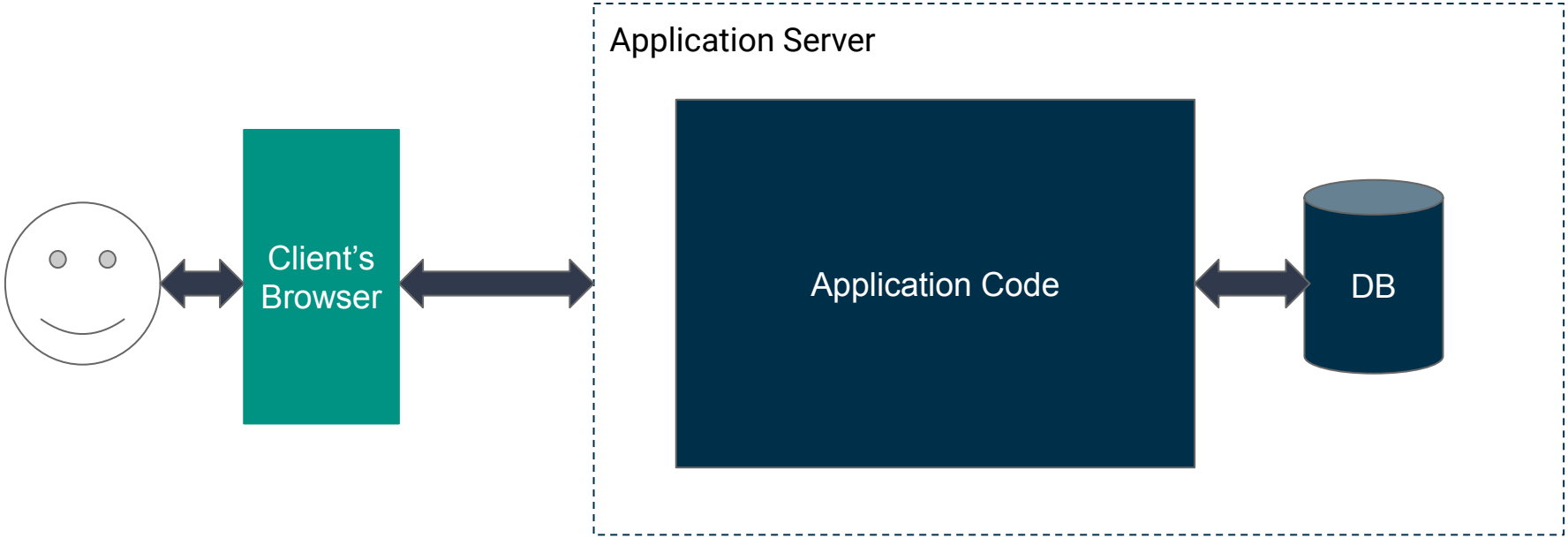
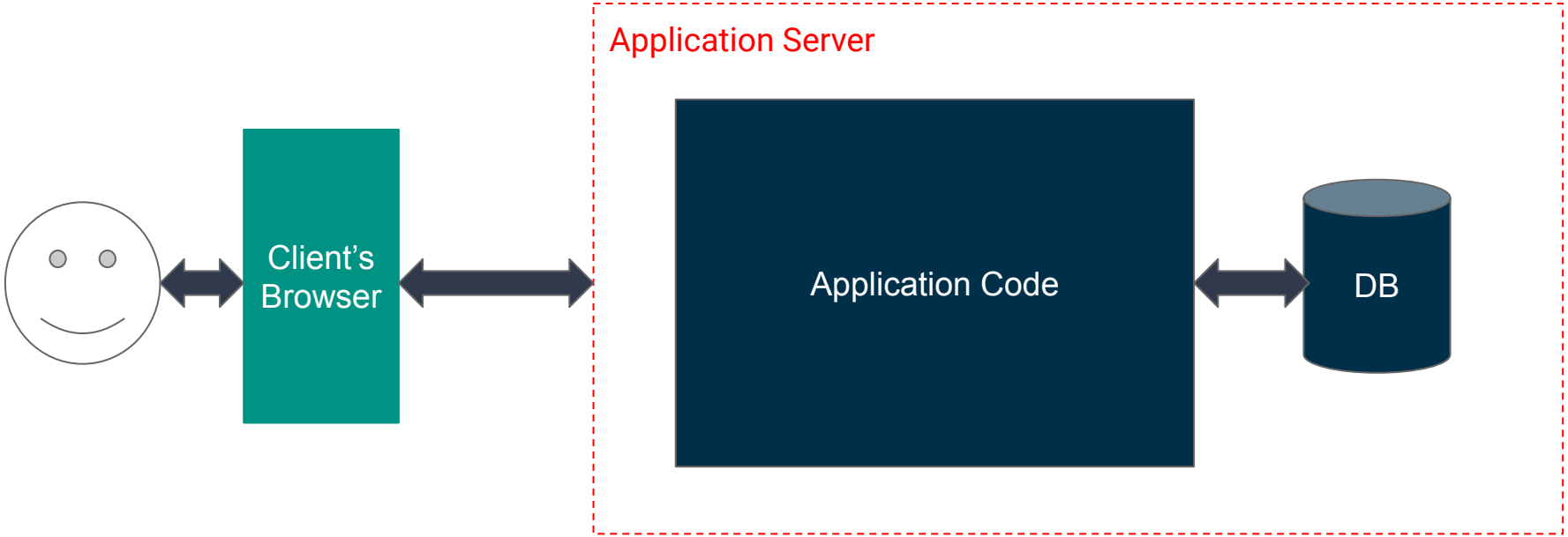
Introduction to Mylar

A visual guide

Threat Model

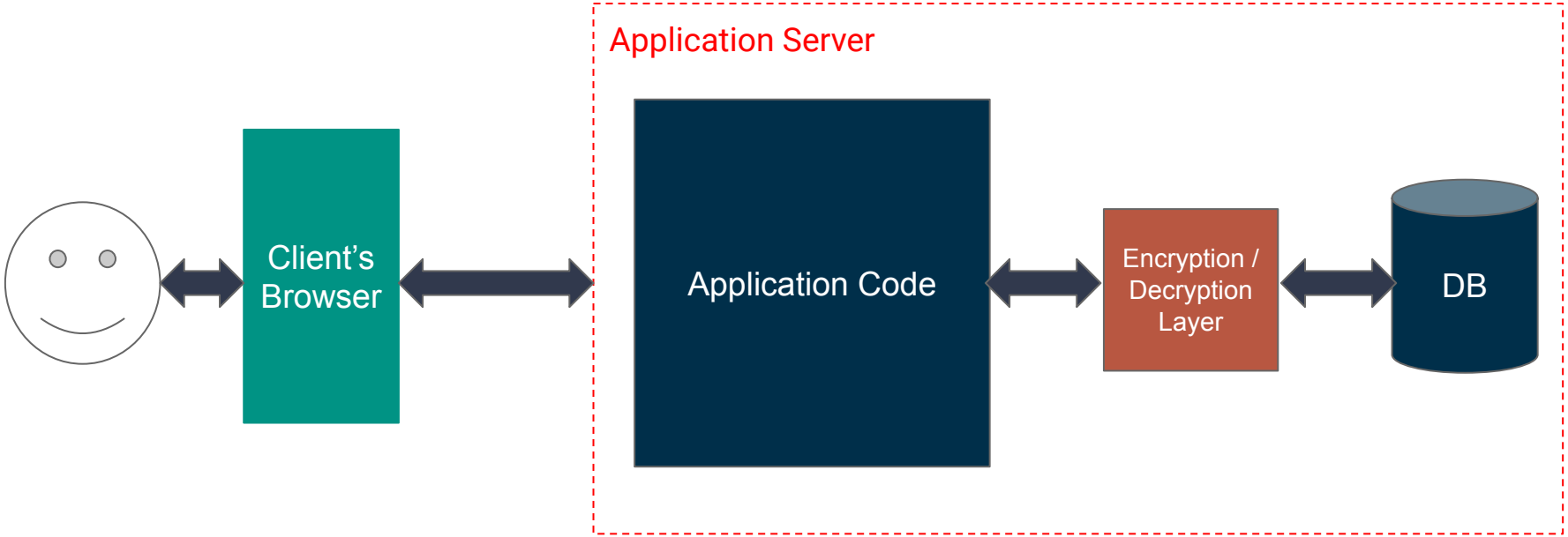


Threat Model

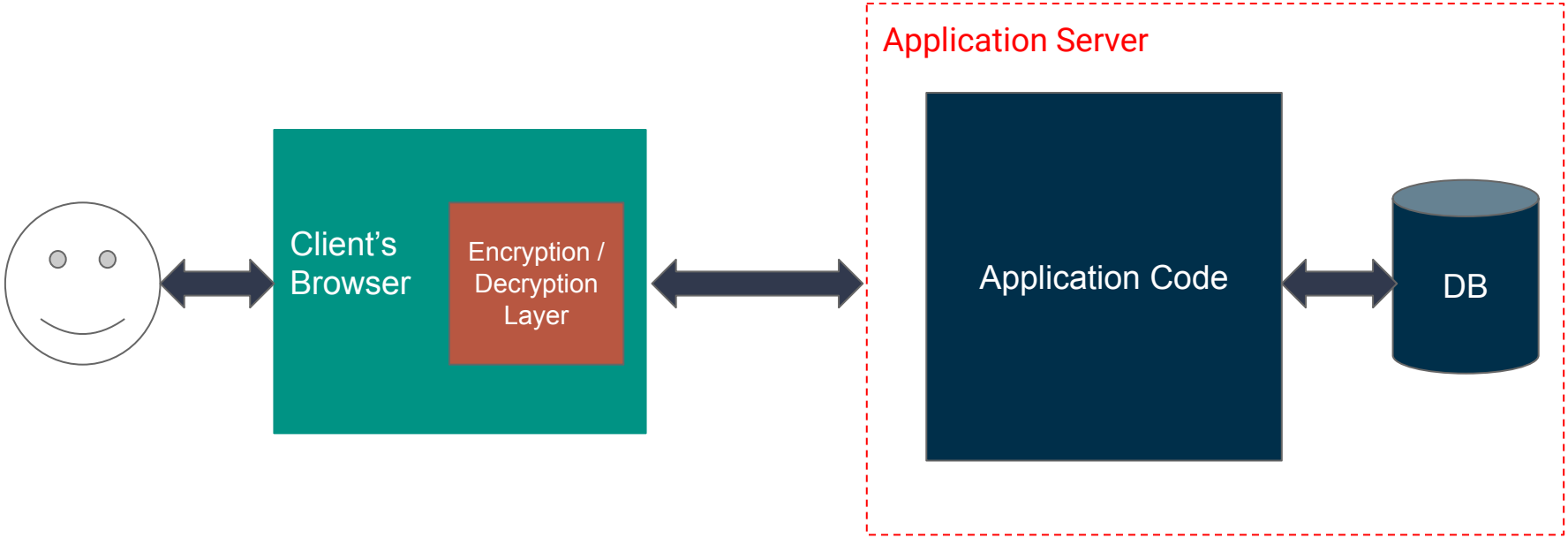


*Assume site owner/developer not malicious (will not leak keys)

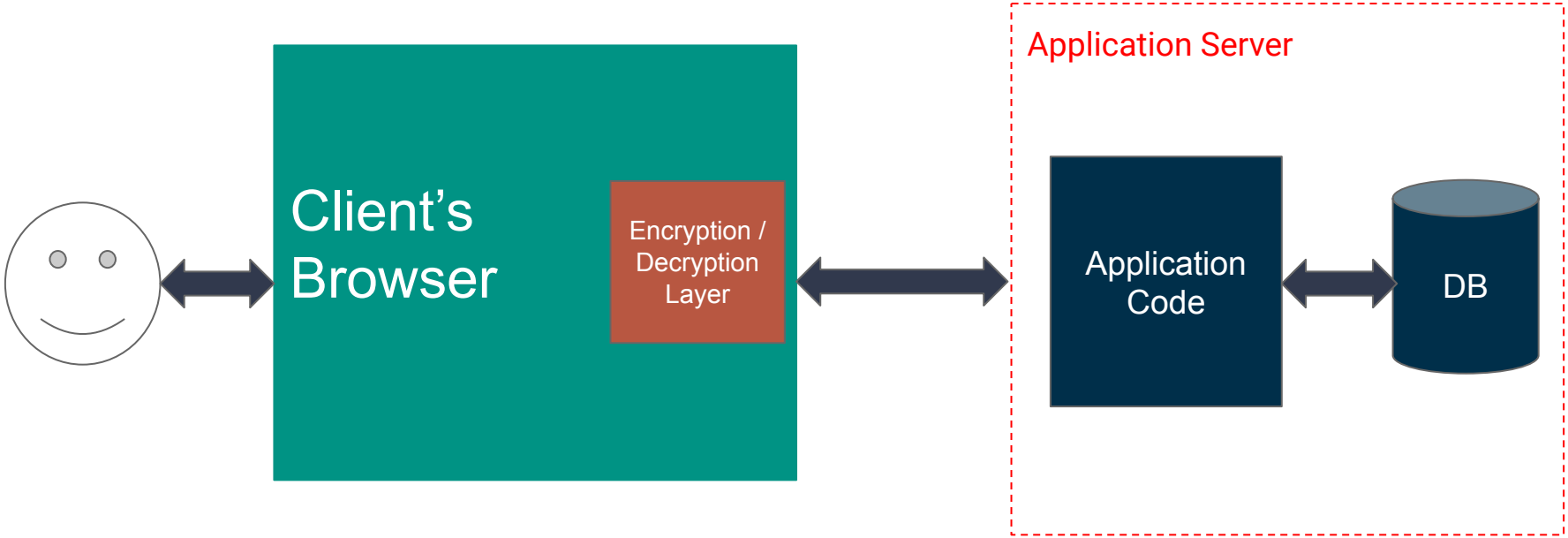
Threat Model



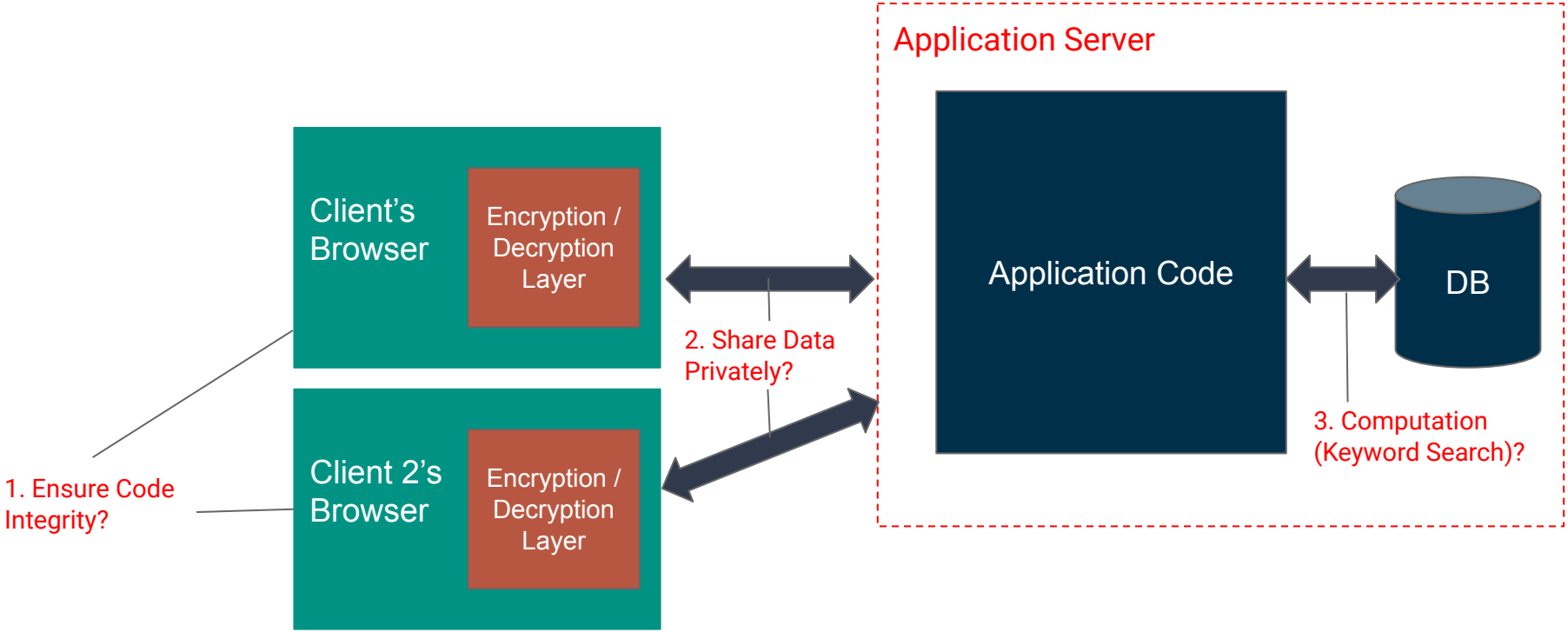
Mylar's Approach



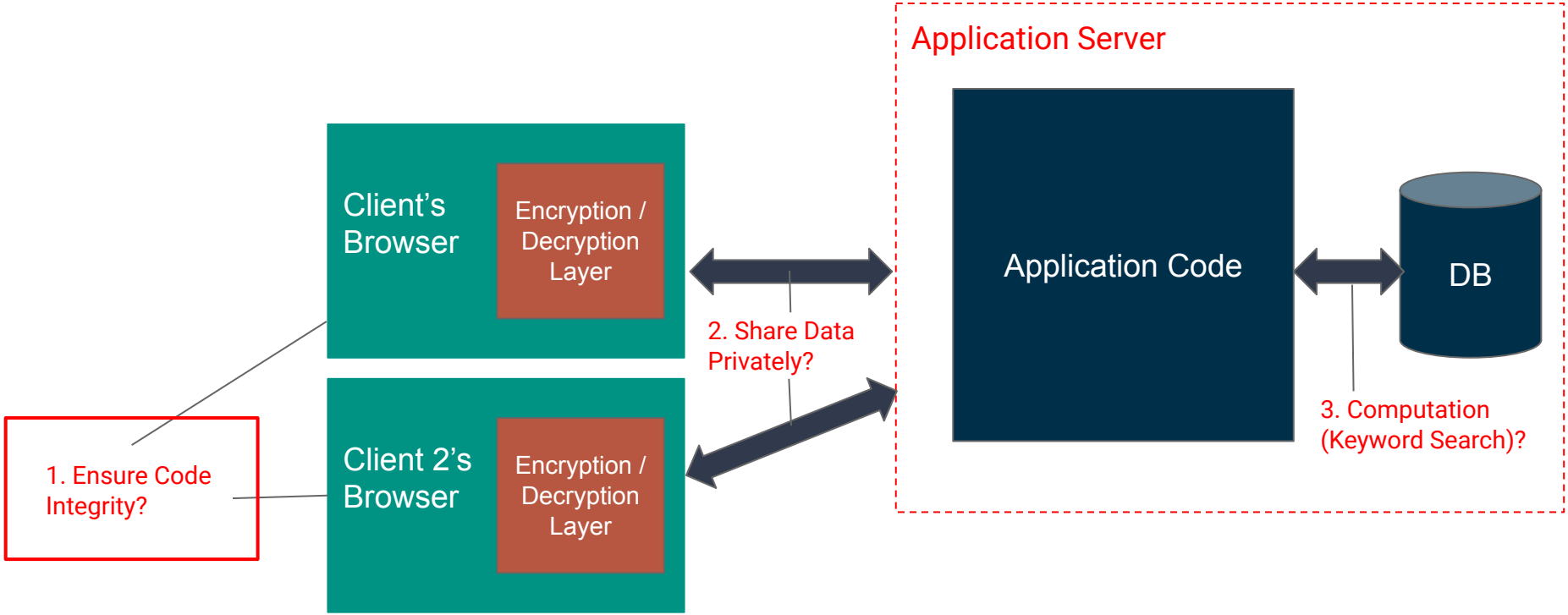
Mylar's Approach



Mylar's Approach



Mylar's Approach



Issue 1 – Ensuring Code Integrity

```
<html>
<head>
    <script src="app-logic.js"></script>
</head>
<body>
    <div>LOL</div>
</body>
</html>
```

to

Primary Origin

https:// www.mydomain.com/

Browser Extension

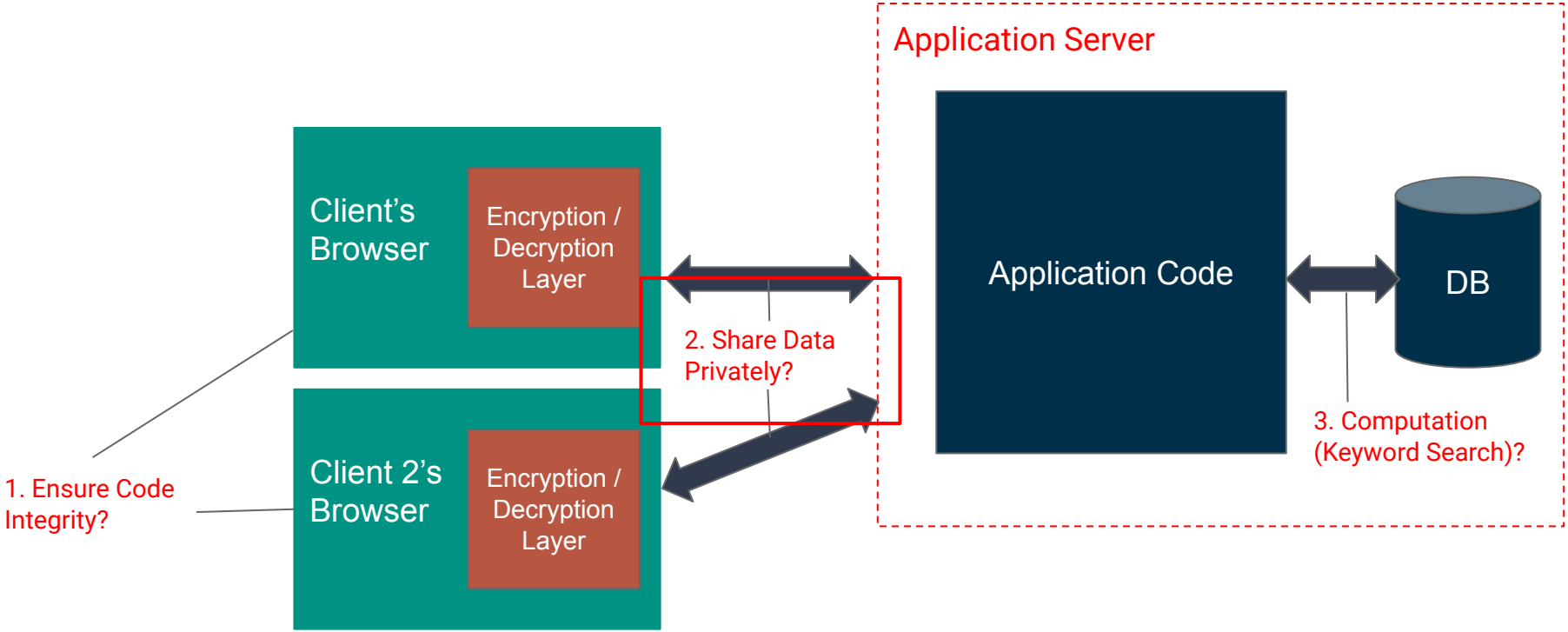
X.509 Certificate with mylar_pubkey

```
response.header["Mylar-Signature"] = "koqewkejsad2131jh12kj"
<html>
<head>
    <script src="https://www.mydomain.com/mylar.js?mylar_hash=dasd88sada"></script>
    <script src="https://origin2.mydomain.com/app-logic.js?mylar_hash=as5das5d67da6"></script>
</head>
<body>
    <div>LOL</div>
</body>
</html>
```

mylar_hash parameter

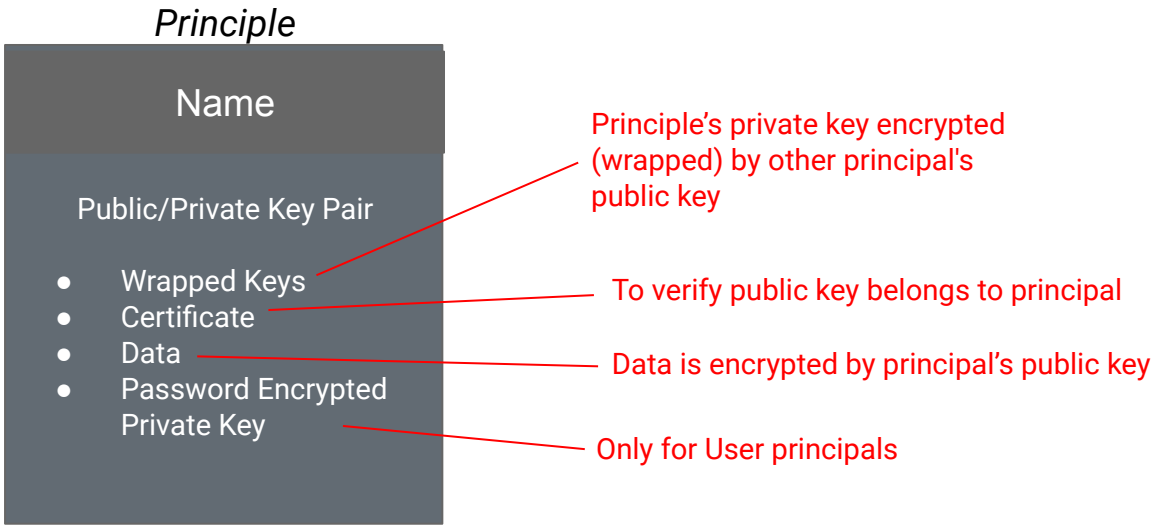
Second Origin

Mylar's Approach



Issue 2 - Share Data Privately

- Represents an application-level access control entity.
- E.g. user, group, shared document



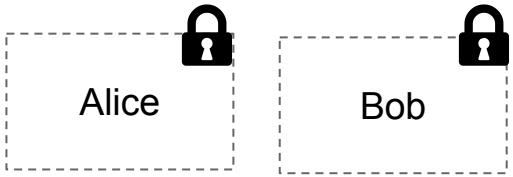
Issue 2 - Share Data Privately

Client-Side

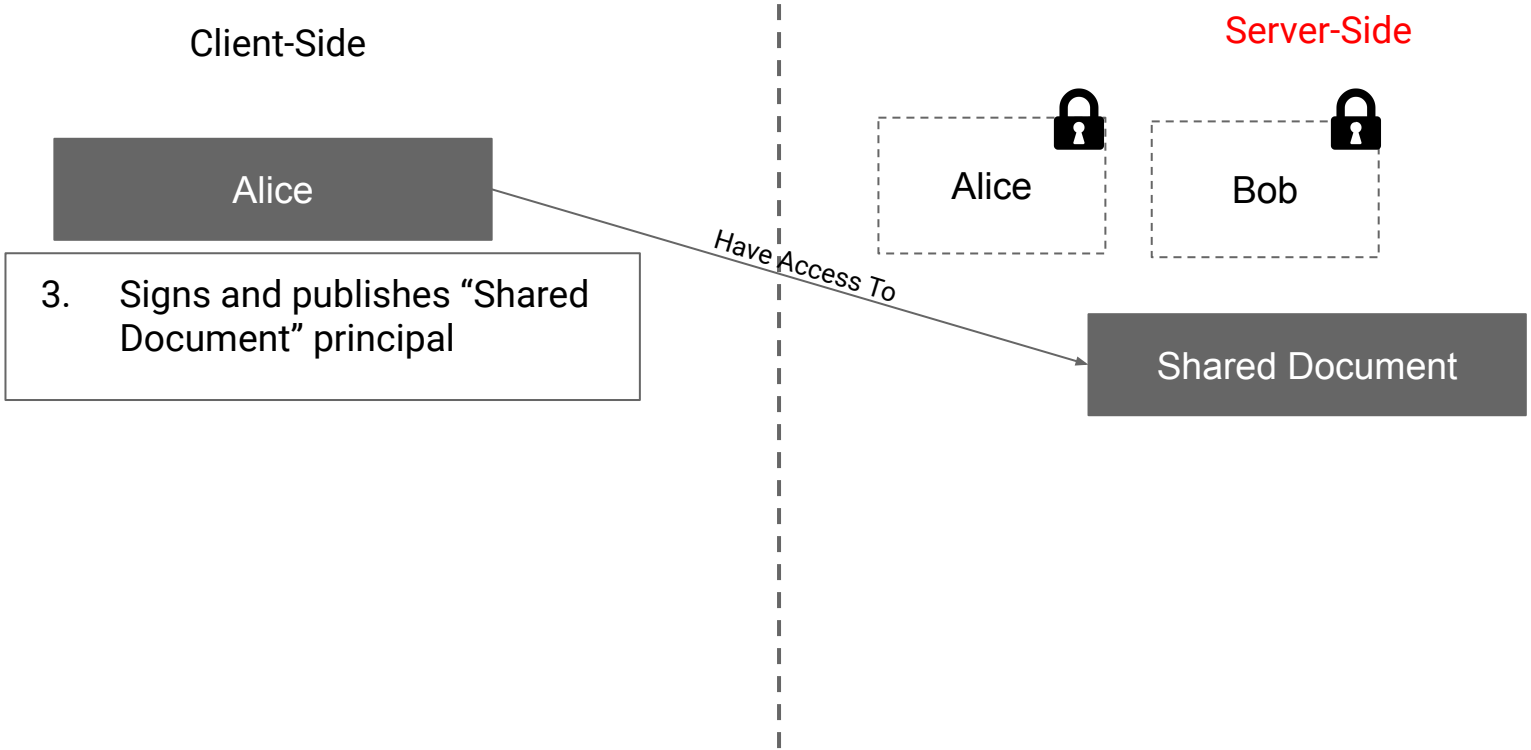
Alice

1. Alice generates “Shared Document” pub/priv key pair
2. Create wrapped key $E(Priv_{Shared\ Doc,}\ Pub_{Alice})$

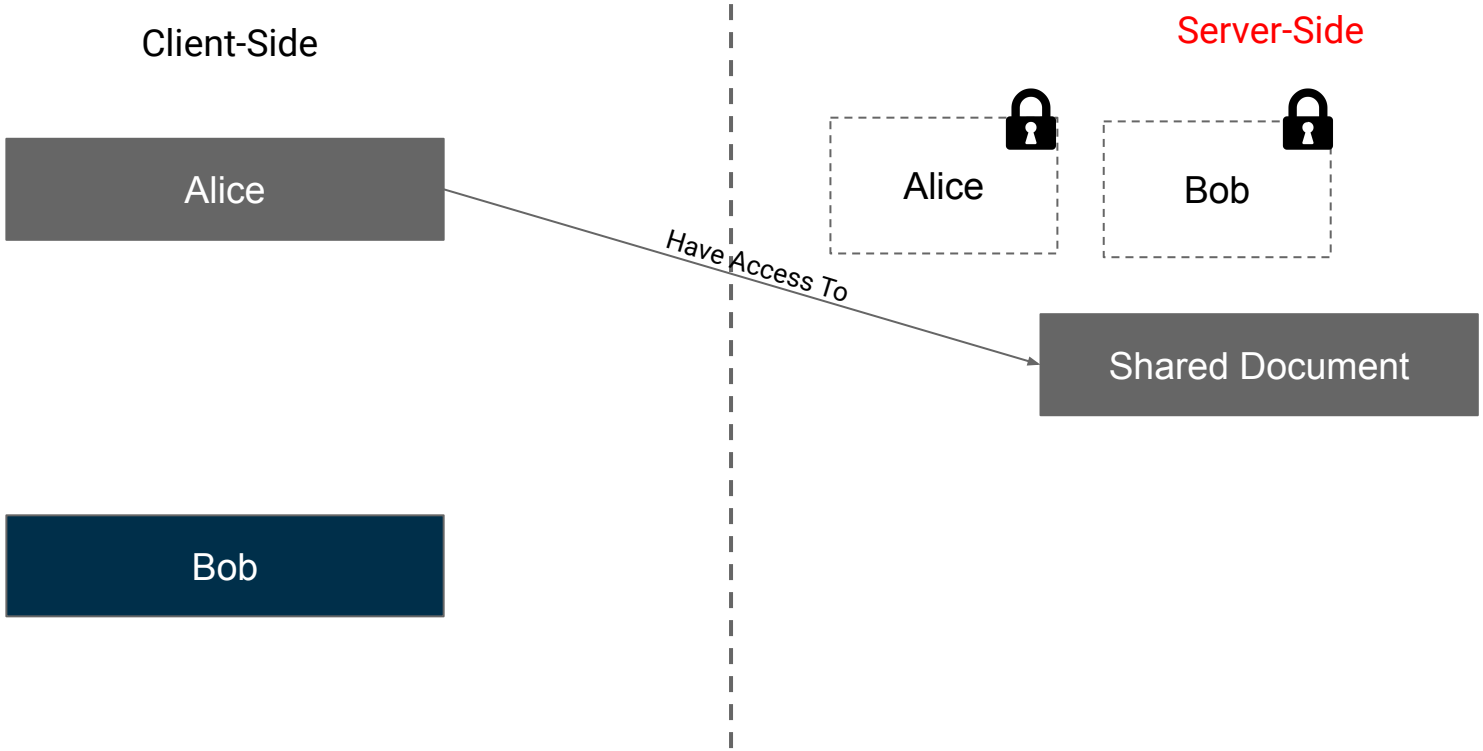
Server-Side



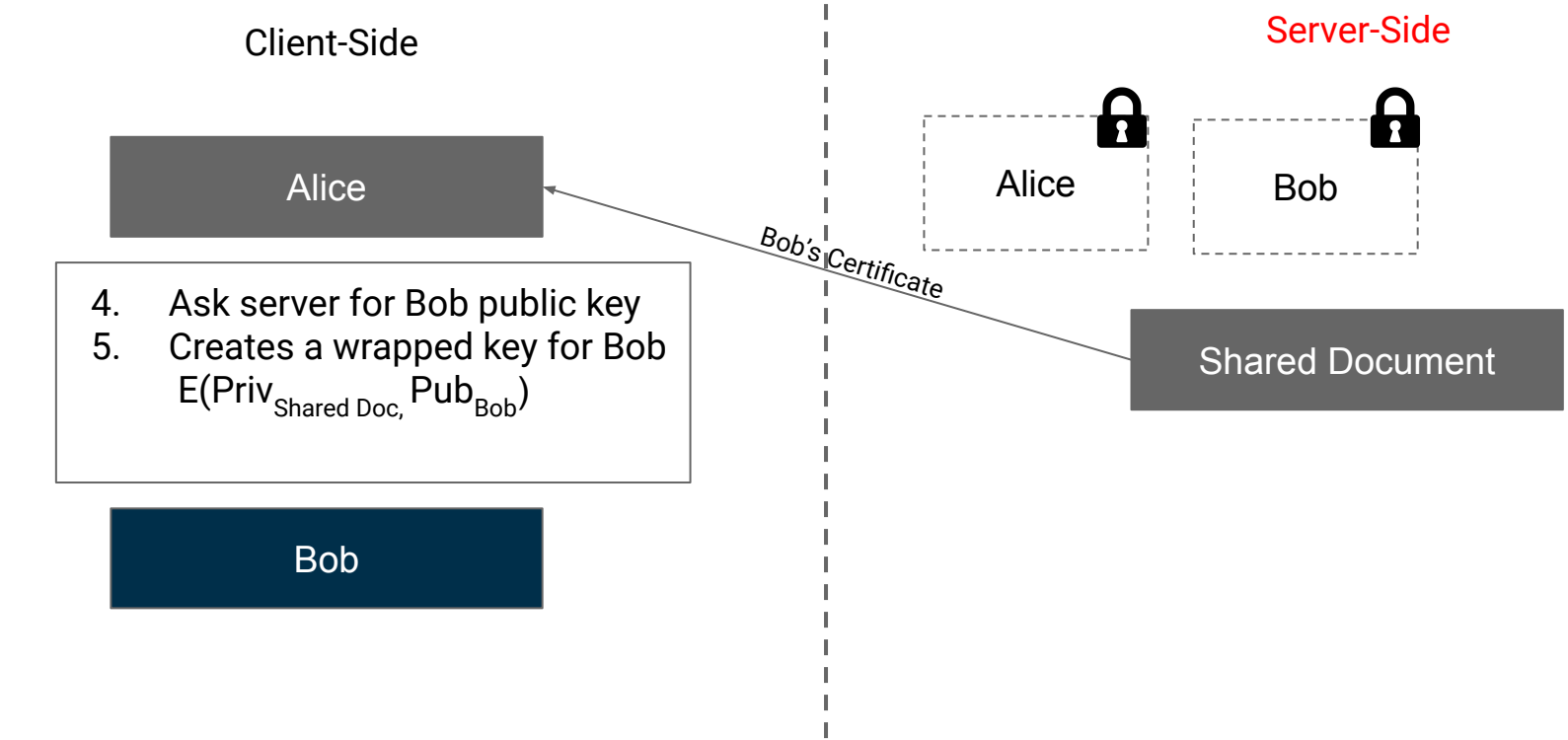
Issue 2 - Share Data Privately



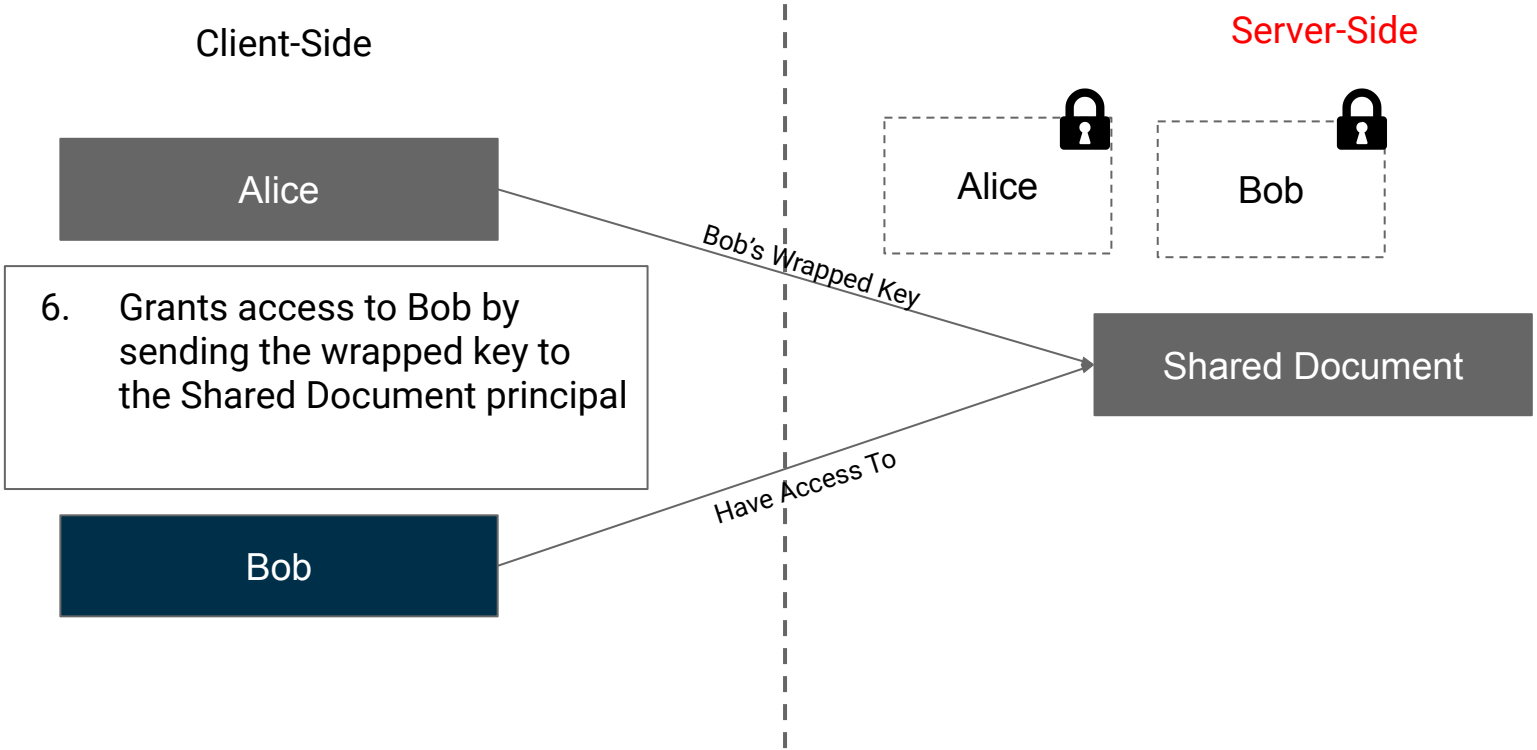
Issue 2 - Share Data Privately



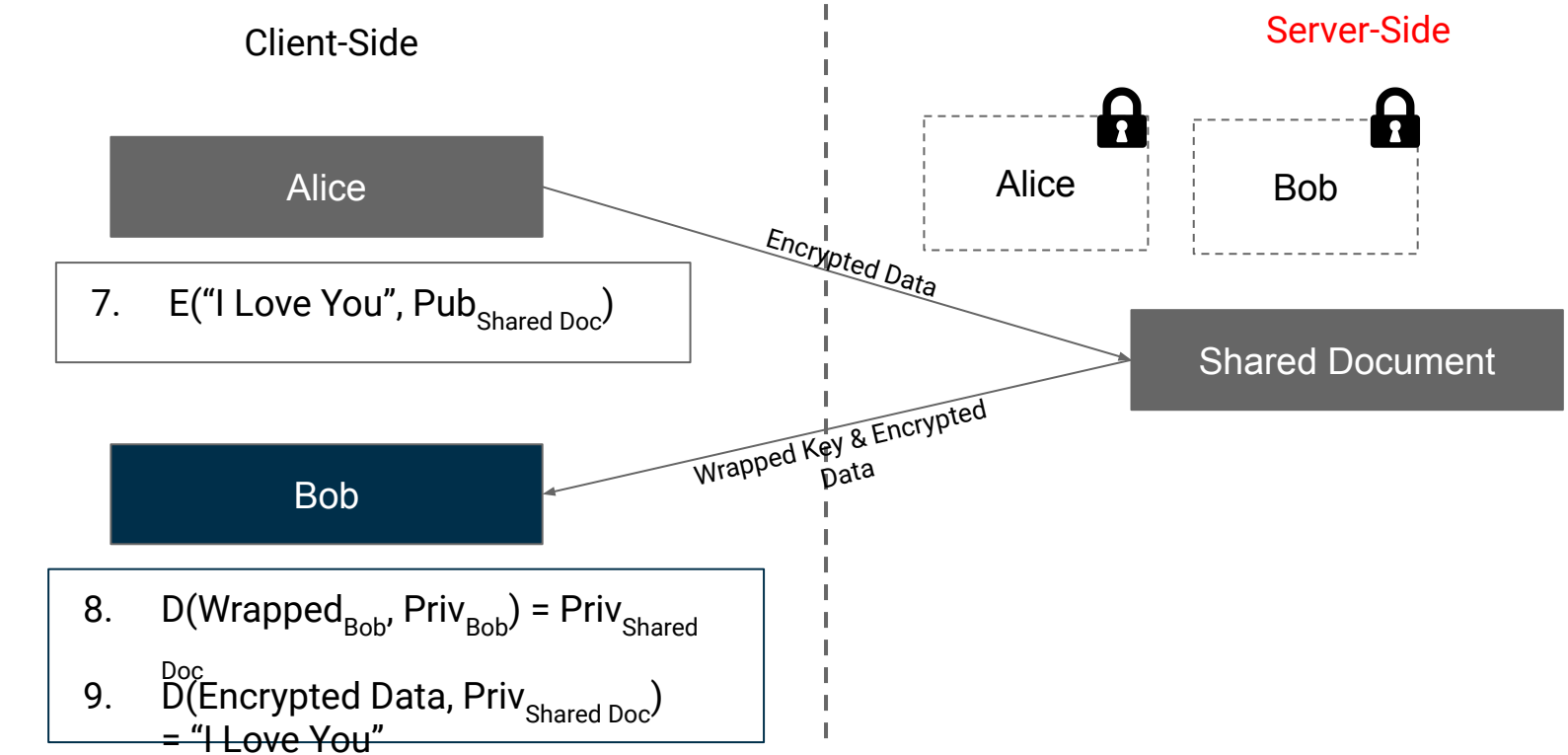
Issue 2 - Share Data Privately



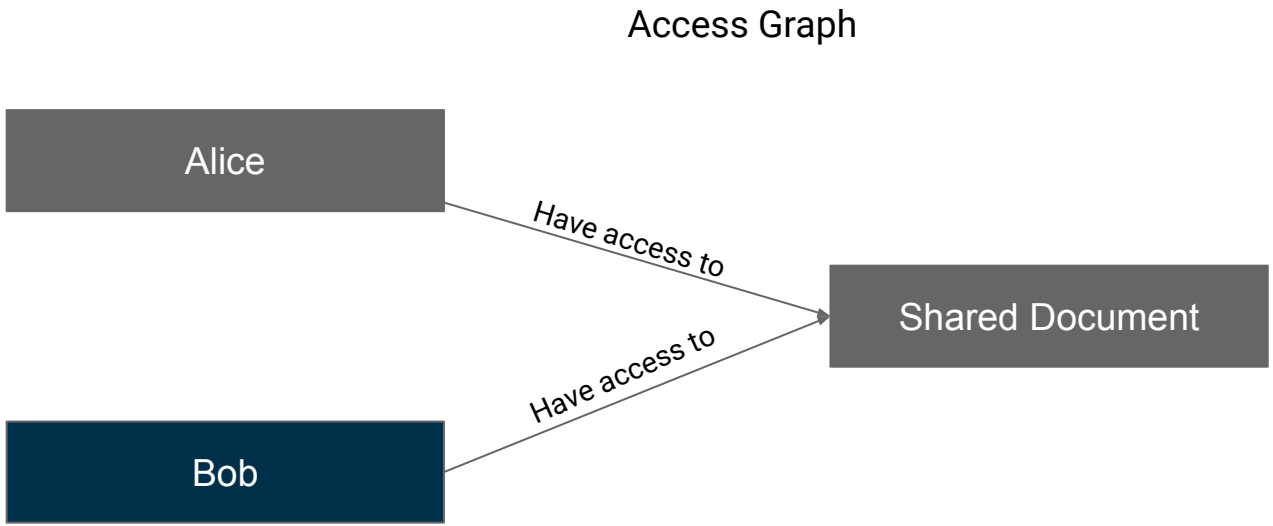
Issue 2 - Share Data Privately



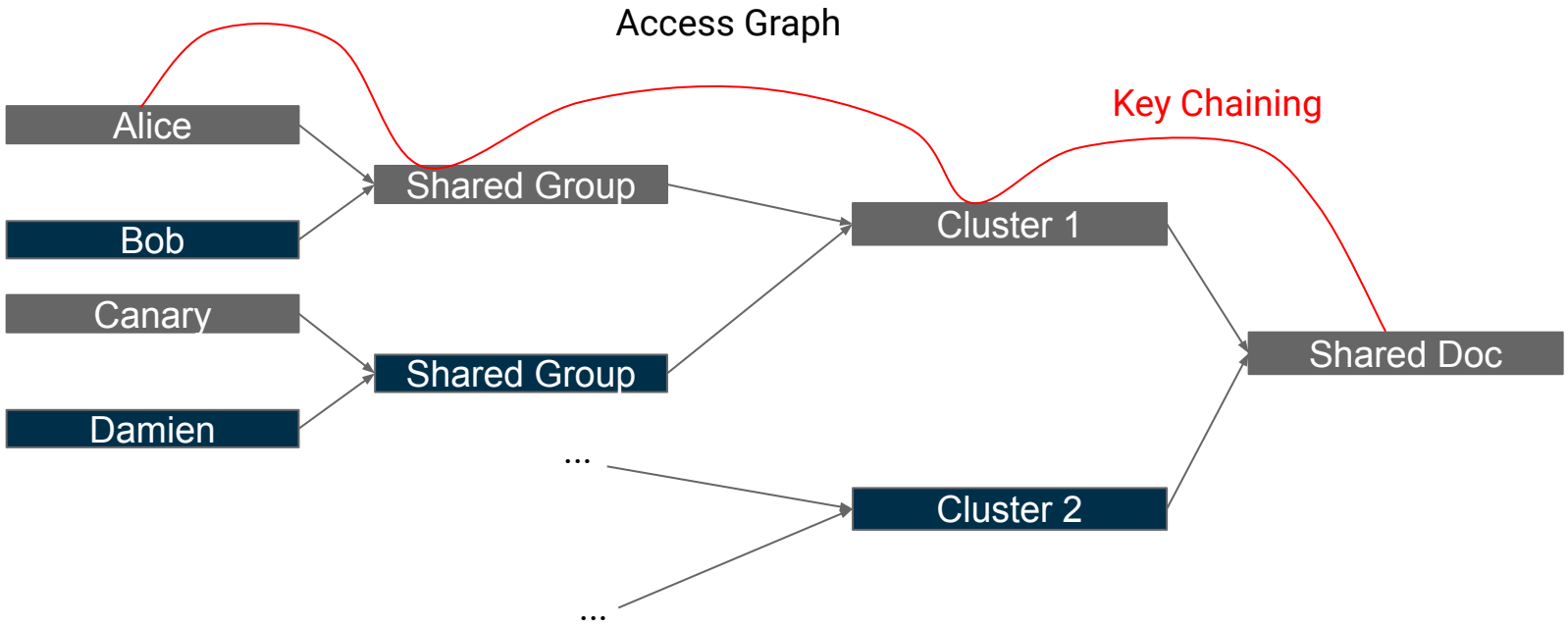
Issue 2 - Share Data Privately



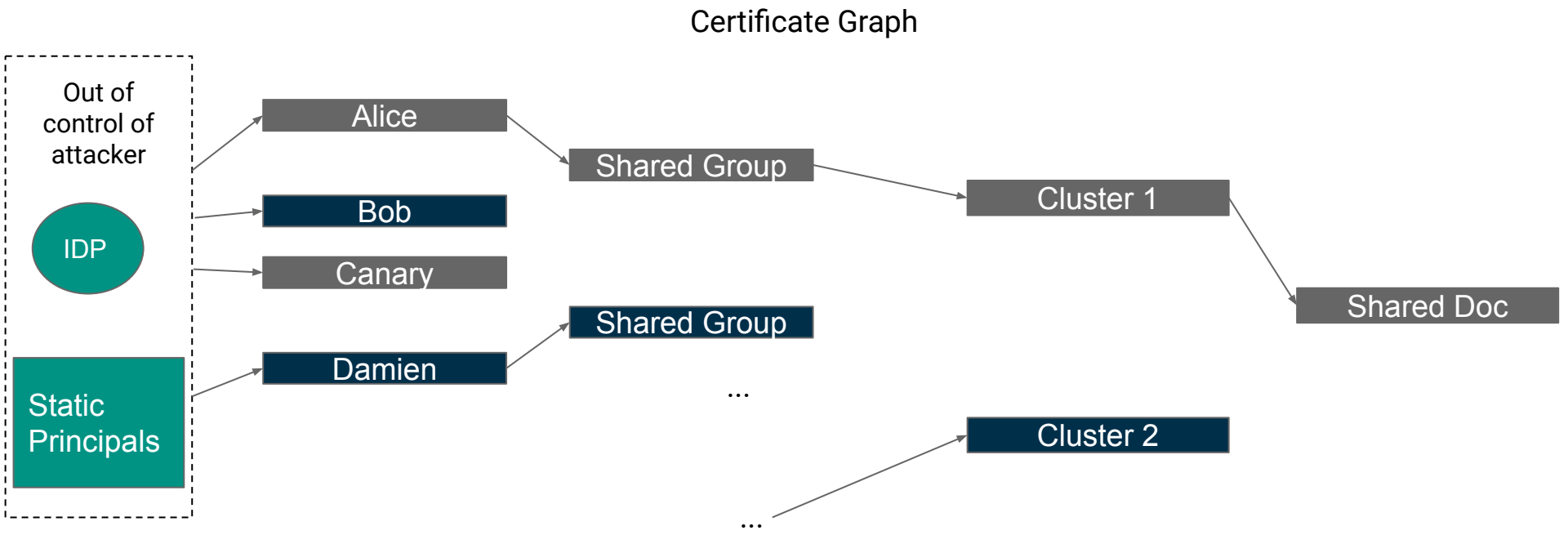
Issue 2 - Share Data Privately



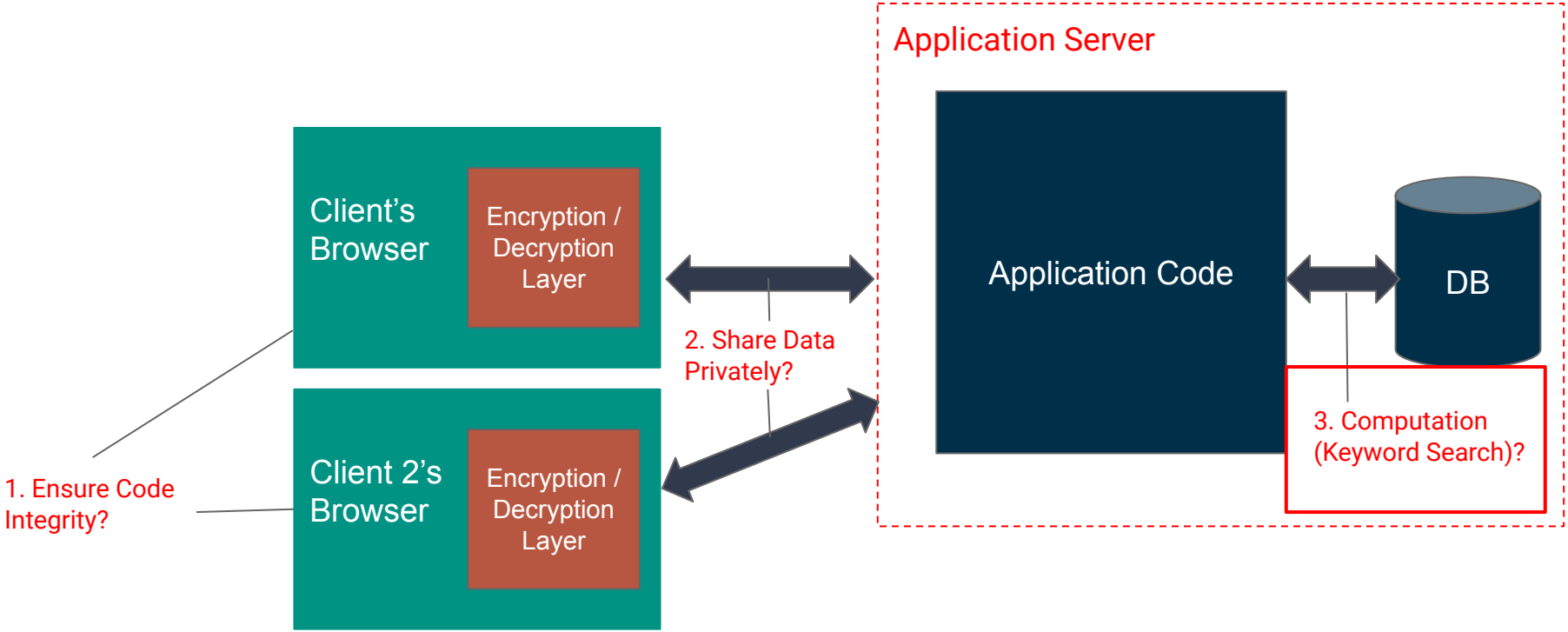
Issue 2 - Share Data Privately



Issue 2 - Share Data Privately



Mylar's Approach



Issue 3 – Computation Over Encrypted Data (Search)

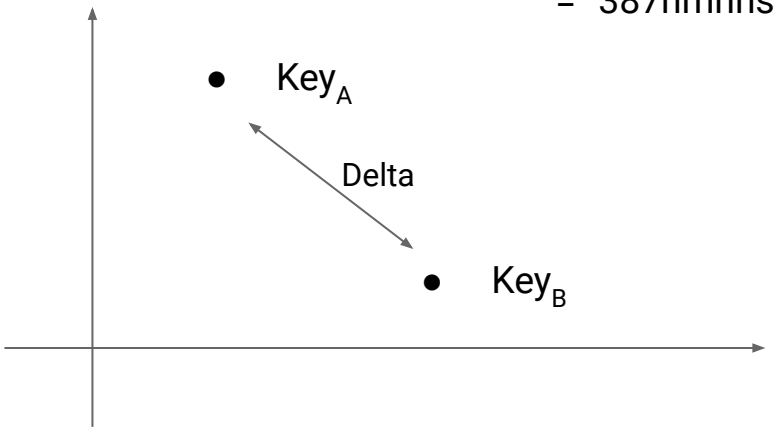
Document A Principal

$H_2(r, e(H(Word), g)^{Key})$

Document B Principal

$H(\text{“Apple”})^{KeyA}$
= “tyu32hj4”

$H(\text{“Apple”})^{KeyB}$
= “387nmhns”



Nice Property: $e(H(w)^a, g^b) = e(H(w), g)^{ab}$

Issue 3 - Computation Over Encrypted Data (Search)

“Apple”

procedure MATCH(atk, $c = \langle r, h \rangle$)
▷ Return whether c and atk refer to same word
$h' \leftarrow H_2(r, atk)$
return $h' \stackrel{?}{=} h$

$h' = H_2(r, atk)$

$= H_2(r, e(tk, \Delta_{KeyA \rightarrow KeyB}))$

$= H_2(r, e(H(\text{“Apple”})^{KeyA}, \Delta_{KeyA \rightarrow KeyB}))$

$= H_2(r, e(H(\text{“Apple”})^{KeyA}, g^{KeyB/KeyA}))$

$= H_2(r, e(H(\text{“Apple”}), g)^{KeyB})$

=

$h = H_2(r, e(H(\text{“Apple”}), g)^{KeyB})$

Guarantees

- Data confidentiality in the face of arbitrary server compromises
  - As long as none of the users that have access to the data is compromised

- Data Authenticity
  - But not freshness or correctness

How is Mylar Different?

Mylar

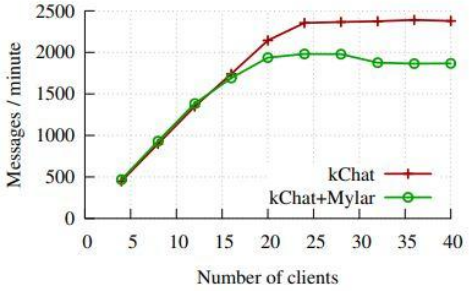
- Threat model assumes entire server compromised
- Provides guarantees for data confidentiality
- Only Search operation supported
- Built-in ACL controls and data sharing
- Better suited for NoSQL variant DBs
- Potentially significant effort on client-side

CryptDB

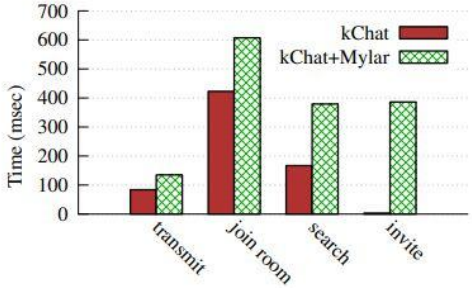
- 2 Threat Models
- Provides partial guarantees for data confidentiality
- Most SQL operations supported
- Isolation of user's data (no sharing)
- Better suited for SQL variant DBs
- Hidden from clients

Effort and Performance

Application	LoC before	LoC added for Mylar	Number and types of fields secured	Existed before?	Keyword search on
kChat [23]	793	45	1 field: chat messages	Yes	messages
endometriosis	3659	28	tens of medical fields: mood, pain, surgery, ...	Yes	N/A
submit	8410	40	3 fields: grades, homework, feedback	Yes	homework
photo sharing	610	32	5 fields: photos, thumbnails, captions, ...	Yes	N/A
forum	912	39	9 fields: posts body, title, creator, user info, ...	No	posts
calendar	798	30	8 fields: event body, title, date, user info, ...	No	events
WebAthena [8]	4800	0	N/A: used for code authentication only	Yes	N/A



Application	Operation for latency	Latency w/o Mylar	Latency with Mylar	Throughput w/o Mylar	Throughput with Mylar	Throughput units
submit	send and read a submission	65 msec	606 msec	723	394	submissions/min
submit w/o search			70 msec		595	
endometriosis	fill in/read survey	1516 msec	1582 msec	6993	6130	field updates/min



4x Space Overhead for kChat

Discussion

Likely to be adopted/implemented in the real world?

Thank You

How do digital signatures work?