International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 04 | Apr 2025 www.irjet.net p-ISSN: 2395-0072

ADVANCING CRYPTOGRAPHIC TECHNIQUE USING HASH BASED MESSAGE AUTHENTICATION CODE IN NETWORK ANALYSIS

V. Pavani[1], K. Rishitha[2], G. Navaneetha[3], Dr. D. Sreenivasulu[4]

[1]B-Tech 4th year, Dept. CSE(DS), Institute of Aeronautical Engineering
[2]B-Tech 4th year, Dept. CSE(DS), Institute of Aeronautical Engineering
[3]B-Tech 4th year, Dept. CSE(DS), Institute of Aeronautical Engineering
[4]Associate Professor, Dept. CSE(DS), Institute of Aeronautical Engineering, Telangana, India

---

Abstract – *In the modern world, information protection and maintenance are vital, and they should receive a lot of attention due to the rapid development of Information and Communication Technologies and the vulnerabilities endangering human societies. The Secure Hashed Identity Message Authentication (SHIMA) generates fixed length outputs, leading to potential collisions where distinct messages produces the same hash value, compromising integrity. To resolve these issues, we propose a HMAC (Hash-based Message Authentication Code) in network security which helps to verify the authenticity and integrity of data or a message transmitted between two parties. In cryptography using Hash-Based Message Authentication Code (HMAC), we can ensure the authenticity of a message. The entitled HMAC which enhance and improve the cryptographic characteristics of SHIMA. The improved algorithm offers a greater resistance to birthday attacks.*

Key Words: **Cryptography, Hash Based Message Authentication Code (HMAC), Network Security, Message Integrity, Authentication, Secure Communication**

1. INTRODUCTION

In the modern digital age, the integrity and authenticity of data transmitted over network are paramount. As data flows across various nodes in a network, it is susceptible to interception, alteration, and unauthorized access. Ensuring the security of this data is a critical challenge for network administrators and cybersecurity professionals. One of the robust solutions to this challenge is to use the Hash-Based Message Authentication Code (HMAC).

A popular cryptographic method called Hash-Based Message Authentication Code (HMAC) is used to confirm a message's authenticity and data integrity. This is accomplished by mixing the message contents with a secret cryptographic key, which is subsequently processed using a cryptographic hash function. The output that is produced, called the message authentication code (MAC), is specific to thekeyand message, thus any changes made to the data will result in a different MAC.

1.1 The Role of HMAC in Network Security:

The primary purpose of HMAC in network security is to provide a means for verifying that data has not been tampered during transmission and that it originates from a trustedsource. This is crucial in preventing various types of cyberattacks.

HMAC is employed in numerous network protocols to secure data transmission. For instance, in SSL/TLS, which underpins secure web communications, HMAC ensures the authenticity and integrity of data exchanged between web browsers and servers. Similarly, in IPsec, HMAC is used to secure internet protocol communications by verifying that the data packets have not been tampered with and that they come from a legitimate source. SSH, used for secure remote logins, also relies on HMAC to protect the authenticity and integrity of the transmitted data.

1.2 Advancements in HMAC and Cryptographic Security:

Inside As cybersecurity threats continue to evolve, so too must the mechanisms designed to counter them. Recent advancements in HMAC and cryptographic security aim to enhance the robustness, efficiency, and adaptability of these techniques in the face of emerging challenges. Enhancing the security, effectiveness, and suitability of these algorithms to counter new threats in contemporary network environments has been the main goal of developments in hash-based message authentication code (HMAC) and cryptographic security.

Enhanced Key Management: Good key management is essential to HMAC security. Modern key management techniques, like secure key distribution systems and automated key rotation, reduce the possibility of key compromise. Additional layers of security for cryptographic keys are offered by methods like secure enclaves and

hardware security modules. Hardware Security Modules (HSMs) offer scalable solutions for enterprise use and tamper-proof key storage environments. Secure, centralized key handling in cloud environments is made possible by cloud-based key management services (KMS), whereas hybrid solutions handle keys across on- premises and cloud infrastructures. In complicated systems, interoperability is guaranteed by standardized protocols such as KMIP.

Integration with Emerging Technologies: Integration with Emerging Technologies: HMAC integration is crucial for preserving security in systems that use new protocols and technologies. For instance, the extensive network of connected devices can safely transmit and authenticate data thanks to the use of HMAC in Internet of Things (IoT) devices and protocols. HMAC ensures data authenticity in resource-constrained contexts by securing device communications in the Internet of Things. It strengthens ledger integrity by securing node interactions and authenticating transactions on blockchain. HMAC safeguards data both in transit and at rest, which is essential for multi-tenant designs in cloud computing.

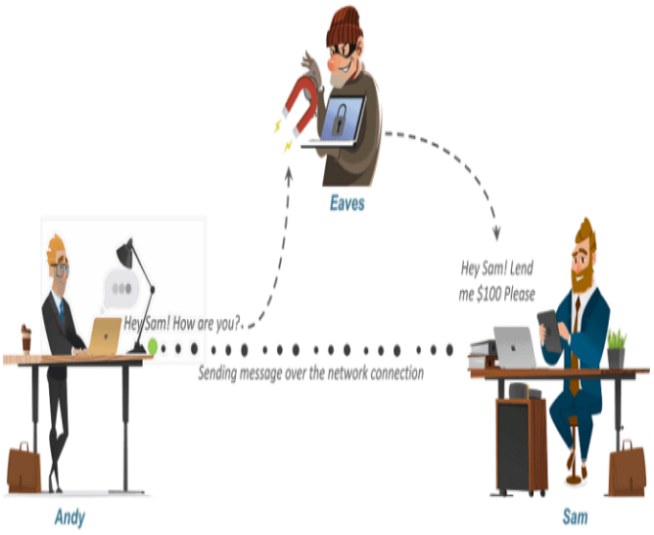

Fig -1: Cryptography Diagram

2. LITERATURE REVIEW

Hash Based Message Authentication Code (HMAC) a cryptographic technique is used to confirm the authenticity and integrity of data. It prevents unauthorized alterations and message manipulation by combining a cryptographic hash function with a secret key. In order to handle changing security issues, research is also concentrated on hybrid models and lightweight IoT implementations. [1] In an effort to address the issues, we suggest Secure Hashed Identity Message Authentication, which helps to confirm the message's authenticity and integrity. Re-encryption due to network security is predicted to be quite expensive. The SHIMA technique decreases end-user control overthedevice's end-to-end encryption and decryption. Studies on security and performance have been finished, and the findings indicate that our approach is more effective and efficient, lasts longer, and lowers latency. [3] Ad hoc networks are wireless networks which doesn't have permanent infrastructure that are typically put together sometimes to carry out certain tasks like combat communications or emergency rescue. [8] The general purpose of attack in MANETs is to fail the first time to send packets or to modify messages that do not match, causing nodes to pass the wrong packets, thus depleting them. > Node the battery. [11] It does this by using the Statistical Uniqueness and Cryptographic Verifiability (SUCV) property of some entities; this information refers to the SUCV identifier and address or the Encrypted code. Its properties allow them to prevent certain types of denial of service attacks and hijacking attacks. Sex problem finding Optimization (CSA) algorithm. Among them, data encryption and key symbols are made using the RSA encryption system to protect data from unauthorized users. The CSA algorithm helps in optimizing the encryption key to avoid brute force attacks.[17] The algorithm uses a lightweight implicit certificate and combines public and private keys to create temporary session keys, thus encrypting and protecting data transfer and solving the problem of security data transfer. cooperating nodes when entering. The solution is not easy, but the key finding solution both has more indexing overhead and has disadvantages.

3. MATERIALS AND METHODS

Hash-based Message Authentication Code is a popular cryptographic algorithm that makes sure data is legitimate and intact while being transferred across networks. It has to do with the use of a hash function in cryptography combined with a secret key to produce an authentication message. This approach enhances security by ensuring that each HMAC is unique to its specific context, making it significantly more resistant to replay and prediction attacks. The dynamic elements introduce variability, so even if an attacker intercepts multiple HMAC values, they cannot easily anticipate future ones. HMAC is widely used in secure communication protocols like TLS and IPsec, as well as in API authentication, due to its flexibility with different hash

functions, efficiency, and well- understood security properties. However, effective key management is crucial to maintaining its security.

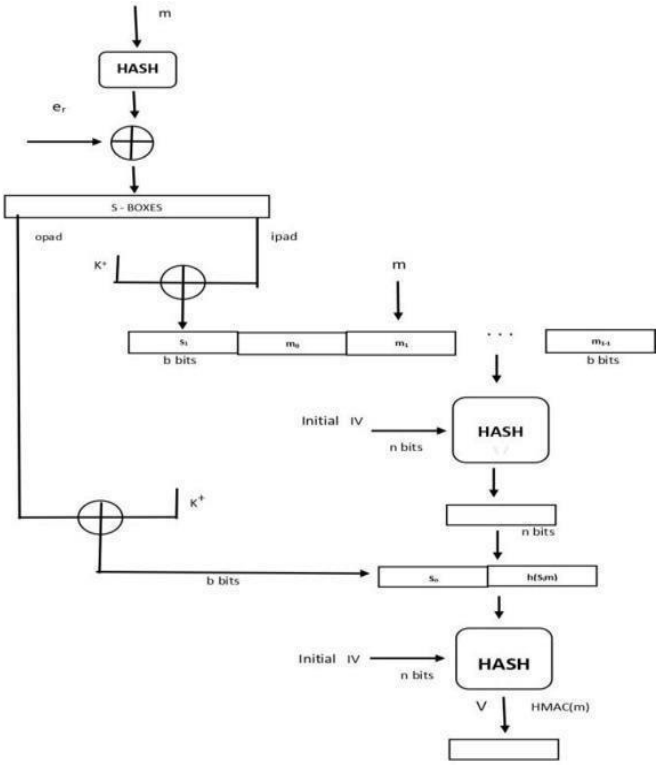

Fig -2: Flow chart of Proposed Technique

A. Input:
A cryptographic hash function HHH.
A secret key KKK.
The message MMM to be authenticated.

B. Key length adjustments:
If the key length is greater than the block size (B):
Hash the key using the hash function to reduce its length to the hash function's output length (L).
If the key length is less than the block size (B): Pad the key with zeros to make it equal to the block size.

C. Preparation:
Two fixed-size pads are defined:
Inner pad (ipad): A string of the block size, each byte is the XOR of the key byte and the byte 0x36.
Outer pad (opad): A string of the block size, each byte is the XOR of the key byte and the byte 0x5c.

D. Padding the key:
Inner Padding (K_ipad): XOR the adjusted key with the inner pad constant (0x36 repeated B times).
Outer Padding (K_opad): XOR the adjusted key with the outer pad constant (0x5c repeated B times).

E. Computing the inner hash:
Concatenate the original message (M) with K_ipad. To generate the inner hash value, hash the concatenated value using the selected hash function

F. Computing the outer hash:
Concatenate the inner hash value with K_opad. The final HMAC value is obtained by hashing the concatenated value using the hash algorithm.

G. Output:
The result is the HMAC value, which offers authenticity and data integrity.

4. SECURITY AND PERFORMANCE

4.1 Security Analysis

Extensive security analyses have been conducted on HMAC since its introduction. Bellare, Canetti, and Krawczyk's original work provided foundational proofs that established HMAC's resistance to collision attacks and length extension attacks. Subsequent research has reinforced these findings, showing that HMAC maintains its security properties when used with various hash functions. However, due to known vulnerabilities in MD5 and SHA-1, SHA-256 and other members of the SHA-2 and SHA-3 families are preferred for modern applications

4.2 Performance Considerations

The performance of HMAC has been a subject of significant research, particularly in the context of its efficiency in different environments. Krawczyk's work, along with other studies, has shown that HMAC is computationally efficient and suitable for both software and hardware implementations. Performance tests in contexts with limited resources, such Internet of Things (IoT) devices, show that even while HMAC adds some computing overhead, it is still practical for secure communication. Utilizing parallel processing capabilities and other methods to improve speed, research has been concentrated on optimizing HMAC for particular hardware architectures.
With strong security features that overcome the drawbacks of basic hash-based message authentication methods, HMAC has made a name for itself as a key tool in the field of cryptography. It is a commonly used solution in many security protocols and applications due to its theoretical soundness, demonstrated security, and practical effectiveness. HMAC's performance and applicability are being improved by ongoing research, guaranteeing its relevance in the rapidly changing field of cryptographic security. HMAC's resilience and adaptability will remain crucial components of its ongoing importance as new threat materialize and computational capabilities develop.

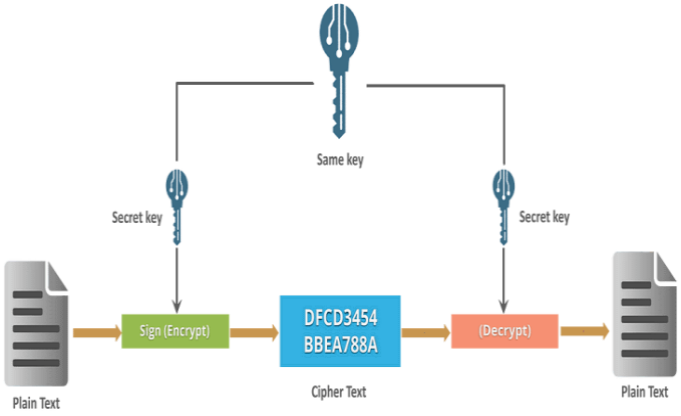

Fig -3: Transmission of Message

5. RESULTS AND DISCUSSION

The result of implementing the dynamic HMAC algorithm is a highly secureandcontext- specific messageauthentication code that ensures the integrity and authenticity of transmitted data. By incorporating dynamic elements such as timestamps, or session- specific data, each generated HMAC is unique and resistant to replay attacks and prediction. This results in robust protection against unauthorized alterations and ensures that the sender's identity can be reliably verified. HMAC significantly strengthens the security of communication protocols, providing a reliable method for safeguarding sensitive information in different applications, including financial transactions, communications, and data transfer processes.

5.1 Time Complexity

By implementing HMAC encryption technology on the network, additional data possibilities are created. The suggested method's complexity is decreased by comparing it to earlier approaches.

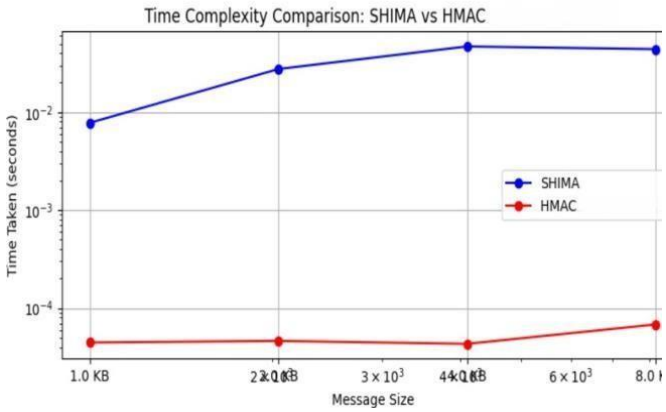

Chart -1: Time Complexity of SHIMA vs HMAC

5.2 Storage Cost

In the below graph x-axis represents proposed and existing algorithm names and y-axis represents 'Storage Cost' and in these both techniques HMAC got less storage when compared to SHIMA algorithm.

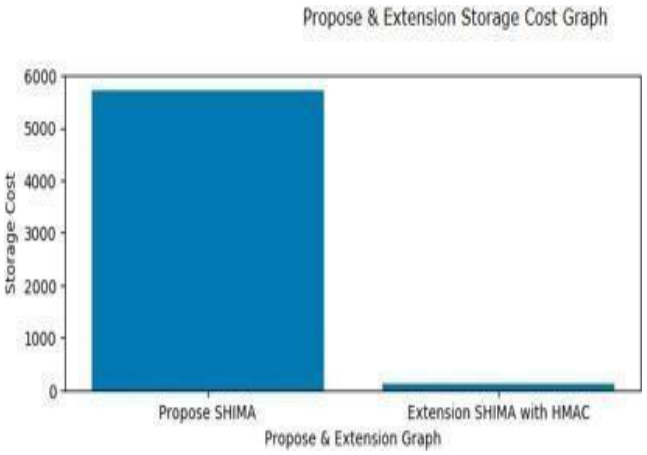

Chart -2: Storage cost of SHIMA vs HMAC

6. CONCLUSIONS

In conclusion, HMAC represents a significant advancement in cryptographic security by integrating changing elements like timestamps or session-specific data into the HMAC generation process. This integration ensures each HMAC is unique to its context, providing strong protection against replay and prediction attacks. The enhanced security of HMAC makes it particularly suitable for safeguarding sensitive data, securing financial transactions, and ensuring the integrity and authenticity of communications in various high-security applications. By adapting to the dynamic aspects of its environment, HMAC offers a robust and reliable method for maintaining data integrity and authentication in an increasingly complex digital landscape.

REFERENCES

[1] Sakshi Pandey, Saurabh Lahoti, "Cryptography based Network Security Analysis using Secure Hashed Identity Message Authentication ", April 2023.

[2] Y. Zhang, W. Lee, and Y. Huang, —Intrusion Detection Techniques for Mobile Wireless Networks‖, ACM Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.

[3] S. Al-Otaibi S, F. Siewe, "Secure Routing Protocol Base on Secure Path in Ad hoc Wireless Networks", IEEE International Forum on Computer Science-Technology and Applications IFCSTA 2009.

[4] S. Al-Otaibi, F. environments based on the history of nodes in ad hoc networks", IEEE the First Asian Himalayas International Conference on Internet AH-ICI 2009.Siewe, "Security of access in hostile

[5] Ali Hilal Mohamad, H. Zedan, A. Cau, ―Security Solution for Mobile Ad Hoc Network of Networks (MANoN)‖, IEEE Fifth International Conference of Networking and Services ICNS 2009.

[6] Esa Hyytiä and Jorma Virtamo, "Random waypoint model in n- dimensional space", Operations Research Letters, vol. 33/6, pp. 567 – 571, 2005.

[7] Haas Z. J., Pearlman M. R., and Samar P., "The Zone Routing Protocol (ZRP)", IETF Internet Draft, draft-ietf-manet-zone-zrp- 04.txt, July 2002.

[8] C. Siva Ram Murthy and B. S Manoj, "Ad Hoc Wireless Networks, Architecture and Protocols", Prentice Hall PTR, 2004.

[9] L. Zhou and Z. J Haas, "Securing Ad Hoc networks," IEEE Network Magazine, vol. 13, no. 6, December 1999.

[10] M. O. Pervaiz, M. Cardei, and J. Wu, "Routing Security in Ad Hoc Wireless Networks," Network Security, S. Huang, D. MacCallum, and D. -Z. Du (eds.), Springer, 2008.

[11] Gabriel Montenegro and Claude Castelluccia, "Crypto-Based Identifiers (CBIDs): Concepts and Applications'" ACM Transactions on Information and System Security, February 2004.

[12] S Neelavathy Pari, Sbrish Jayapal and Sridharan Draisamy, "A Trust Security in MANET with Secure Key Authentication Mechanism", ICRTIT – 2012.

[13] X. Duan and X. Wang, ''Authentication handover and privacy protection in 5G hetnets using software-defined networking,'' IEEE Commun. Mag . vol. 53, no. 4, pp. 28–35, Apr 2015.

[14] S. R. Shree, A. C. Chelvan, and M. Rajesh, ''an efficient RSA cryptosystem by applying cuckoo search optimization algorithm,'' Concurrency Computer, Pract. Exper., vol. 31, no. 12, Jun 2019.

[15] W. Jiajia, Y. Chuanwei, W. Lei, and S. Jiaqi, ''Research on LTE decryption Method based on air interface,'' Electron. Products World, vol. 26, no. 8, pp. 40–42, 2019.

[16] Liu, F., Huo, W., Han, Y., Yang, S., & Li, X. (2020). Study on Network Security Based on PCA and BP Neural Network Under Green Communication. IEEE Access, 8, 53733–53749.

[17] Chen, B., Wu, L., Wang, H., Zhou, L., & He, D. (2019). A Block chain Based Searchable Public-Key Encryption with Forward and Backward Privacy for Cloud-Assisted Vehicular Social Networks. IEEE Transactions on Vehicular Technology, 1–1.