusion

- Blind storage primitive
  - Can have other applications
- Much simpler, scalable and secure dynamic SSE scheme
- More practical scheme: No server-side computation
  - Can be deployed on commercial cloud storage services such as Dropbox
- Several possible extensions (Ongoing work)

Paper and Slides available at

www.cryptoonline.com