Vallum: Database Privacy, Confidentialy and Access Rights for Sensitive Data in Cloud Environments

Ronny Peterson[1], André Carvalho[1], Gabriel Fernandez[2], Lucas Cavalcante[3], Altigran da Silva[1] and Christof Fetzer[2]

Federal University of Amazonas[1], Technische Universität Dresden[2], Federal University of Campina Grande[3]

E-mail: {ronny,andre@}icomp.ufam.edu.br

INTRODUCTION

- **Sensitive data** management and protection is a growing concern. Examples of such data are medical records, biometric data, buyer information, query logs and even business-related information.
- In cloud environments there is no external control on who has **physical access to the infrastructure**, or whether there are no security flaws in the software stack.
- It is essential to guarantee that no unwanted third party has access to sensitive data, i.e., to provide secure **access control.** In many times, in **multiple granularities.**
- Even when compliant to access restrictions, sensitive data might also have **privacy constraints**, i.e., identification of data subjects.
- Even with data encryption at rest, during main memory processing sensitive data is **vulnerable** to main memory sniping.

THREAT MODEL

Infrastructure Level Adversary

- Controls software stack.
- RAM Manipulation and Reading.
- May have physical host access.
- Is not able to decrypt TLS connection

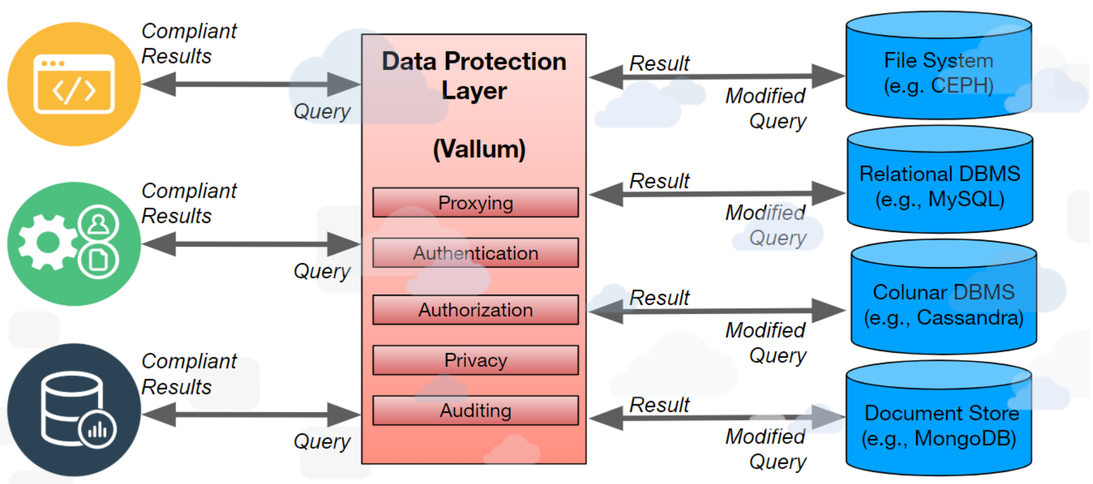
May read or modify sensitive data through main memory attacks

User Level Adversary

- Has valid credentials.
- No abnormal control over system or host
- Has total control over client side.
- May have the highest credentials in the system.

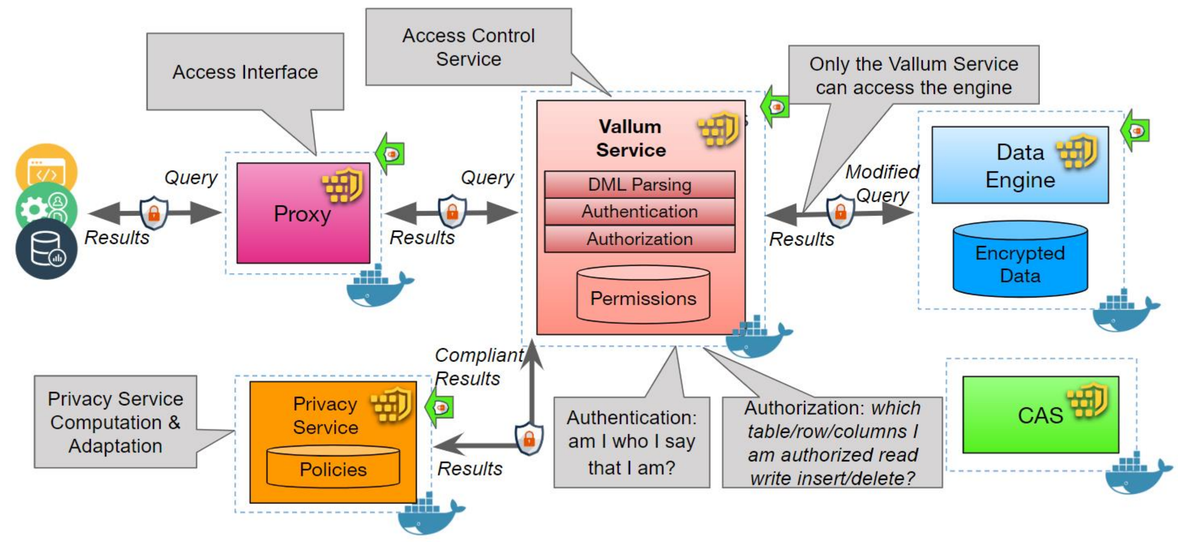
May access private data through the use of finely-crafted queries

VALLUM



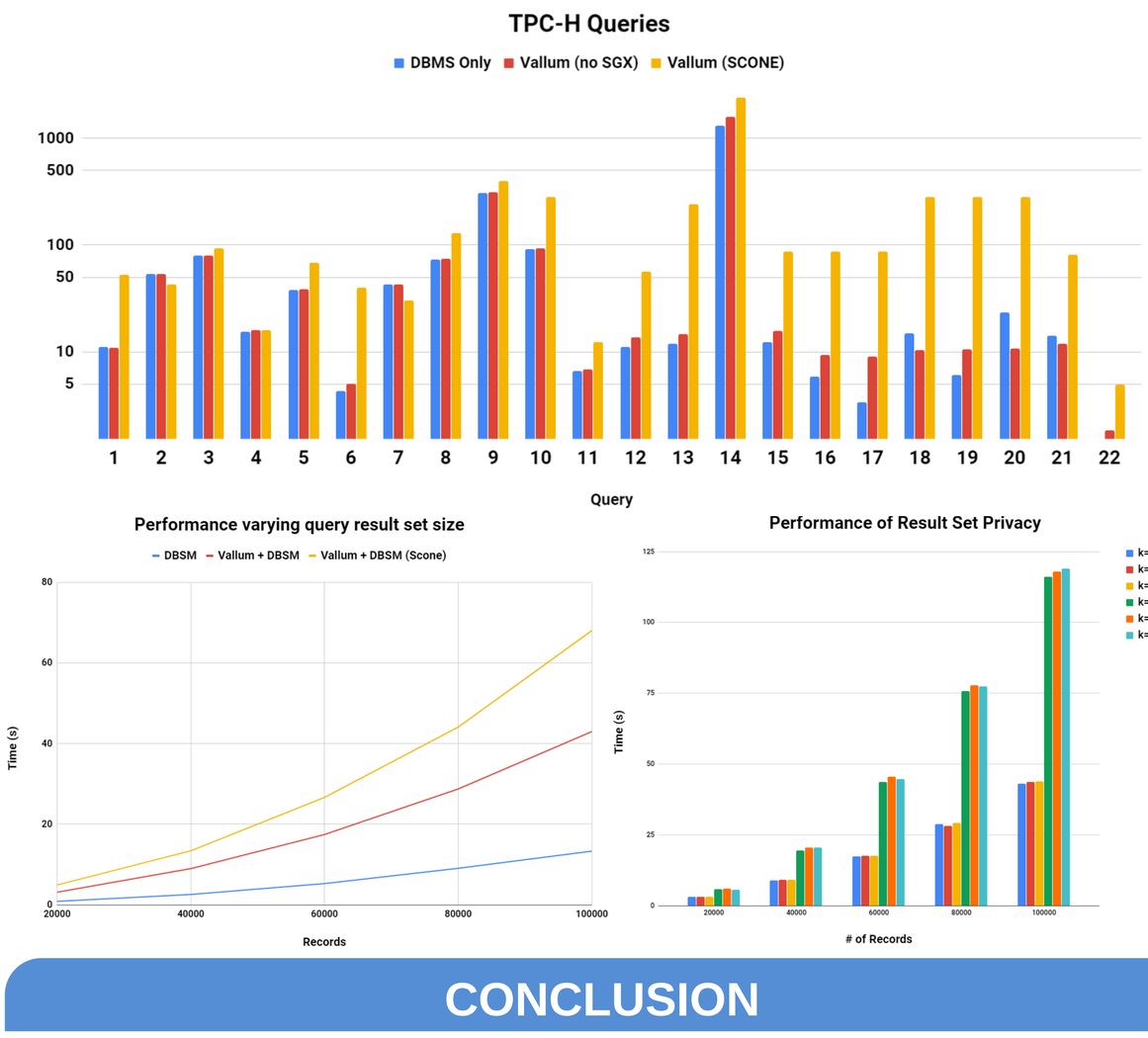
- **Data processing protection layer,** where the users communicate with the layer instead of directly with the data source.
- **Isolating the data source**, by guaranteeing that it only accepts queries from Vallum.
- All communications between modules done through secure TLS connections.
- Vallum is responsible for:
  - Verifying if user has valid credentials.
  - Verifying whether the user is **authorized** to perform the query.
  - **Modifying** issued query for compliance with **access constraints**.
  - Verifying if the query results are compliant to **privacy constraints** (k-anonymity, l-diversity, among others).
  - **Modifying** query results in order to comply to privacy constraints
- In order to guarantee that sensitive data is not vulnerable for a infrastructure level adversary, during this processing, all modules will be run in **SGX enclaves [1]**.
  - Guaranteeing that they are safe from memory-sniping attacks.
- Implementation: **SCONE Containers [2]**.

ARCHITECTURE



PERFORMANCE EVALUATION

- Experiments to evaluate the impact of using Vallum in system performance:
  - **TPC-H** queries to show impact on different queries.
  - Varying **result set size. S**how the impact of memory usage on the enclave.
  - Secure result set modification for privacy compliance, regarding varying levels of k-anonymity.
  - Tested methods: DBMS only (not secure), Vallum without SGX, Vallum on SCONE containers (SGX).



CONCLUSION

- Vallum is a trustworthy method to process sensitive data.
  - It isolates the user from data processing, assuring that no access or privacy constraints are violated
  - Its use of SGX Enclaves via SCONE containers protects the sensitive data against memory sniping and other physical-access based attacks,
  - Those protections come at a cost on extra computational time, however our experiments show that those are non-prohibitive.

REFERENCES

[1] V. Costan and S. Devadas, “Intel sgx explained.” IACR Cryptology ePrint Archive, vol. 2016, no. 086, pp. 1–118, 2016.

[2] S. Arnautov, B. Trach, F. Gregor, T. Knauth, A. Martin, C. Priebe, J. Lind, D. Muthukumaran, D. O’keeffe, M. Stillwell et al., “Scone: Secure W. A. Jansen, “Cloud hooks: Security and privacy issues in cloud computing,” in hicss. IEEE, 1899, pp. 1–10.

[3] Y. Xu, W. Cui, and M. Peinado, “Controlled-channel attacks: Deterministic side channels for untrusted operating systems,” in Security and Privacy (SP), 2015 IEEE Symposium on. IEEE, 2015.

[4] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam,“l-diversity: Privacy beyond k-anonymity,” innull. IEEE, 2006, p. 24.

[5] M. Poess and C. Floyd, “New tpc benchmarks for decision support andweb commerce,”ACM Sigmod Record, vol. 29, no. 4, pp. 64–71, 2000