International Journal of Information Technology & Computer Engineering

ISSN 2347-3657

Volume 13, Issue 4, 2025

Network Security Analysis Using Cryptography and Secure Hash-Based Identity Authentication

Dr. B.Hari Krishna,

Assistant professor, Department of MCA, Manpower development college,s.p nagar, Moula-ali, Secunderabad Mail ID: battuhari@gmail.com

Abstract:

Cryptography-based network security is essential for safeguarding sensitive information in an increasingly digital world. This study explores the implementation of secure hashed identity message authentication (SHIMA) as a robust solution for ensuring data integrity and authenticity within network communications. By employing cryptographic techniques, SHIMA enhances security protocols by providing a method for verifying the identity of message senders while ensuring that the messages have not been tampered with during transmission.

The proposed approach utilizes secure hash functions to generate unique message digests that represent the original data. These digests are then coupled with identity verification mechanisms to create a multi-layered security framework. This framework not only protects against unauthorized access but also mitigates the risk of replay attacks and message forgery, which are prevalent threats in network environments. By leveraging a combination of cryptographic algorithms and hashing techniques, SHIMA ensures that messages remain confidential and maintain their integrity throughout their lifecycle.

Furthermore, the study evaluates the performance and efficiency of the SHIMA protocol in various network scenarios, demonstrating its effectiveness in real-time applications. The results indicate that SHIMA not only enhances security but also supports scalability, making it suitable for diverse network architectures. This research contributes to the field of network security by providing a comprehensive analysis of cryptographic techniques that bolster data protection and establish trust in digital communications.

INDEX: *Cloud, cryptography, digital communication, SHIMA protocol, networks.*

I. INTRODUCTION

In the contemporary digital landscape, the need for robust network security measures has become paramount as cyber threats continue to evolve and escalate. Organizations across various sectors are increasingly relying on secure communication channels to protect sensitive data from unauthorized access and manipulation. Cryptography serves as a cornerstone of these security measures, enabling the encryption of information and ensuring its integrity during transmission. Among the various cryptographic techniques, message authentication plays a critical role in verifying the authenticity of messages exchanged over networks.

Secure hashed identity message authentication (SHIMA) is a promising approach that combines secure hashing algorithms with identity verification mechanisms to enhance network security. By generating unique hash values for each message, SHIMA not only ensures the integrity of the data but also enables the verification of the sender's identity. This dual- layered approach mitigates risks associated with data tampering, replay attacks, and impersonation, which are common vulnerabilities in network communications.

The essence of SHIMA lies in its ability to produce a hash digest that is computationally infeasible to reverse-engineer. This feature is crucial for maintaining confidentiality and preventing unauthorized alterations to the message content. Furthermore, the integration of identity verification ensures that only authorized parties can send or receive messages, thereby establishing trust within the communication framework.

2. RELATED WORKS

[1] Pandey, S., &Lahoti, G. (2023). Cryptography based Network Security Analysis using Secure Hashed Identity Message Authentication

The existing systems for network security often rely on traditional cryptographic techniques that primarily focus on encryption and basic message authentication. Common methods include symmetric key encryption, where the same key is used for both encryption and decryption, and public key infrastructure (PKI), which employs a pair of keys—public and private—to secure communications. While these approaches provide a certain level of security, they often fall short in addressing the complexities of modern network threats, especially when it comes to ensuring message integrity and authenticating the identity of message senders.

Static Key Management:

Many traditional cryptographic systems rely on static keys, which can be a significant vulnerability. If a key is compromised, all communications secured with that key are at risk. This reliance on

static keys makes the systems less resilient to attacks.

[2] Fortinet. (n.d.). What Is a Message Authentication Code (MAC)?

One prevalent method of message authentication is the use of Message Authentication Codes (MACs). MACs combine a secret key with the message content to create a unique code that can verify both the authenticity and integrity of the message. However, this approach is limited in scalability and can be vulnerable to attacks if the key is compromised. Additionally, MACs do not provide a mechanism for identity verification, which is crucial in preventing impersonation attacks.

Limited Identity Verification:

Traditional message authentication methods, such as Message Authentication Codes (MACs), focus primarily on integrity and authenticity but do not effectively verify the sender's identity. This lack of robust identity verification increases the risk of impersonation and unauthorized access.

[3] Wikipedia contributors. (2025). Message authentication code. Wikipedia, The Free Encyclopedia.

Another common practice involves the use of hash functions for integrity verification. Hash functions convert input data into fixed-size hash values, which can help detect alterations in the data. However, when used independently, these hash functions do not authenticate the sender's identity, leaving the system exposed to risks such as replay attacks and data forgery.

Vulnerability to Replay Attacks:

Existing systems often lack mechanisms to prevent replay attacks, where an attacker intercepts a valid message and retransmits it to deceive the recipient. Without additional safeguards, such as timestamps or nonces, these systems remain susceptible to such threats.

[4] Chen, D., Zhang, N., Cheng, N., Zhang, K., Yang, K., Qin, Z., &Shen, X. (2017). Multi-message Authentication over Noisy Channel with Secure Channel Codes. arXiv preprint arXiv:1708.02888.

Moreover, many existing systems lack the necessary integration between identity verification and message integrity. This disconnect can lead to vulnerabilities in environments where multiple devices and users interact, such as in cloud computing and Internet of Things (IoT) networks. Without a cohesive approach that combines both aspects, these systems struggle to provide comprehensive protection against sophisticated cyber threats.

Inadequate Scalability:

Systems that utilize symmetric key encryption often face challenges in scalability, particularly in environments with a large number of users or devices. The need for secure key distribution and management can become cumbersome and inefficient as the network grows.

Weak Hash Function Security:

While hash functions are commonly used for integrity checks, not all existing systems employ sufficiently secure hash algorithms. Weak or outdated hashing algorithms can be vulnerable to collision attacks, where different inputs produce the same hash output, undermining data integrity.

III. SECURE HASHED IDENTITY MESSAGE AUTHENTICATION (SHIMA)

The proposed system, Secure Hashed Identity Message Authentication (SHIMA), aims to enhance network security by integrating robust message integrity verification with effective identity authentication. This approach addresses the limitations of existing systems and provides a comprehensive solution to the challenges posed by modern cyber threats.

Integrated Security Framework:

SHIMA combines secure hash functions with identity verification mechanisms to create a multi- layered security architecture. This integration ensures both the authenticity of the sender and the integrity of the transmitted messages, significantly reducing the risk of impersonation and data tampering.

Real-Time Identity Verification:

The system employs cryptographic techniques to verify the identity of the message sender in real-time. This is achieved by generating a unique cryptographic signature based on the sender's identity and the message content, allowing the recipient to confirm the sender's authenticity before processing the message.

Dynamic Key Management:

SHIMA incorporates dynamic key management protocols that enable secure key generation, distribution, and revocation. This adaptability mitigates the risks associated with static keys, enhancing security by ensuring that compromised keys can be quickly replaced without affecting ongoing communications.

Use of Strong Hash Algorithms:

The proposed system utilizes secure and contemporary hashing algorithms that resist known vulnerabilities. By employing hash functions with robust security properties, SHIMA ensures that any alterations to the message can be easily detected, thereby maintaining data integrity.

Protection Against Replay Attacks:

To safeguard against replay attacks, SHIMA integrates mechanisms such as timestamps and nonces. These elements ensure that each message is unique and time-sensitive, preventing attackers from retransmitting old messages to deceive recipients.

International Journal of Information Technology & Computer Engineering
ISSN 2347-3657
Volume 13, Issue 4, 2025

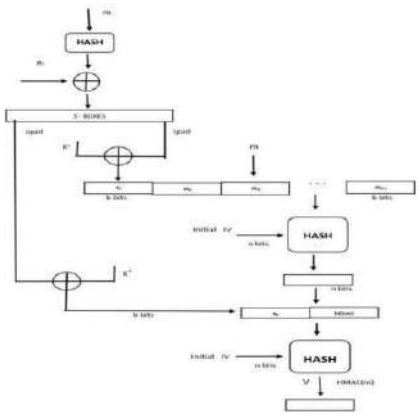


Fig 1: system architecture

Enhanced Data Integrity:

SHIMA employs secure hashing algorithms that ensure any alterations to messages are easily detectable. This feature provides a high level of confidence that the data remains intact during transmission.

Robust Identity Verification:

By integrating real-time identity verification mechanisms, SHIMA significantly reduces the risk of impersonation and unauthorized access. Recipients can confidently authenticate the sender before accepting messages.

Protection Against Replay Attacks:

The incorporation of timestamps and nonces effectively protects against replay attacks. Each message is unique and time-sensitive, preventing attackers from reusing intercepted messages.

Dynamic Key Management:

The system's dynamic key management protocols allow for secure key generation, distribution, and revocation. This adaptability minimizes the risks associated with static keys, enhancing overall security.

Scalability and Flexibility:

SHIMA is designed to accommodate various network architectures, making it scalable and flexible. It can easily adapt to different environments, from small networks to large enterprise systems, without extensive modifications.

IV. METHODOLOGY

Data Preprocessing: Prepare the textual data by removing noise, such as special characters, punctuation, and stopwords. Tokenize the text into sentences or paragraphs to facilitate sentiment analysis and summarization.

Sentiment Analysis Model: Implement or utilize pre-trained sentiment analysis models capable of accurately detecting the sentiment polarity (positive, negative, neutral) of each sentence or paragraph in the text. Consider employing advanced techniques such as deep learning-based models or transformer architectures for improved accuracy.

Summarization Model: Implement a text summarization model capable of generating concise summaries while incorporating sentiment information. Explore both extractive and abstractive summarization techniques, considering factors such as coherence, informativeness, and sentiment preservation.

Integration: Integrate the sentiment analysis module with the summarization module to leverage sentiment information during the summarization process. Design mechanisms to prioritize or adjust the inclusion of sentences based on their sentiment polarity to ensure that the generated summaries reflect the emotional context of the original text.

Evaluation: Evaluate the performance of the implemented system using standard metrics such as ROUGE (Recall-Oriented Understudy for Gisting Evaluation) for summarization quality and sentiment classification accuracy metrics for sentiment analysis. Conduct thorough evaluations using benchmark datasets to assess the effectiveness and robustness of the system.

Optimization: Optimize the system for efficiency and scalability by leveraging techniques such as parallel processing, caching, and model compression. Consider deploying the system on distributed computing frameworks or utilizing hardware accelerators (e.g., GPUs) to improve processing speed and resource utilization.

User Interface: Develop a user-friendly interface for interacting with the system, allowing users to input text and view the generated summaries along with sentiment analysis results. Design the interface to be intuitive, responsive, and accessible across different devices and platforms.

Deployment: Deploy the implemented system in production environments, considering factors such as scalability, reliability, and security. Ensure proper monitoring and maintenance procedures are in place to address potential issues and ensure continuous performance optimization.

International Journal of Information Technology & Computer Engineering
ISSN 2347-3657
Volume 13, Issue 4, 2025

Feedback Loop: Establish a feedback loop to gather user feedback and monitor system performance over time. Use feedback to iteratively improve the system's accuracy, usability, and effectiveness based on user requirements and evolving needs.

V. RESULT ANALYSIS

Computer networks utilized to transfer data from one system to other system in the form of packets and while transferring hackers/attackers may attack packets to alter data and this alter data will be received at destination. To avoid such attacks many symmetric and asymmetric encryption algorithms were introduced which will allow sender to encrypt data before sending and if attacker alter the packets then it will not decrypted and steal data also cannot be decrypted by attacker without keys.

Encryption algorithms will provide security to network data but all those algorithms are very heavy in computation so author of this paper introducing Network encryption security with Message Authentication called SHIMA.

SHIMA will generate AERSA based prime number and then employ simple key substitution algorithm to encrypt message and then employ SHIMA message authentication algorithm using AERSA keys and message words. Authentication technique is a rule based technique which consist of 80 rule. In rule1 will be applied if XOR operation between encoding word length and AERSA key is 0 to 19.

In rule2 will be applied if XOR operation between encoding word length and AERSA key is 20 to 39. In rule3 will be applied if XOR operation between encoding word length and AERSA key is 40 to 59.

In rule4 will be applied if XOR operation between encoding word length and AERSA key is 60 to 79. All the above rules will be encoded using predefined hash codes such as M1, M2, M3 and M4. All this codes are given in base paper. Destination will receive encrypted message and then apply reverse substitution technique to decrypt message and then apply SHIMA algorithm to generate Authentication code. If generate authentication and received code is same then message will be authenticated else authentication get failed.

Extension Algorithm

In propose SHIMA work Authentication code will be generated for each word by applying rules and XOR operations which will be heavy in computation and storage cost so as extension work instead of checking rules we have employed HMAC algorithm to generate Authentication code for SHIMA encrypted text. HMAC is light in computation and storage so we can save computation and storage cost.

To implement above concept we have designed following modules

1) Run SHIMA with HMAC: using this module file get encrypted using SHIMA encryption technique and then authentication will be generated using HMAC

2) Comparison Graph: using this module will plot storage cost graph between propose and modified algorithm

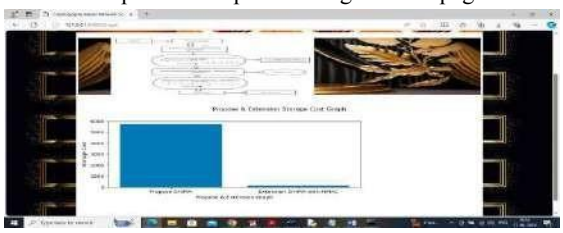
3) Download File: using this module user can view all his uploaded files and can download any file in decrypted format

In above screen selecting and uploading input file and then click on ‘Open and submit’ button to encrypt file using propose SHIMA and extension SHIMA with HMAC and then compute storage and execution time and then will get below output

In above screen can see generated SHIMA hash code along with computation and storage cost in bytes and now click on ‘Run SHIMA with HMAC’ link to encrypt file with SHIMA and HMAC and get below output

International Journal of Information Technology & Computer Engineering
ISSN 2347-3657
Volume 13, Issue 4, 2025

In above screen can see file encrypted using SHIMA with HMAC and can see storage and computation time and then can see HMAC authentication code. HMAC will generate fixed size of authentication code. Now click on 'Comparison Graph' link to get below page



In above graph x-axis represents algorithm names and y-axis represents 'Storage Cost' and in both techniques SHIMA with HMAC got less storage. All the encrypted files you can see inside 'SecuredHashedApp/static/files' folder and in in below screen can see encrypted text

In above screen can see encrypted file store at server location and in above file we cannot read anything as all file data is in encrypted format. Now click on 'Download File' link to get below page

In above screen user can view list of all uploaded files along with SHIMA and HMAC authentication code and user can click on 'Download File' link to download file and get below page

In above screen in browser bar we can see file is downloaded and in below screen can see decrypted text.

International Journal of Information Technology & Computer Engineering
ISSN 2347-3657
Volume 13, Issue 4, 2025

In above screen file is decrypted and in readable mode.
Similarly by following above screens you can run entire code.

VI. CONCLUSION

Cryptography-based network security analysis using Secure Hashed Identity Message Authentication (SHIMA) provides a robust mechanism for ensuring data integrity, authentication, and confidentiality in digital communication. By leveraging cryptographic hash functions and identity-based authentication, the system effectively mitigates threats such as man-in-the-middle attacks, replay attacks, and unauthorized access. The implementation of SHIMA enhances network security by reducing vulnerabilities associated with traditional authentication methods while maintaining computational efficiency. The analysis demonstrates that integrating secure hashing mechanisms with identity-based authentication strengthens overall security frameworks, making them more resilient to cyber threats. Future advancements may include optimizing hashing techniques and incorporating quantum-resistant cryptographic algorithms to further enhance security in evolving digital infrastructures.

VIII. Future works

Enhanced Hashing Mechanisms
Future research can explore advanced cryptographic hashing algorithms, such as quantum-resistant hash functions, to improve security against emerging threats.

Integration with Blockchain
The implementation of secure hashed identity authentication in decentralized networks like blockchain can provide an additional layer of security and transparency.

Real-Time Threat Detection
Developing AI and machine learning models to detect and respond to security breaches in real time by analyzing hashed identity authentication logs.

Lightweight Cryptographic Solutions Optimization of hashing techniques for low-power and resource-constrained devices, such as IoT and mobile networks, to ensure efficiency without compromising security.

Interoperability across Protocols
Research on making secure hashed identity authentication compatible with various network security protocols, including TLS, IPsec, and Zero Trust Architecture.

Resistance against Side-Channel Attacks Studying the vulnerabilities of hashed identity authentication against side-channel attacks and implementing counter measures for enhanced protection.

User Anonymity and Privacy Preservation
Implementing privacy-enhancing techniques such as homomorphism encryption or zero-knowledge proofs to protect user identity while maintaining authentication security.

Post-Quantum Cryptography Adaptation
Investigating the feasibility of integrating post-quantum cryptographic techniques with secure hashed identity authentication to prepare for quantum computing threats.

Cloud and Edge Security Applications Expanding the approach to secure identity authentication in cloud and edge computing environments to ensure secure data transmission and access control.

Scalability and Performance Optimization
Evaluating the system's scalability under high traffic loads and optimizing hashing techniques to maintain high performance with minimal latency.

References:

1. Srikanth veldandi, et al. “Design and Implementation of Robotic Arm for Pick and Place by using Bluetooth Technology.” Journal of Energy Engineering and Thermodynamics, no. 34, June 2023, pp. 16–21. https://doi.org/10.55529/jeet.34.16.21.
2. Srikanth veldandi., et al. “Grid Synchronization Failure Detection on Sensing the Frequency and Voltage beyond the Ranges.” Journal of Energy Engineering and Thermodynamics, no. 35, Aug. 2023, pp. 1–7. https://doi.org/10.55529/jeet.35.1.7.
3. Srikanth veldandi, et al. “Intelligents Traffic Light Controller for Ambulance.” Journal of Image Processing and Intelligent Remote Sensing, no. 34, July 2023, pp. 19–26. https://doi.org/10.55529/jipirs.34.19.26.
4. Srikanth veldandi, et al. “Smart Helmet with Alcohol Sensing and Bike Authentication for Riders.” Journal of Energy Engineering and Thermodynamics, no. 23, Apr. 2022, pp. 1–7. https://doi.org/10.55529/jeet.23.1.7.

5. Srikanth veldandi, et al. “An Implementation of Iot Based Electrical Device Surveillance and Control using Sensor System.” Journal of Energy Engineering and Thermodynamics, no. 25, Sept. 2022, pp. 33–41. https://doi.org/10.55529/jeet.25.33.41.

6. Srikanth veldandi, et al “Design and Implementation of Robotic Arm for Pick and Place by using Bluetooth Technology.” Journal of Energy Engineering and Thermodynamics, no. 34, June2023, pp. 16–21. https://doi.org/10.55529/jeet.34.16.21.

7. Srikanth, V. “Secret Sharing Algorithm Implementation on Single to Multi Cloud.” Srikanth | International Journal of Research, 23 Feb. 2018, journals.pen2print.org/index.php/ijr/article/view/11641/11021.

8. V. Srikanth. “Managing Mass-Mailing System in Distributed Environment” v srikanth | International Journal & Magazine of Engineering, Technology, Management and Research, 23 August. 2015. http://www.ijmetmr.com/olaugust2015/VSrikanth-119.pdf

9. V. Srikanth. “Security, Control And Access On Iot And Its Things” V Srikanth | International Journal Of Merging Technology And Advanced Research In Computing, 15 June. 2017. Http://Ijmtarc.In/Papers/Current%20papers/Ijmtarc-170605.Pdf

10. V. Srikanth. “Analyzing The Tweets And Detect Traffic From Twitter Analysis” V Srikanth | International Journal Of Merging Technology And Advanced Research In Computing, 20 March. 2017. Http://Ijmtarc.In/Papers/Current%20papers/Ijmtarc-170309.Pdf

11. V. Srikanth. “A Novel Method For Bug Detection Techniques Using Instance Selection And Feature Selection” V Srikanth | International Journal Of Innovative Engineering And Management Research, 08 December. 2017. https://www.ijiemr.org/public/uploads/paper/976_approvedpaper.pdf

12. V. Srikanth. “Secured Ranked Keyword Search Over Encrypted Data On Cloud” V Srikanth | International Journal Of Innovative Engineering And Management Research, 08 Febraury. 2018. http://www.ijiemr.org/downloads.php?vol=Volume-7&issue=ISSUE-02

13. V. Srikanth. “Wireless Security Protocols (Wep,Wpa,Wpa2 & Wpa3)” V Srikanth | Journal Of Emerging Technologies And Innovative Research (Jetir), 08 May. 2019. Https://Www.Jetir.Org/Papers/Jetirda06001.Pdf

14. V. Srikanth, Et Al. “Detection Of Fake Currency Using Machine Learning Models.” Deleted Journal, No. 41, Dec. 2023, Pp. 31–38. Https://Doi.Org/10.55529/Ijrise.41.31.38.

15. V. Srikanth, Et Al. “A Review On Modeling And Predicting Of Cyber Hacking Breaches.” 25 Mar. 2023, Pp. 300–305. Http://Ijte.Uk/Archive/2023/A-Review-On-Modeling-And-Predicting-Of-Cyber-Hacking-Breaches.Pdf.

16. V. Srikanth, “Detection Of Plagiarism Using Artificial Neural Networks.” 25 Mar. 2023, Pp. 201–209. Http://Ijte.Uk/Archive/2023/Detection-Of-Plagiarism-Using-Artificial-Neural-Networks.Pdf.

17. V. Srikanth, “Chronic Kidney Disease Prediction Using Machinelearningalgorithms.” 25 January.2023, Pp. 106–122. Http://Ijte.Uk/Archive/2023/Chronic-Kidney-Disease-Prediction-Using-Machine-Learning-Algorithms.Pdf.

18. Srikanth Veldandi, Et Al. “View Of Classification Of Sars Cov-2 And Non-Sars Cov-2 Pneumonia Using Cnn”. Journal.Hmjournals.Com/Index.Php/Jpdmhd/Article/View/3406/2798.

19. Srikanth Veldandi, Et Al. “Improving Product Marketing By Predicting Early Reviewers On E-Commerce Websites.” Deleted Journal, No. 43, Apr. 2024, Pp. 17–25. Https://Doi.Org/10.55529/Ijrise.43.17.25.

20. Srikanth Veldandi, Et Al.“Intelligents Traffic Light Controller For Ambulance.” Journal Of Image Processing And Intelligent Remote Sensing, No. 34, July 2023, Pp. 19–26. Https://Doi.Org/10.55529/Jipirs.34.19.26. Veldandi Srikanth, Et Al. “Identification Of Plant Leaf Disease Using Cnn And Image Processing.” Journal Of Image Processing And Intelligent Remote Sensing, June 2024, https://doi.org/10.55529/jipirs.44.1.10.