A. G. M. RURAL COLLEGE OF ENGINEERING AND TECHNOLOGY, Varur
Approved By AICTE, New Delhi, Affiliated To VTU, Belagavi and Recognized by State Govt.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

2023-2024

Technical Seminar on

SECURITY PROTOCOL

Under the Guidance of

Dr. Channamma P

Presented By

Veena F Agadi [2AV20CS016]

SECURITY PROTOCOL

AGENDA

- Introduction
- Literature Rewiiew
- Design
- Implementation
- Conclusion

Title: “A Policy-based Interaction Protocol between Software Defined Security Controller and Virtual Security Functions”

Authors:

Sara Farahmandian
Department of Electrical and Data Engineering
University of Technology Sydney
Sydney, Australia
Email: Sara.Farahmandian@student.uts.edu.au

Doan B. Hoang
Department of Electrical and Data Engineering
University of Technology Sydney
Sydney, Australia
Email: Doan.Hoang@uts.edu.au

Date: 2020

INTRODUCTION

- This paper focuses on the Design and the Implementation of the Sec-Manage Protocol and Demonstrates its use in Setting, Monitoring and Conveying relevant Policy-Based Interaction Security Parameters.
- Here they Inroduced Software-Defined Security Service (SDS2) and Policy-based Interaction Model for Managiing, Detecting and Predicting Security Violations.
- A Virtual Security Functions (VSF) in our usage is created to perform specific Security functions and Deployed at Strategic Locations in the Cloud Infrastructure that Requires Protection.
- Software-Defined Networking (SDN) uses OpenFlow Protocol for Communication between the Network Controller and Switches.

- To Tackle Limitations over Security , in this paper they propose the Sec-Manage Protocol to Transfer Security Messages and Interaction Parameters between a Security Controller (SC) and its VSF.

- The Main Aims of Designing the Sec-Manage Protocol are

1. To Provide Direct Communication between the SDS2 Security Controller and its VSF
2. To Transfer the Parameters to the Security aspects of objects Interaction between a VSF and the SC to Monitor Parameters of an Interaction to Detect Predict Security Violations.

LITERATURE REVIEW

- Various southbound protocols have been proposed for networking, including OpenFlow, NETCONF, SNMP, OVSDB, ForCES, and S-manage protocol.
- While OpenFlow focuses on networking management between controllers and switches, Sec-Manage protocol specializes in managing security functions.
- ForCES decouples control and data planes using Logical Function Blocks, though it's not widely deployed.
- SNMP and NETCONF offer network management but lack agility for dynamic security networks.
- Sec-Manage protocol, designed for SD-IoT controllers, addresses challenges by configuring virtual security functions based on a policy-based model, simplifying security network management.

DESIGN

- The Security Architecture Consist of Three Main Components

1. Security Controller (SC)
2. Virtual Security Functions (VSF)
3. Sec-Manage Protocol

SOFTWARE-DEFINED SECURITY SERVICE (SDS 2) AND INTERACTION MODEL

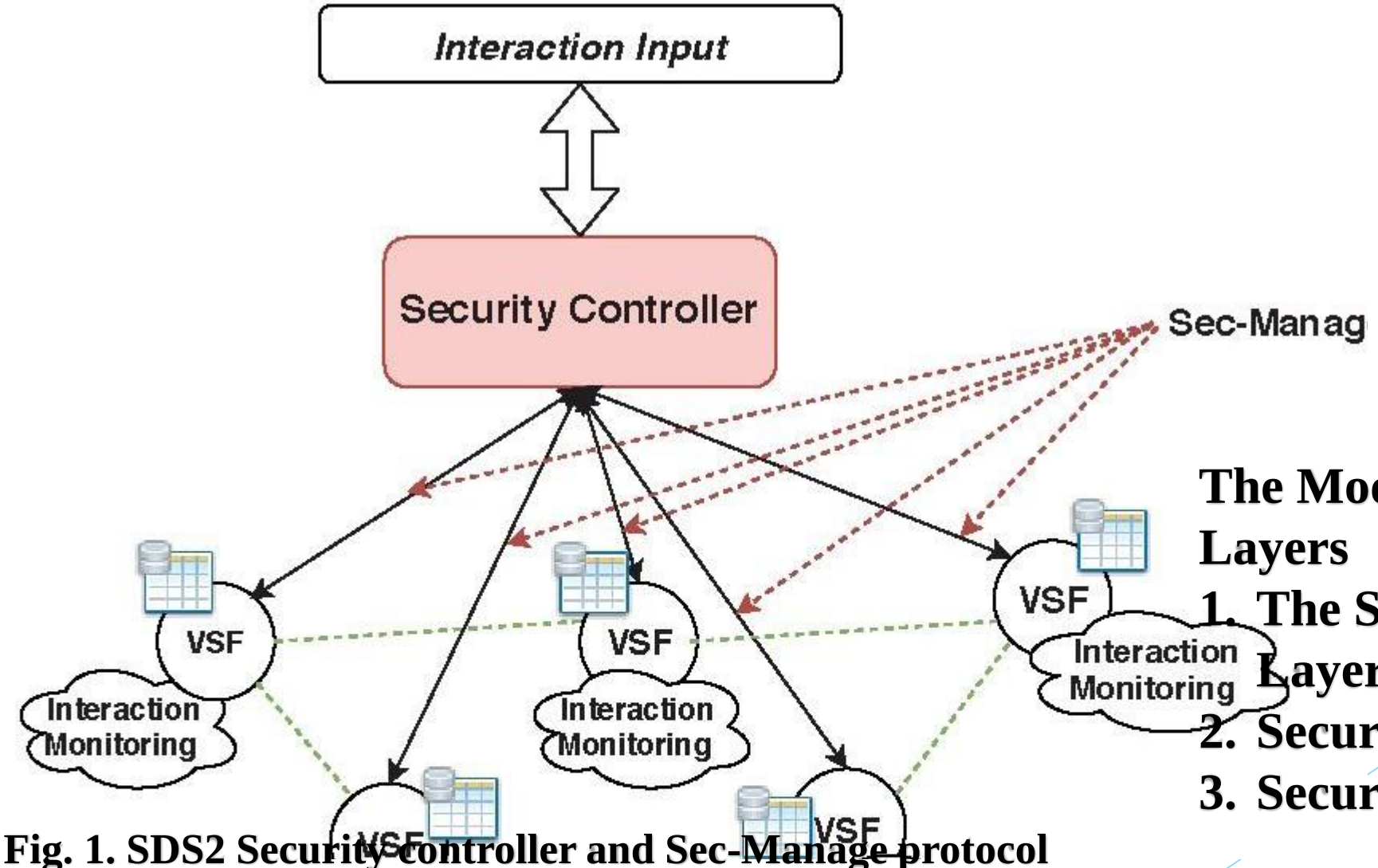

Fig. 1. SDS2 Security controller and Sec-Manage protocol

The Model Structured in 3 Layers

1. **The Security Application Layer**
2. **Security Control Layer**
3. **Security Data Layer**

SEC-MANAGE PROTOCOL DESIGN

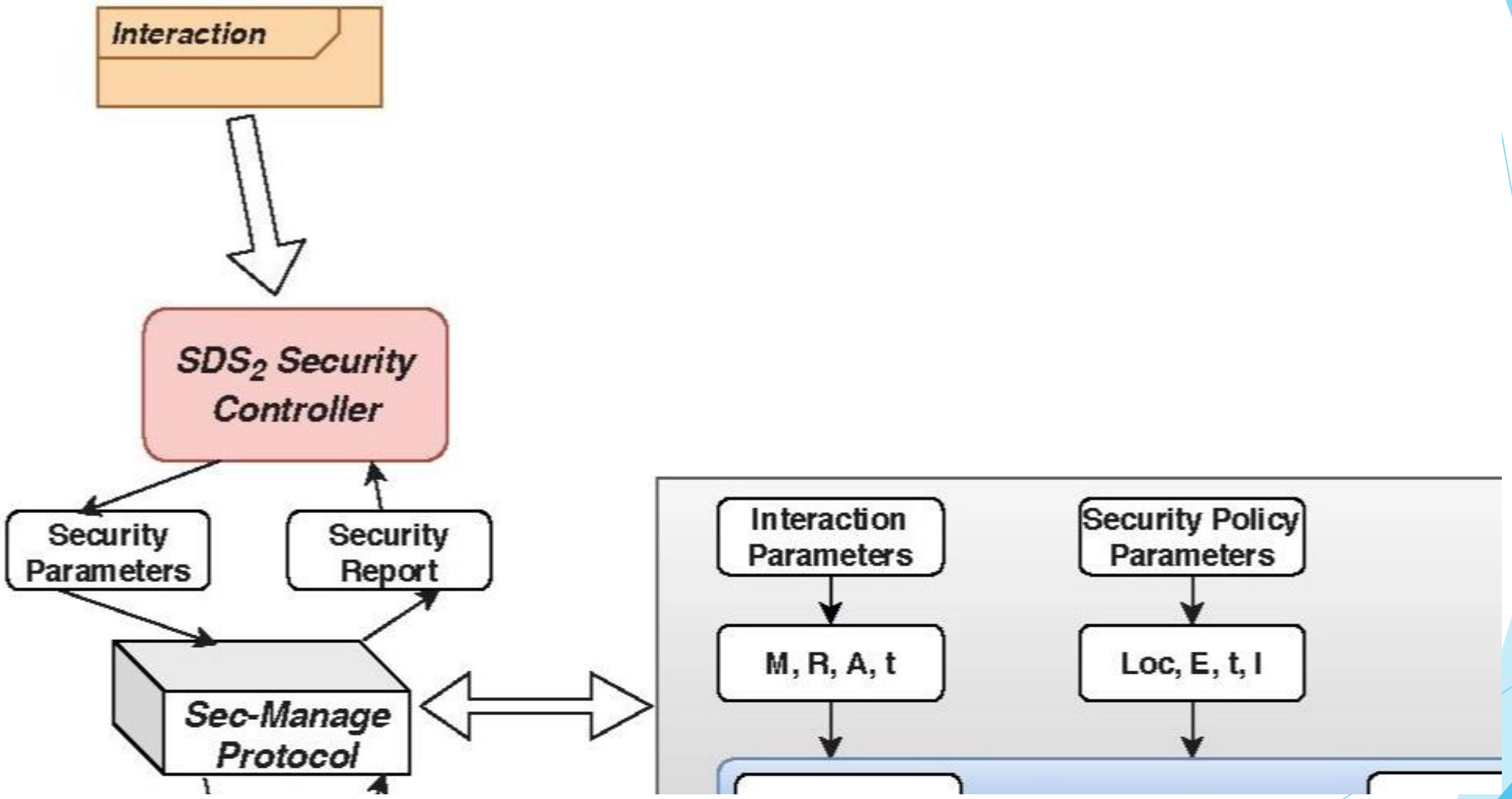

Fig. 2. Interaction and Sec-Manage Protocol

Connection Establishment

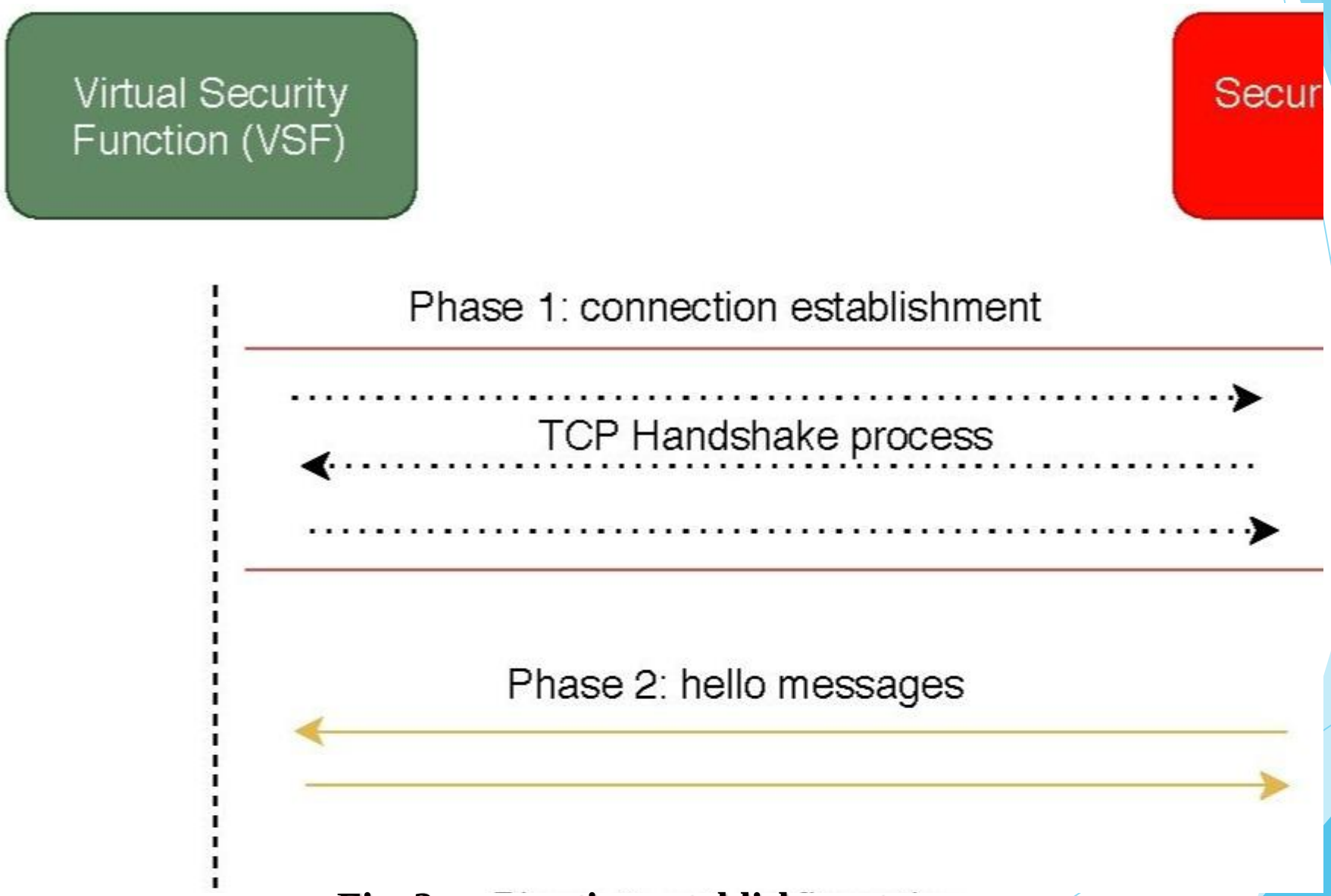

Fig. 3. connection establishment

Sec-Manage Header and payload

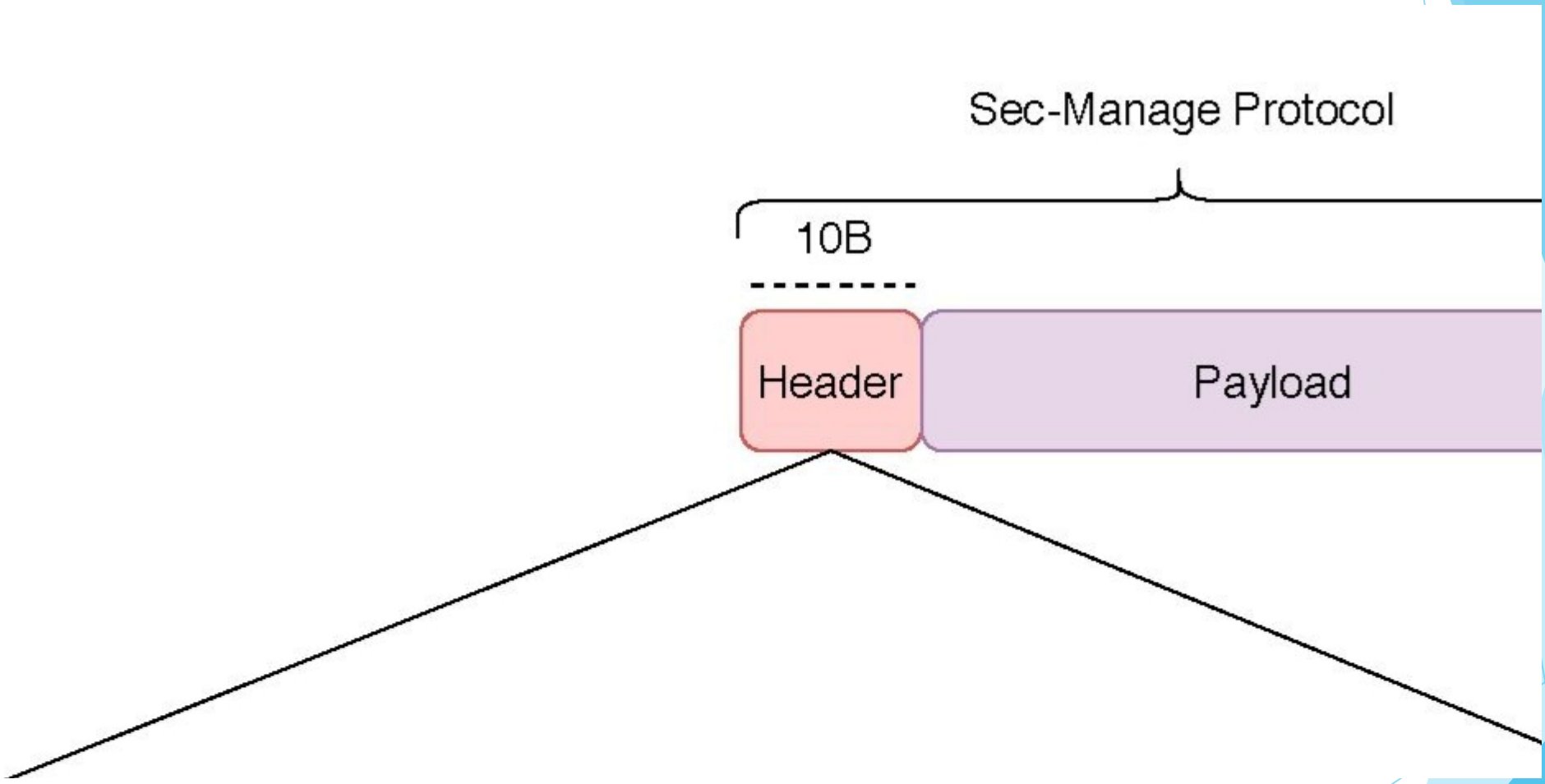

Fig. 4. Sec-Manage Header and payload

IMPLEMENTATION

The implementation of the prototype

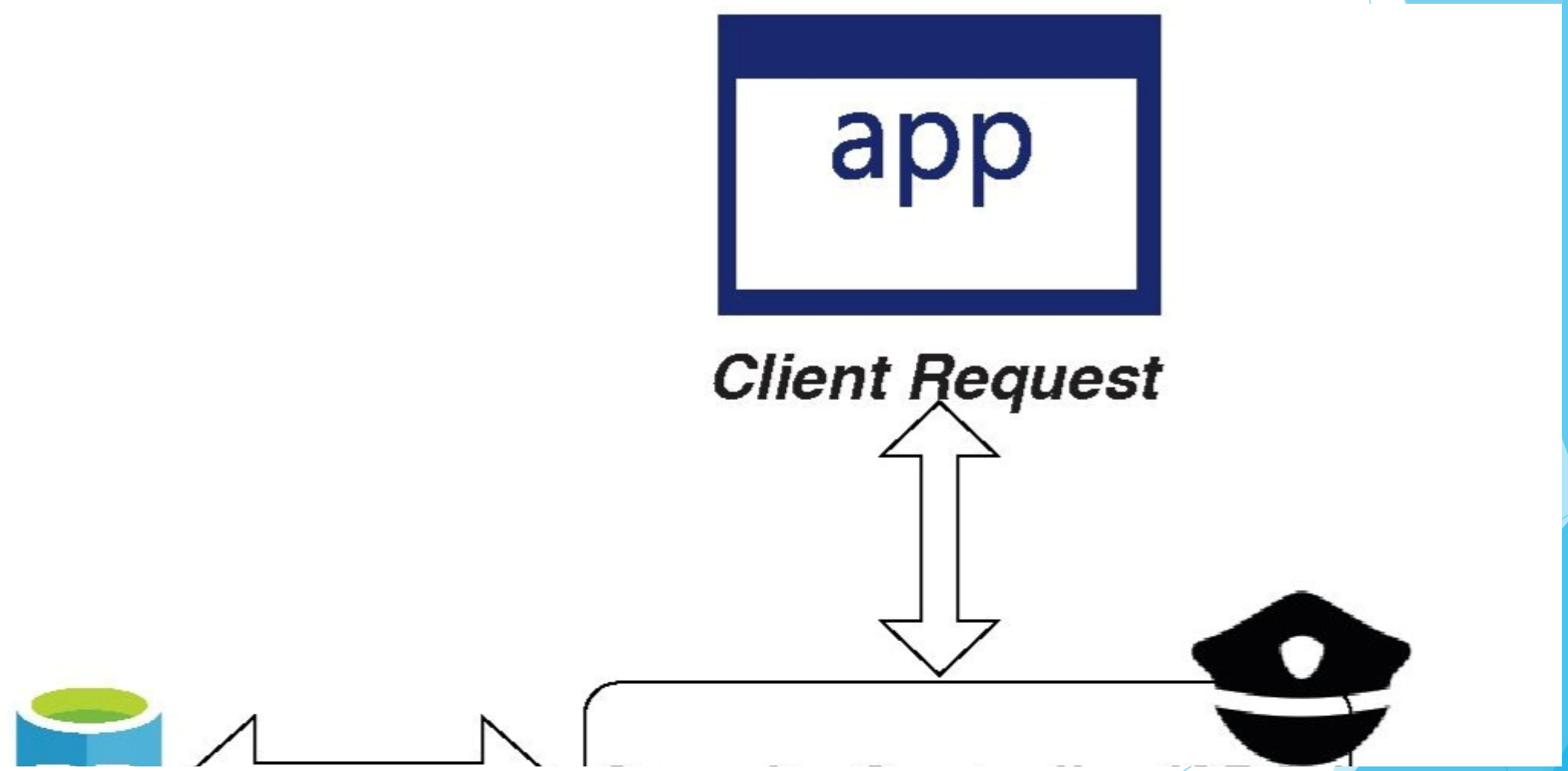

Fig. 5. The implementation of the prototype

Client sending request to the security controller

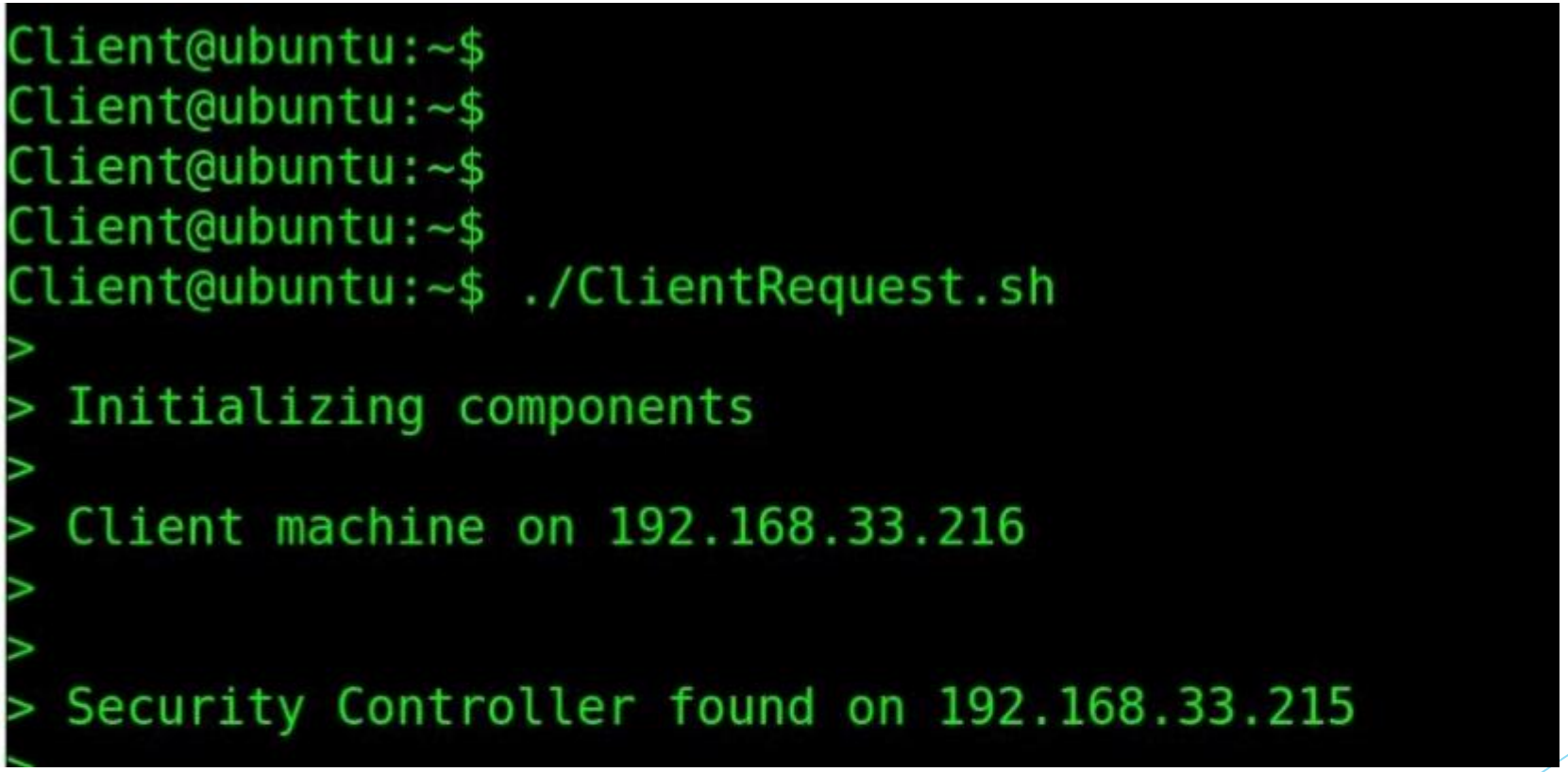

Fig. 6. Client sending request to the security controller

CONCLUSION

- **The Sec-Manage protocol addresses the challenge of efficient communication between Security Controller (SC) and Virtual Security Functions (VSFs) for security violation detection and prediction.**
- **Operating on a policy-based interaction model, it enables dynamic VSF control, paving the way for enhanced security management in cloud systems and future research in virtual security function orchestration**

References

- [1] R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," Computer Science Review, vol. 33, pp. 1-48, 2019.
- [2] S. Farahmandian and D. B. Hoang, "Sds 2: A novel software-defined security service for protecting cloud computing infrastructure," in 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA). IEEE, 2017, pp. 1-8.
- [3] D. B. Hoang and S. Farahmandian, "Security of software-defined infrastructures with SDN, NFV, and cloud computing technologies," in Guide to Security in SDN and NFV. Springer, 2017, pp. 3-32.
- [4] O. S. Specification, "Version 1.5.1, standard, open networking foundation. 2015," 2017.
- [5] A. Doria, J. H. Salim, R. Haas, H. M. Khosravi, W. Wang, L. Dong, R. Gopal, and J. M. Halpern, "Forwarding and control element separation (forces) protocol specification." RFC, vol. 5810, pp. 1-124, 2010.

Thank You