IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305016 |

A Secure Communication Protocols in a Cloud Computing

P. Chenchu Sasank, CH. Eswar Chandra Vidya Sagar, Dr. A. Vijay Kumar

U.G. Student, Department of Computer Science & Engineering, Jain (Deemed-to-be University), Bangalore, India

U.G. Student, Department of Computer Science & Engineering, Jain (Deemed-to-be University), Bangalore, India

Associate Professor, Department of Computer Science & Engineering, Jain (Deemed-to-be University), Bangalore, India

ABSTRACT: Secure Communication in Cloud computing environment is a billion dollar question now a days. Yes, there are protocols to support communication in the Cloud but these are not secure enough to communicate. A detailed study over the existing protocols is done to check whether they are secured or not. Unfortunately, result is no. Since there is an emerging need to have a more secure communication protocol for the cloud, started working on developing a Robust communication protocol with zero vulnerabilities to exploit the communication.

KEYWORDS: Cloud Computing, Vulnerability, Exploitation, Communication protocol, Secure Communication.

I. INTRODUCTION

In the rapidly advancing era of cloud computing, the efficiency and security of communication protocols stand as pivotal components in the seamless functioning of digital ecosystems. As organizations increasingly entrust their operations to cloud environments, the paramount need for robust and secure communication protocols becomes evident. This major project addresses the critical intersection of cloud computing and communication security, acknowledging the prevailing challenges in existing protocols.

While various communication protocols facilitate the exchange of information within cloud infrastructures, their ability to withstand sophisticated security threats is a growing concern. The susceptibility of these protocols to vulnerabilities raises questions about the confidentiality, integrity, and accessibility of transmitted data. This project stems from the imperative recognition that the current state of communication protocols within cloud computing may not adequately meet the stringent security standards demanded by modern digital landscapes.

A meticulous exploration of existing communication protocols forms the foundation of this research. The primary objective is to assess the security posture of prevalent protocols, identifying potential vulnerabilities and weaknesses. The outcomes of this assessment affirm the necessity for a paradigm shift, as current protocols reveal vulnerabilities that may expose critical information to exploitation.

Motivated by these findings, this major project is embarked upon with the ambitious goal of designing and implementing a cutting-edge, secure communication protocol tailored explicitly for the cloud environment. This novel protocol endeavors to address the identified vulnerabilities comprehensively, providing an impervious framework for secure data transmission. The project places particular emphasis on fortifying user privacy, protecting sensitive information, and mitigating emerging cyber threats within the dynamic realm of cloud computing.

As we delve into the intricacies of cloud communication, this research not only aims to fill existing security gaps but also aspires to set new standards for secure communication protocols. By contributing to the evolving discourse on secure cloud computing, this major project seeks to offer practical solutions that elevate the security and reliability of communication protocols in the contemporary digital landscape.

In our investigation of various protocols, we have selected the Secure Shell Protocol and Internet Group Management Protocol (IGMP) as focal points. Recognizing the significance of these protocols in secure communication within cloud computing environments, we aim to innovate and create a distinct protocol that builds upon the strengths of Secure Shell and IGMP.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305016 |

The intention is to develop a specialized communication protocol tailored to meet the specific needs and challenges posed by the dynamic nature of cloud computing. This initiative involves the integration of advanced security features, efficient data transmission mechanisms, and compatibility with modern cloud infrastructures. By creating a dedicated protocol derived from Secure Shell and IGMP, we strive to contribute to the evolution of secure communication protocols in the context of cloud computing, setting new standards for reliability and security.

1.1 **OBJECTIVES**

To Develop a more Secured Communication Protocol for Cloud Computing.

II. LITERATURE SURVEY

Protocol	Gossip Protocol
Author	Demers et al. (1987)
Advantages	- Robustness: Able to withstand node failures and network partitions - Scalability: Can handle large numbers of nodes - Fault Tolerance: Resilient to faults and failures
Disadvantages	- Inconsistency: Challenges in ensuring all nodes converge to the same information - Convergence Speed: Speed at which all nodes agree on the information can be slow
Proposed Work	- Models like Epidemic: Introducing variations to improve convergence speed - HyParView: Hybrid approach for scalability and consistency

Protocol	Media Transfer Protocol
Author	Zeldovich et al. (2005)
Advantages	- Efficient Media Transfer: Facilitates seamless transfer of multimedia content - Potential Latency Reduction: Enables faster transfer of media files
Disadvantages	- Security Concerns: Vulnerable to interception and tampering - Potential Latency: Transfer times may be affected by network congestion
Proposed Work	- Incorporating Encryption: Enhancing security through encryption mechanisms - Latency Optimization: Techniques to minimize transfer delays

Protocol	Connectionless Network Protocol
Author	Tanenbaum and Wetherall (2011)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305016 |

Advantages	- Speed: Fast transmission of data packets without connection setup overhead - Simplicity: Minimal protocol overhead and complexity
Disadvantages	- Lack of Reliability: No guarantee of packet delivery or order - Congestion Control: Inability to manage network congestion efficiently
Proposed Work	- Models like QUIC: Incorporating reliability features while preserving speed - Congestion Control Mechanisms: Strategies to manage network congestion

Protocol	Coverage Enhanced Ethernet Protocol
Author	Gupta et al. (2012)
Advantages	- Extended Network Coverage: Enhances reachability in large-scale network deployments - Potential Reliability Improvements: Reduced packet loss and increased network stability
Disadvantages	- Increased Complexity: Introduction of additional protocols and mechanisms may complicate network management - Energy Consumption: Enhanced coverage may lead to higher energy consumption by devices
Proposed Work	- Energy Efficiency Optimization: Developing techniques to reduce energy consumption in extended networks - Reliability Enhancement: Improving protocol robustness to reduce packet loss and enhance stability

Protocol	State Routing Protocols
Author	Perkins and Bhagwat (1994)
Advantages	- Adaptability: Ability to dynamically adjust routing based on network conditions and topology - Potential Overhead Reduction: Efficient use of network resources through on-demand routing
Disadvantages	- Potential Overhead: Exchange of routing information may lead to increased network traffic - Reliability: Dependency on accurate network state information may introduce vulnerabilities
Proposed Work	- Models like Dynamic Source Routing (DSR): Introducing reactive routing for reduced

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305016 |

	overhead - Scalability and Reliability Enhancements: Techniques to improve scalability and reliability of state routing protocols

Protocol	Secure Shell Protocol (SSH)
Author	Ylonen and Lonvick (2006)
Advantages	- Robust Security: Provides encrypted communication and authentication for secure remote access - Flexibility: Supports various authentication methods and cryptographic algorithms
Disadvantages	- Potential Vulnerabilities: Susceptible to security exploits and weaknesses in encryption algorithms - Continuous Updates: Requires frequent updates to address emerging security threats
Proposed Work	- Key Management Enhancements: Strengthening key management practices for improved security - Authentication Improvements: Enhancing authentication mechanisms to mitigate vulnerabilities

Protocol	Internet Group Management Protocol
Author	Deering et al. (1999)
Advantages	- Scalable Multicast: Efficiently manages group communication for scalable multicast applications - Compatibility: Standardized protocol supported by various network devices and platforms
Disadvantages	- Potential Security Vulnerabilities: Lack of authentication mechanisms may lead to unauthorized access - Protocol Overhead: Introduction of additional control messages may increase network overhead
Proposed Work	- Secure Variations: Introducing secure extensions or variants to mitigate security risks - Overhead Reduction: Optimizing protocol overhead to minimize impact on network performance

III. CONCLUSION

In the Present Research we made a Secured genetic attempt to avoid a more robust IGMP Protocol with Data Confidentiality and Data Authentication features. The developed Protocol found to be secured against impersonation

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305016 |

attack and Data Reveal Attacks still the IGMP Protocol is having which we would like to fix in some Limitations in Future.

IV. FUTURE SCOPE

Quantum-Resistant Encryption:- Our project is dedicated to developing a robust encryption method, similar to a secret language, to protect our data from potential threats posed by powerful quantum computers. This quantum-resistant encryption functions like an unbreakable code, ensuring the security of our data and maintaining the confidentiality of sensitive information.

REFERENCES

[1] Birman, K. (2007). The promise, and limitations, of gossip protocols. ACM SIGOPS Operating Systems Review, 41(5), 8-13.
[2] Kwiatkowska, M., Norman, G., & Parker, D. (2008). Analysis of a gossip protocol in PRISM. ACM SIGMETRICS Performance Evaluation Review, 36(3), 17-22.
[3] Jenkins, K., Hopkinson, K., & Birman, K. (2001, April). A gossip protocol for subgroup multicast. In Proceedings 21st International Conference on Distributed Computing Systems Workshops (pp. 25-30). IEEE.
[4] Clausen, T., Hansen, G., Christensen, L., & Behrmann, G. (2001, September). The optimized link state routing protocol, evaluation through experiments and simulation. In IEEE symposium on wireless personal mobile communications (Vol. 12). Denmark: Aalborg.
[5] Jacquet, P., Muhlethaler, P., Clausen, T., Laouiti, A., Qayyum, A., & Viennot, L. (2001, December). Optimized link state routing protocol for ad hoc networks. In Proceedings. IEEE International Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. (pp. 62-68). IEEE.
[6] Hoque, A. M., Amin, S. O., Alyyan, A., Zhang, B., Zhang, L., & Wang, L. (2013, August). NLSR: Named-data link state routing protocol. In Proceedings of the 3rd ACM SIGCOMM workshop on Information-centric networking (pp. 15-20).
[7] Papadimitratos, P., & Haas, Z. J. (2003, January). Secure link state routing for mobile ad hoc networks. In 2003 Symposium on Applications and the Internet Workshops, 2003. Proceedings. (pp. 379-383). IEEE.
[8] Islam, S., & Atwood, J. W. (2006, November). The internet group management protocol with access control (IGMP-AC). In Proceedings. 2006 31st IEEE Conference on Local Computer Networks (pp. 475-482). IEEE.
[9] Judge, P., & Ammar, M. (2003). Security issues and solutions in multicast content distribution: A survey. IEEE network, 17(1), 30-36.
[10] Baltatu, M., Lioy, A., Maino, F., & Mazzocchi, D. (2000). Security issues in control, management and routing protocols. Computer Networks, 34(6), 881-894.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details