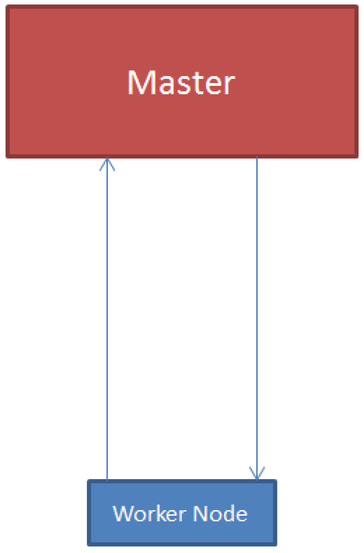
Data Security in Hybrid Clouds

Undergraduate Student: Francesca Russum
Faculty Advisors: Xinghui Zhao
Computer Science, Washington State University, Vancouver WA 98686, U.S.A.

Introduction

- Clouds can be used to perform resource-consuming tasks
- The results of these tasks can then be accessed by remote systems
- This accessibility can create undesired vulnerabilities when performing calculations on sensitive data
- In Hybrid clouds, calculations can be shared among systems.
- How can hybrid clouds be made more secure?

Hybrid Cloud Usage

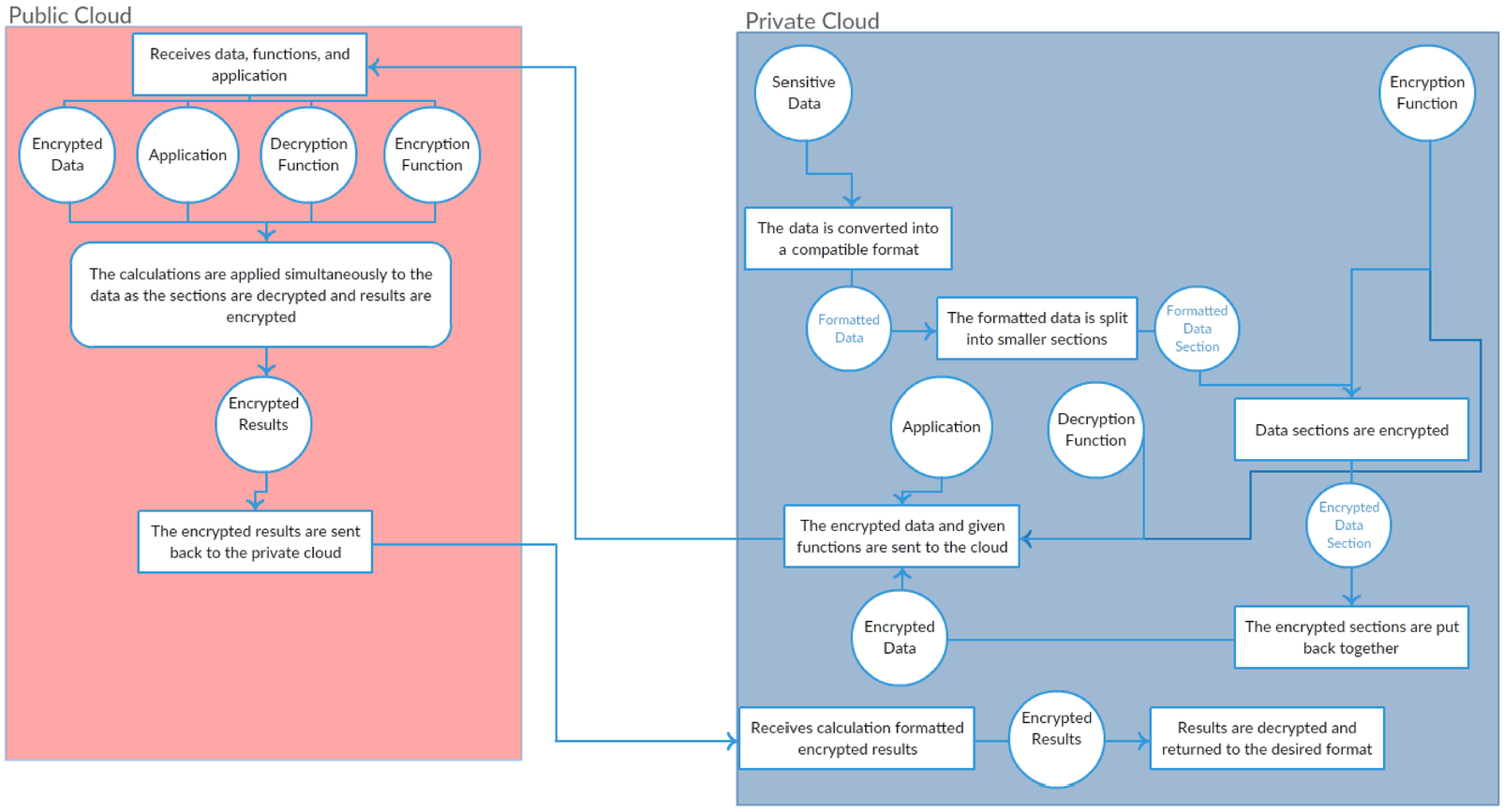


The calculation is split between the two nodes instead of being performed entirely on one

Objectives

- Create a hybrid cloud
- Create a program to use a given encryption and decryption program to securely perform a calculation based in a hybrid cloud

Secure Hybrid Cloud Calculation Design



Evaluation

Security v.s. Flexibility

- This model secures the sensitive data by encrypting it in the private cloud before sending it to the public cloud and decrypting it only sections at a time
- In order to allow the program to accept the user's choice of encryption/decryption functions and applications, the encryption/decryption functions had to be separated from the application
- A more secure method could be created by more closely integrating the encryption/decryption processes into the application
- This approach sacrifices security for flexibility

Conclusion

- Hybrid clouds can be used to take advantage of the accessibility and resource allocation of a public cloud while enjoying the security of a private cloud when handling more sensitive data
- A secure method for performing calculations in a hybrid cloud appears to be feasible
- More secure methods can be created using known encryption/decryption functions and applications so they can be more closely integrated and create confusion for outside observers