Building Enclave-Native Storage Engines for Practical Encrypted Databases

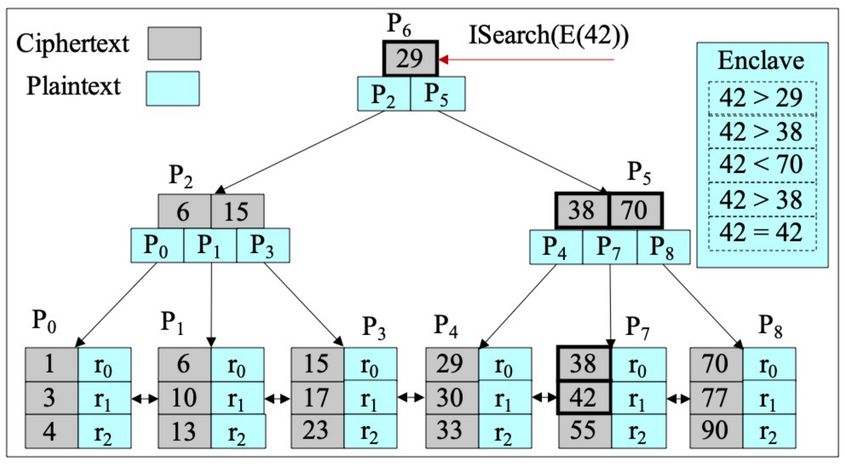
Yuanyuan Sun, Sheng Wang, Huorong Li, Feifei Li
Alibaba Group

Alibaba Group 阿里巴巴集团

DingTalk

Paper

Challenges



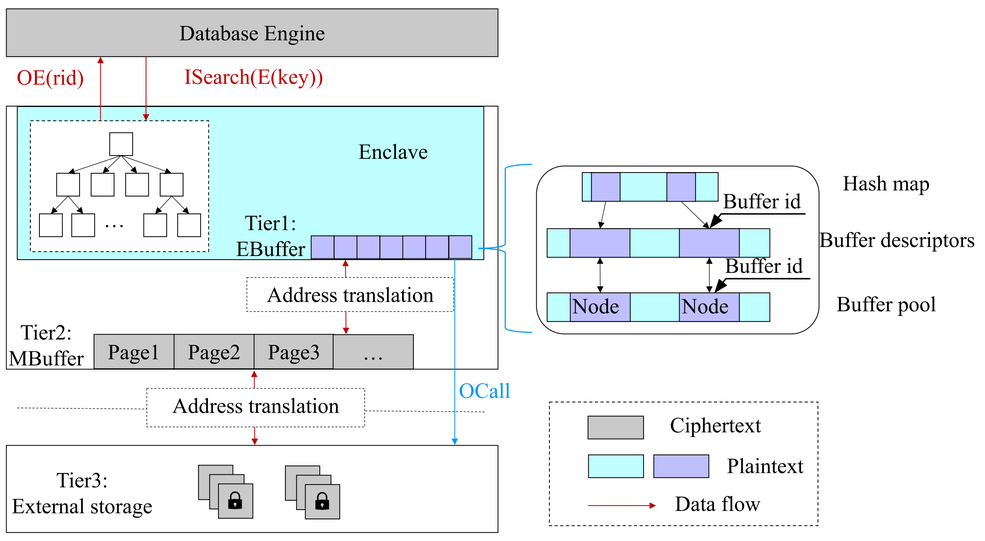
- Frequent enclave interaction
- High overheads on computation and storage
- Severe information leakage

Design space exploration

Design Dimension	Design Choice	Influence		
		Security (Information Leakage)	Performance	Functionality
Encryption Granularity	item-level encryption	leak structural information	high storage overhead; fast for a single read	can fetch data w/o enclave
	page-level encryption *	leak data volume only	low storage overhead; fast for batched small reads	all data access must be in enclave
Execution Logic in Enclave	index: key comparison	leak key ordering and search path	low performance from massive `ECalls`	can split or merge node w/o enclave
	index: index node access	leak node-level search path	high performance from a few `ECalls`	all index access must be in enclave
	table: none	leak record-level identity and location	high performance from no `ECall`	can fetch or scan record(s) w/o enclave
	table: data page access *	leak page-level identity and location	medium performance from a few `ECalls`	all record access must be in enclave
Memory Access Granularity	item-level access *	leak item-level access pattern	high performance from on-demand read	require small footprint in enclave
	page-level access	leak page-level access pattern	moderate performance from page copy	require large footprint in enclave
Enclave Memory Usage	minimum usage *	no additional access protection	low performance from active data fetching	no EPC capacity requirement
	fixed usage	hide a few frequently accessed items	medium performance from data caching	low EPC capacity requirement
	proportional usage	hide many frequently accessed items	medium performance from data caching	high EPC capacity requirement
	unlimited usage	hide access to all items	high performance from data caching	high EPC capacity requirement
Record Identity Protection	no action	leak record identity among queries	no influence	no influence
	***rid* encryption** *	hide linkage between *rid* and record	little influence	only useful in some settings
	ciphertext re-encryption *	hide cipher identity among queries	little influence	only useful in some settings

- Possible design choices for encrypted storage categorized in five dimensions
- Bolded for Enclage Index
- Tagged with an asterisk mask for Enclage Store
- The trade-off of security, functionality and performance

Enclage Index

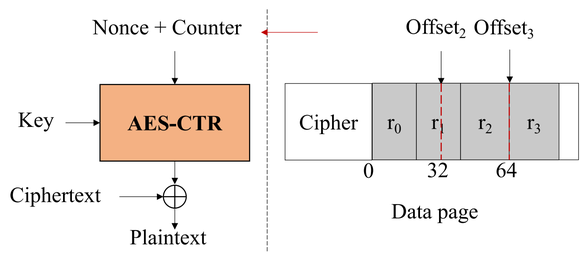


- A B⁺-tree-like index
- Three-tier hierarchical architecture
- Page-level encryption
- Index execution logic in enclave
- Fix enclave memory usage

Optimizations

- Reduction of EPC page swapping overhead
- Mitigation of enc/decryption cost
- Avoidance of unnecessary of OCalls

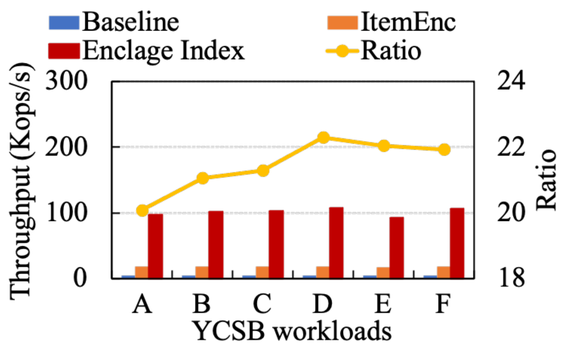
Enclage Store



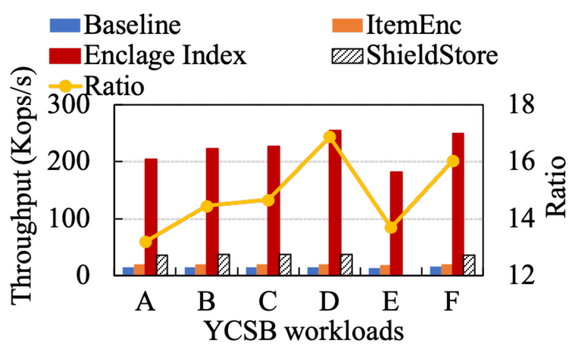
- A heap-file-like table store
- Append-only strategy
- Delta-decryption protocol for saving time

Evaluations

Overall performance

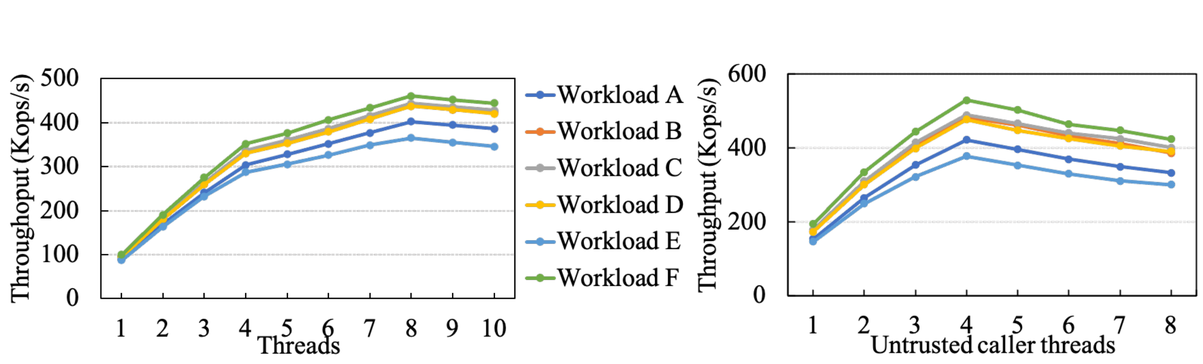


Switch mode

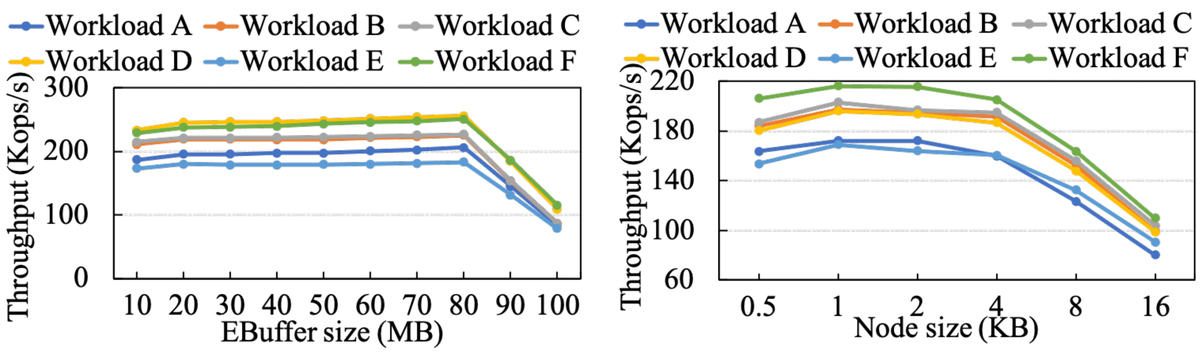


Switchless mode

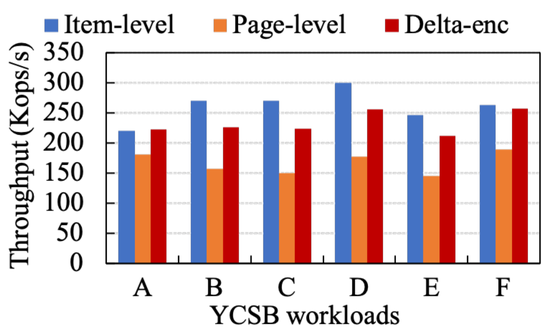
Scalability to Multiple Cores



The impact of sizes



Different Decryption Protocols



	16B	32B	64B	128B	256B
Item-level (GB)	0.67	0.89	1.36	2.29	4.09
Page-level (GB)	0.23	0.45	0.91	1.85	3.81
Ratio	2.99	1.98	1.50	1.24	1.07