Pertanika J. Sci. & Technol. 32 (1): 31 - 44 (2024)

PERTANIKA
JOURNALS

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

Towards Maximising Hardware Resources and Design Efficiency via High-Speed Implementation of HMAC based on SHA-256 Design

Shamsiah Suhaili*, Norhuzaimin Julai, Rohana Sapawi and Nordiana Rajaee

Department of Electrical and Electronic Engineering, Faculty of Engineering, Universiti Malaysia Sarawak, 94300 UNIMAS, Kota Samarahan, Sarawak, Malaysia

ABSTRACT

Some applications, such as Message Authentication Code (MAC), rely on different hashing operations. There are various hash functions, including Message-Digest 5 (MD5), RACE Integrity Primitives Evaluation Message Digest 160 (RIPEMD-160), Secure Hash Algorithm 1 (SHA-1), and Secure Hash Algorithm 256 (SHA-256), among others. The network layer is the third of seven layers of the Open Systems Interconnection (OSI) concept, also known as the Internet. It handles network addressing and physical data routing. Nowadays, enhanced internet security is necessary to safeguard networks from illegal surveillance. As a result, Internet Protocol Security (IPsec) introduces secure communication across the Internet by encrypting and/or authenticating network traffic at the IP level. IPsec is an internet-based security protocol. Encapsulating Security Payload (ESP) and Authentication Header (AH) protocols are separated into two protocols. The MAC value is stored in the authentication data files of the Authentication Header and Encapsulating Security Payload. This article analyses a fast implementation of the Hash-based Message Authentication Code (HMAC), which uses its algorithm to ensure the validity and integrity of data to optimise hardware efficiency and design efficacy using the SHA-256 algorithm. During data transfer, HMAC is critical for message authentication. It was successfully developed using Verilog Hardware Description Language (HDL) code with the implementation of a Field Programmable Gate Array (FPGA) device using the Altera Quartus II Computer-Aided Design (CAD) tool to enhance the maximum frequency of the design. The accuracy of the HMAC design, which is based on the SHA-256 design, was examined and confirmed

ARTICLE INFO

Article history:
Received: 04 November 2022
Accepted: 10 May 2023
Published: 06 November 2023

DOI: https://doi.org/10.47836/pjst.32.1.02

E-mail addresses:
sushamsiah@unimas.my (Shamsiah Suhaili)
jnorhuza@unimas.my (Norhuzaimin Julai)
srohana@unimas.my (Rohana Sapawi)
rnordiana@unimas.my (Nordiana Rajaee)
* Corresponding author

ISSN: 0128-7680
e-ISSN: 2231-8526

using ModelSim. The results indicate that the maximum frequency of the HMAC-SHA-256 design is approximately 195.16 MHz.

Keywords: Field Programmable Gate Array, hash function, Hash-based Message Authentication Code, Secure Hash Algorithm 256, Verilog Hardware Description Language

INTRODUCTION

There are seven layers, and the internet layer is the network layer in which data transfer from one terminal to another depends on the address and routing network. Traffic networks are prone to eavesdropping and illegal access without a network-integrated security element. However, selecting a suitable encryption and authentication product for the network can solve this problem. The internet community created the Security Protocol (Randall, 1999). The third network layer of the seven-layer OSI architecture employs the IPsec protocol. The seven layers are divided into application, presentation, session, transport, network, data link, and physical layers. One of the network encryption protocols is IPsec (IP Security), the most recent IP-based technology.

The IP provides network authentication and encryption to protect the network from illegal surveillance. Because of its improved capabilities, IP Security has become a fact of life in terms of network security for Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). The IPsec is divided into two protocols: Authentication Header (AH), which examines IP packet authentication and data integrity, and Encapsulating Security Payload (ESP), which encrypts and authenticates the message. Both AH and ESP are equipped with two different modes: tunnel mode and transit mode; as a whole, the IP packet is encrypted in tunnel mode, while only the transport layer is encrypted in the latter. On the other hand, HMAC-MD5, HMAC-SHA, and HMAC-RIPEMD160 are authentication and data integrity methods. These methods may be used to safeguard all distributed applications, e-mail, file transfers, and web access.

This article focuses on computing the Hash-based Message Authentication Code (HMAC) using the MAC (Message Authentication Code) algorithm. Message Authentication Code (MAC) is used to verify the validity of a message, while HMAC is a subset of MAC that uses a cryptographic hash function and a private key for verification. It accepts arbitrary input with a specified key and produces MAC output. The authentication data element in the AH header contains this MAC value. Network transmission operations are followed using the same key to obtain the same MAC at the destination. The message is valid if the MAC value received at the destination corresponds to the one broadcasted. Similar to AH, ESP enables the use of MAC with HMAC. The encryption procedure takes place before the IP layer, which is at the IPsec layer when the application sends the message across the network. A message is routed via the network to its destination using an IP address, part of an IP layer. The router will then determine