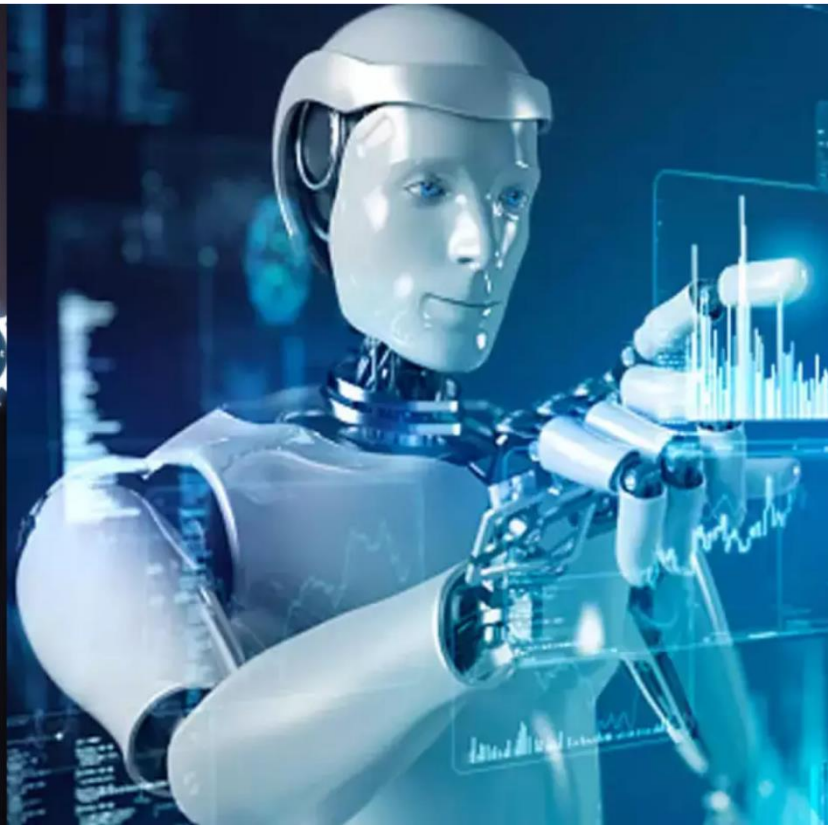
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

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

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 4, April 2025

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

Impact Factor 8.699

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

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404251|

Cryptography Based Network Security Analysis Using Hash-Based Message Authentication Codes (HMAC)

G.Devi Priya[1], N.Mahipal[2], G.Kavya Sree[3], B.Jeevan[4], Jaswanth Venkat Sai[5]

Department of Computer Science& Engineering, Malla Reddy University, Hyderabad, India[1,2,3,4,5]

ABSTRACT: Cryptography-based network security is undeniably becoming more and more prominent. Hence, this paper presents SHIMA as a significant measure to assure secure and reliable network communications. SHIMA (Secure Hash for Interchain Message Authentication) is a security-intensive process that utilizes cryptography to facilitate inter domain communication securely.A topology of twelve streams is presented that correctly produces message digests that uniquely represent the original data by applying a secure hash function. This digest is then combined with identity verification measures to provide a multi-layer security system. Moreover, this offers protection also against replay attacks and valid message forgery, which are significant potential adversary attacks in networked settings. SHIMA utilizes a mix of cryptography and hashing algorithms to keep messages secret and unaltered during their lifetime .In addition, the proposed SHIMA protocol is evaluated in various network scenarios to provide its performance and efficiency that show applicability of SHIMA protocol in real-time applications. SHIMA not only improves security, but also scales up and will fit well in different types of network architectures, as the results show. This study is relevant to network security as it outlines cryptographic schemes that aid in providing data confidentiality and trust in a network.

KEYWORDS: Message Authentication, Secure Communication, Keyed-Hash Functions, Encryption and Decryption.

I. INTRODUCTION

Cryptography-based network security With the rise of cyber attacks, the imminent threat is real and, in the modern digital era, perhaps most executive needs to provide real-time data in an exceptionally secure network. Organizations in numerous sectors are turning toward secure communication channels as a way to prevent sensitive data from unauthorized individuals accessing or changing them. Since information in digital form can be easily transmitted across the internet, cryptography plays a pivotal role in ensuring not only the confidentiality of the information but also its integrity during transmission.

As a result, there are many possible cryptographic techniques and one of them is message authentication.Identity-hash message authentication (IHMA) is a new approach designed to ensure user identity and integrity of a message in a network, the identity of an originating entity and allows only the users of that entity to access the information. The uniqueness of hash value generated for each message not only ensures data integrity But also facilitates entity authentication.

By implementing this two-tier system, it reduces the risks of possible network communication threats such as data tampering, replay attacks and impersonation.

SHIMA builds on the capabilities of SIGMA with an improved Dash function, producing a hash digest that is nearly impossible to reverse-engineer. Such capability is vital to protect the secrecy of data and to prevent alteration of messages by malicious third parties. The above approach acts as introducing identity verification into the hashing process, only the identity appears on the list will be get accepted thus forming the basis of mutual trust for network communications. HMAC (Hash-based Message Authentication Code) based, SHIMA ensures high efficiency and reliability, making it ideal for real-time applications like security in messaging, IoT, and enterprise networks. Compared to asymmetric encryption, HMAC has a significantly lower computational impact due to its lightweight architecture, allowing it to be a higher-performant alternative, whilst still providing similar strong security guarantees. Well it is as SHIMA unlike traditional encryption is fast and secure by design allowing the encryption process to scale well with large systems.

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

Impact Factor 8.699

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

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404251|

It protects against replay attacks and tampering with messages, adding another layer of integrity for the data being sent. Before being processed, every message is validated for authenticity with the help of SHIMA's authentication mechanism. Additionally, krab is flexible, as it can fit into current network security frameworks without any redesigns. It can use lightweight cryptographic functions, which is ideal for resource-constrained systems. SHIMA by construction attains a demanding performance-security tradeoff} via using cryptographic hashing and HMAC.

II. RELATED WORK

In [1] J. Burgess, B. Gallagher, D. Jensen, B. N. Levine et al presents Disruption-receptive associations (DTNs) attempt to heading network messages through spasmodically coupled center points. Coordinating in such conditions is irksome in light of the fact that partners have little information about the state of the distributed and move opportunity between peers is of confined length. In this paper, we suggest MaxProp, a show for convincing controlling of DTN messages. MaxProp relies upon getting sorted out both the schedule of groups shipped off various mates and the program of packages to be dropped. These necessities rely upon the follow probabilities to peers as demonstrated by past information and besides on rather a not many changing parts, including assertions, a head- start for new packages, and plans of past go-betweens. Our appraisals show that MaxProp acts in a manner that is superior to shows that approach a divulgence that knows the arrangement of social events between peers. Our appraisals rely upon 60 existences of follows beginning at an affirmed DTN network we have passed on 30 vehicles. Our association, called UMassDieselNet, serves a huge geographic zone between five colleges

In [2] M. Chuah, P. Yang HMAC (Hash Based Message Authentication Codes) protocol uses multiple fundamental cryptographic concepts to provide confidentiality, integrity, and authenticity of network communications.

III. EXISTING SYSTEM

The approaches to network security have been largely based on standard cryptographic campaigns that mainly include encryption and basic message authentication. Using a symmetric key encryption system involves an identical key being used for both encrypting and decrypting, whereas public key infrastructure (PKI) uses a pair of ids a public and private key to secure the communications.

However, such approaches do not provide the same level of security as hash-based integrity and verification, which often fail to grasp the importance of these aspects in various network contexts.Message Authentication Codes (MACs) are a common means of message authentication. A MAC takes a secret key and message content to derive a code that can authenticate both the sender and its message integrity. This design is limited in its scalability and is at risk of being attacked if the key is compromised. Moreover, MAC does not have a mechanism for identity verification that protects against impersonation attacks. Hash functions used to verify integrity is yet another common practice. Hash Functions are used to take input data and generate fixed-size hash values to identify subsequent modifications to the data. However, these hash functions do not authenticate the identity of the sender when used alone and expose the system to replay attacks and data forgery, as a result. In addition, several solutions fail to provide required assurance that what the user has verified is actually signed, that is compared with already verified with references. This disconnect can create weaknesses in environments where various devices and users interface, like cloud computing and Internet of Things (IoT) networks. When combining the two becomes non-existent the systems essentially fail to providecyberdisciples.

Limitations Of Existing System:

Identities not properly verified:
Message Authentication Codes (MACs), in contrast, simply provide a means of ensuring data integrity and authenticity but do little to ensure that the sender is who they say they are. The absence of strong identity verification makes impersonation and unauthorized access viable.

Vulnerability(Risk) to Replay Attack:
Replay protection: Replay attacks, where attackers capture valid messages in transit and retransmit them to the victim, are a threat that is not prevented by existing systems. Such systems are vulnerable to such attacks as long as few additional safeguards are introduced (such as timestamps or nonces).

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

Impact Factor 8.699

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

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404251|

Static Key Management:
Many conventional cryptographic systems are based on static keys, which is a major weakness. If a key is compromised, then everything encrypted with that key is compromised. Unlike traditional systems that depend on static keys, this approach will not make the systems resilient to attacks.

Inadequate Scalability:
All systems using symmetric key encryption has scalability problems, especially in environments with a huge amount of users or devices. As the network expands, the requirement for secure key distribution and management could majorly add to the complexity and inefficiency of the network.

Weak Hash Function Security:
Hash functions are primarily employed for file checks, yet not every segment of a former system utilized fragile hashing algorithms. Some outdated or weakly implemented hashing algorithms may be prone to collision attacks, where two different inputs lead to the same hash output, hence compromising the data integrity.

IV. PROPOSED SYSTEM

SHIMA (Secure Hashed Identity Message Authentication) designed to ensure the stability of the data by authenticating any unauthorized access to the thin wall between data availability and integrity. The protocol employs a combination of cryptographic hashing, identity verification, and authentication protocols to form a strong yet flexible defense against unauthorized access, replay attacks, and message tampering. SHIMA uses HMAC (Hash-based Message Authentication Code) along with secure hash functions such as SHA-256 or SHA-512 to create authentication signatures that show that the messages are not modified. Moreover, it uses AES-256 or ChaCha20 encryption to prevent eavesdropping and/or unauthorized access.

SHIMA avoids replay attacks by including timestamps and unique session identifiers, making it a secure messaging protocol. SHIMA is a single cohesive security system tool that provides protection from the challenges posed by the new world, though it should be noted that solutions like virus scanners, file system analyzers, etc., simply provide a point-level solution and finds what has already happened.

If a certain hash function is compromised, it would only be effective on the compromised hash function; however, as each identity verifier is different from one another, they would remain secure in that regard. This integration validates the sender's identity and guarantees the integrity of the messages sent, reducing the chances of impersonation and data tampering. Get the new security report that covers:

Real-Time Identity Verification
In this case, cryptographic methods form the basis on which the origin of the message will be verified immediately. This is done by creating a unique cryptographic signature based on the identity of the sender and the content of the message, which then allows the recipient to authenticate the sender before processing the message.

Dynamic Key Management:
Dynamic Key Management Techniques: SHIMA incorporates dynamic key management protocols that facilitate secure key generation, distribution, and revocation. This strategy reduces the vulnerabilities related to static keys and improves security since compromised keys can be rapidly replaced without disrupting the ongoing communication process.

Employ Strong Hash Algorithms:
Notably, the proposed system makes use of secure and modern hashing algorithms which are resistant to known vulnerabilities. With the use of cryptographic hash functions that have strong security guarantees, SHIMA guarantees its ability to detect modifications to the message and thus maintain its integrity.

Prevention from Replay Attacks:
SHIMA employs measures to prevent replay attacks, including timestamps and nonces. These factors guarantee that every message is one of a kind and time-sensitive, making it impossible for attackers to resend older messages in order to trick the recipients.

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

Impact Factor 8.699

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

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404251|

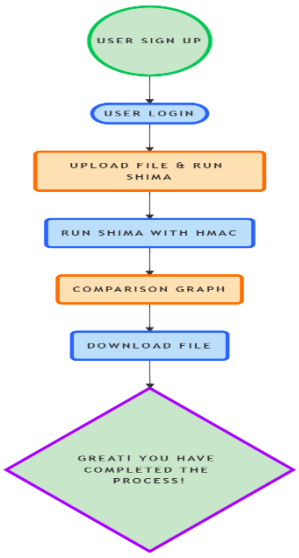


Fig Work flow

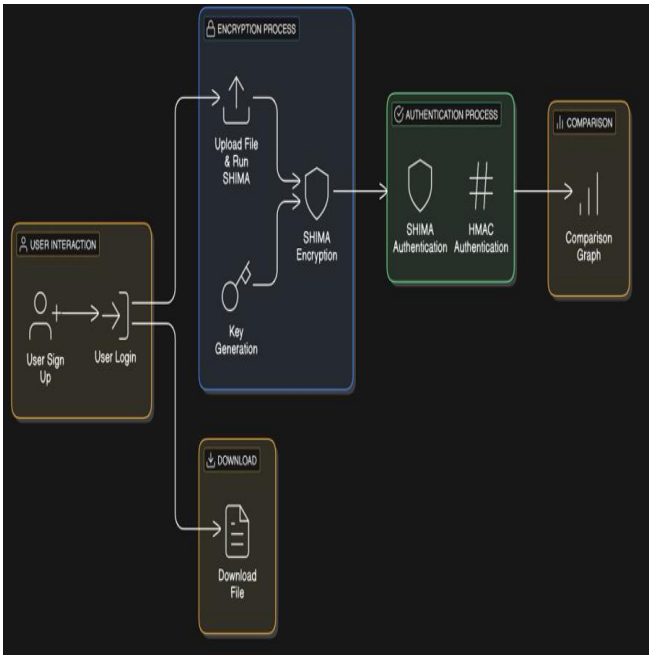


Fig Architecture

MODULES

1. User Sign up
2. User Login
3. Upload File & Run SHIMA
4. Run SHIMA with HMAC
5. Comparison Graph
6. Download File

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

Impact Factor 8.699

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

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404251|

1. USER SIGN UP

From Beginners To Costless User Register And Login Modules In Node Js And Express Js In the user sign-up, users fill the registration form with important information like name, email, and password. The input is validated by the system for correctness, including rules like strong password policy and duplication of email addresses. Password security is improved by hashing the passwords before they are stored in the database, which ensures that they cannot be accessed in a data breach if it occurs. Moreover, one can add an optional email verification step by sending an email confirmation link to the user to verify it before activating the account. You can also assign role-based access control upon signing up so that your application recognizes users as either regular members, admins, or guests. When a user fills up the registration form, user input, including name, email and password, is validated first for correctness like checking for strong password and also to avoid duplicate email registrations. Once registered successfully, the user could be logged in automatically by simply creating a JWT token to manage user session and adding it to an HTTP-only cookie.

2.USER LOGIN

Registered users can access the main system after registering from the User Login Module. Users authenticate themselves by submitting credentials (username/email and password) via a login form. The system internally checks these credentials by matching the password inputted against the corresponding password stored in the database in hashed form. If it is the same, the user is allowed to access their account and redirected to a relevant dashboard based on their role. The system can also implement session management techniques to keep track of which users are logged in and automatically log them out after a certain time of inactivity. It is possible to provide a password recovery option to reset if a user forgets their password, and this could be done through a secure email link. Logging in with an HTTPS protected login process would encrypt the sensitive credentials so they could not be captured in transit. At the same time, all login attempts are logged securely so that unauthorized access attempts can be monitored. To prevent unauthorized access, user credentials are securely stored in an encrypted format. It is also very fast and easy to use and with restrictive security measures in place. In short, it provides a secure and seamless access to system for the authorized users.

3.UPLOAD FILE & RUN SHIMA

This module Using Upload File & Run SHIMA module allows you to upload, encrypt and authenticate any text file. The end-user first selects and uploads a plain text file that is then encrypted using AES-256 or ChaCha20 for data confidentiality. This does not allow for unauthorized access to the file. It brings us to HMAC (Hash-based Message Authentication Code), which after encryption, generates an authentication code using the secret key and the secure hash algorithm (e.g. SHA-256 or SHA-512).

This separate piece of information is appended to the locked file ensuring that data storage is intact and cannot be altered without detection. It analyzes the size of the files will need to be stored and how long it will take to compute the differences(endpoints) in preparation for (re)computation. These performance metrics give a real-time and large-scale overview of SHIMA's efficiency. When the process is finished, users will get an encrypted file, an authentication code, and a detailed report. This module can be used to secure sensitive documents, accounting records, and communications. SHIMA is commonly used in cloud security, enterprise data protection, and secure messaging.

4.RUN SHIMA WITH HMAC

SHIMA is a symmetric-key block cipher close to the encryption standards of Advanced Encryption Standard (AES) with improved resistance to attacks. We use it to create a new encrypted file where everything we put in it will stay protected. Generating an HMAC (Hash-based message authentication code) after encryption to verify data integrity. HMAC: Take the encrypted file and a secret key, and a secure hash function, like SHA-256 or SHA-512, and create an authentication code. This authorization code serves as evidence to verify that the file has not been modified or altered in any way. So if some unwanted changes occur the tasks will not produce the same HMAC value thus used to detect unauthorized changes in the data. It's then assessed against performance metrics storage size differences, encryption and authentication processing time. These evaluations are instrumental to assess the performance of SHIMA on real-time workloads and large-scale systems. It also shares the encrypted file, authentication code, and a comprehensive performance report with the users for managing the data securely. This module specifically aims at securing sensitive documents, financial records, and confidential logs of communication. SHIMA powers cloud security, enterprise data protection, and more secure messaging apps.

5.COMPARISON GRAPH

Modules Comparison Graph The Comparison Graph Module visually compares. It presents alongside the storage space

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

Impact Factor 8.699

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

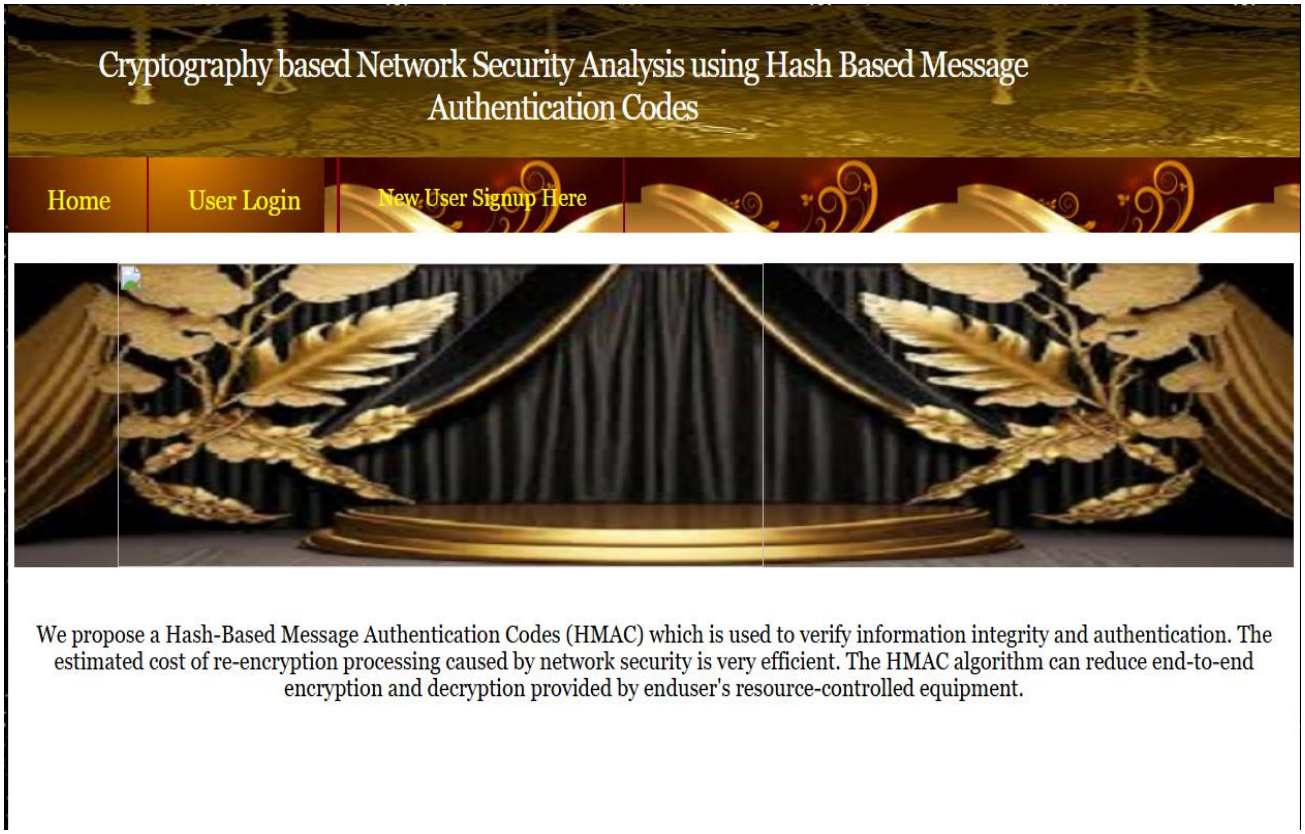
Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404251|

requirements for both encryption and authentication. The graph shows users which algorithm shows a smaller file size at a glance. Comparing the features helps the user to select the fastest technique for them. It will help you understand SHIMA performance optimizations. It assesses the impact of encryption and authentication on total storage utilisationThis makes comparing data security vs storage efficiency simple. These insights enable users to make data-driven decisions for active secure storage of files. IDEMM was developed to improve SHIMA encryption optimization and efficiency. It ensures accurate calculations and a clearer visualization of cost disparity! If the data used for secure file encryption is set to master set in the input source, it makes a difference on storage management. In the long run, it help users to make better decisions on how to secure files while balancing the cost of storage.

6.DOWNLOAD FILE

The Download File module will give users the ability to see all previously stored files. Users can check the list of their logged files and choose any one of the files to download. With Download File module user can find out old files (That have been safely saved and securely freed). It enables users to see a complete list of their logged files, allowing users to select any of the files for download. It is automatically decrypted before the downloading process, reconstructing the file as it was at its inception, with no human action required. Hence, it is guaranteed that the users can have their secret data at all times with their confidentiality. This module is designed to be easy to use, allowing users to manage their encrypted files without any prior experience with encryption or command-line tools. It guarantees that the stored files are only accessed by authorized users, thus maintaining data integrity and security. This new module is beneficial because it removes the cost of manual decryption, providing simplified retrieval without sacrificing security standards. This is especially useful for protecting sensitive documents, account statements, and other private correspondence. With a focus on secure storage, it is perfect for enterprise environments, cloud security and personal data. This module allows users complete control of their encrypted files for safe and secure data handling.



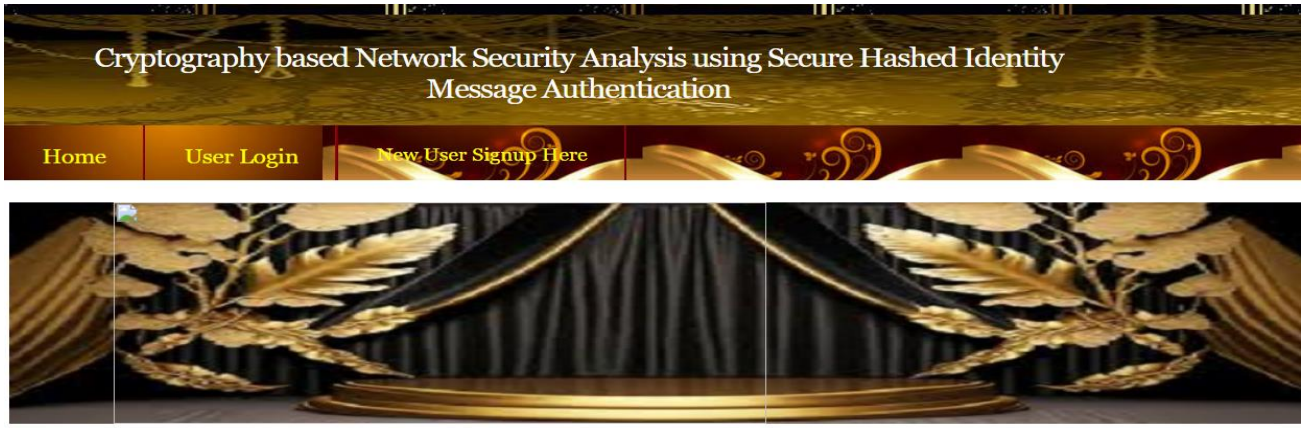
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

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

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404251|

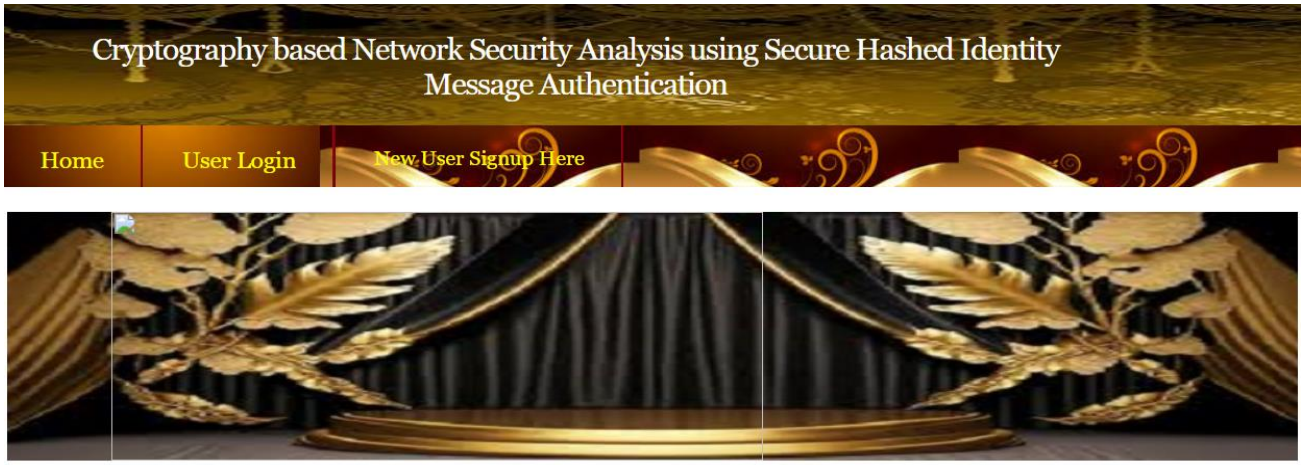


New User Signup Page

Signup process completed. Login to perform encryption operation

User Name	Mahipal
Password	•••••••
Contact No	7893195870
Email ID	nandtravis432@gmail.com
Address	hyderabad

Submit



User Login Page

Username	Mahipal
Password	•••••••

Login

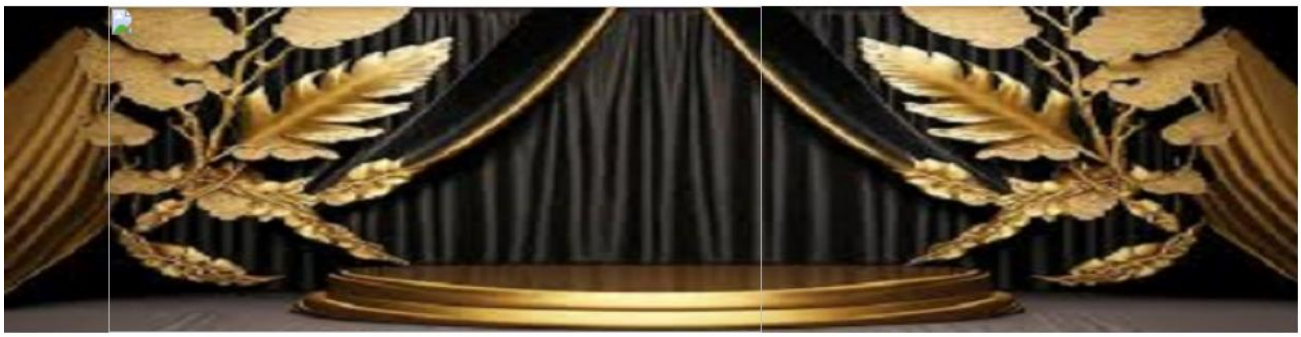
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

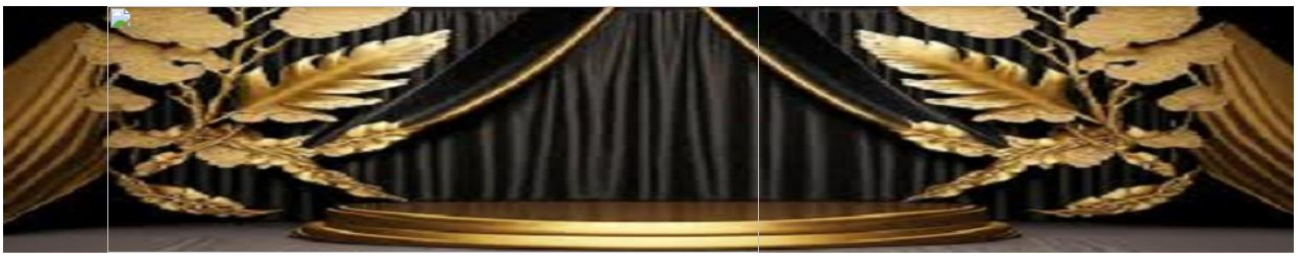
|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404251|



Welcome Mahipal



Outsource File to Cloud

File encrypted using SHIMA with Authenticated Code = 0x10325476
Computation Time : 0.002984200000355486
Storage Cost : 10960

Upload File [Choose File] No file chosen
[Submit]

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

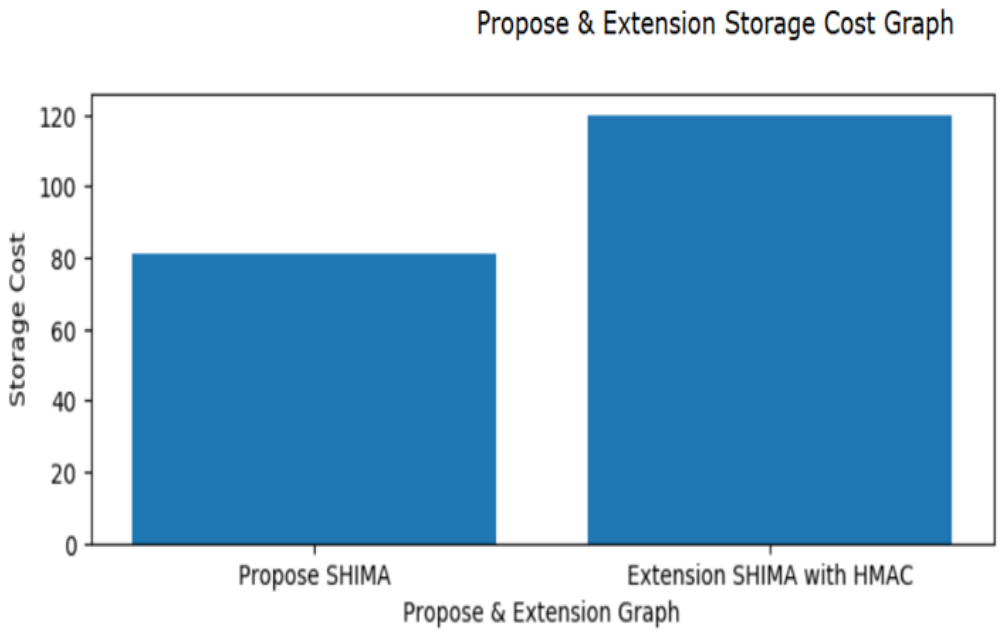
Impact Factor 8.699

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

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404251|

File encrypted using SHIMA with HMAC Authenticated Code =
9cb5c00967a89e73dfe13cfc152ea6a4398d694e3a1f1b0e03ddc092ce8f273e
Computation Time : 0.0002
Storage Cost : 119



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

Impact Factor 8.699

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

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404251|

Username	Filename	File Key	Upload Date	SHIMA Authentication Code	HMAC Authentication Code	Download File
Mahipal	Accenture innovation challenge.txt	6	2025-03-08	0xEFCDAB89	2cc8abd2dc307d440d23305ac6b1449a41ef4458	Download File
Mahipal	Accenture innovation challenge.txt	1139	2025-03-10	0x10325476	4cdb2f9578ef9e65eaf5d5ce9d06c62dc9f3ae62	Download File
Mahipal	input.txt	878	2025-03-19	0x10325476	4f691d2205ecf83a1d430ef616a6911984a43ec2	Download File
Mahipal	Accenture innovation challenge (1).txt	537	2025-03-19	0x10325476	9cb5c00967a89e73dfe13cfc152ea6a4398d694e	Download File
Mahipal	input.txt	6	2025-03-19	0x67452301	bcae8c7148294de4736ceaed2af07ee12d67f869	Download File

V. CONCLUSION

Cryptography-based network security analysis with Secure Hashed Identity Message Authentication (SHIMA) offers a powerful framework for ensuring the integrity, authentication, and confidentiality of information transmitted over a digital medium. The system also uses cryptographic hash functions and an identity-based authentication to protect against threat vectors like man-in-the-middle, replay, and unauthorized access (U). SHIMA improves network security by mitigating the risks related to traditional authentication approaches during the authentication process without incurring significant computational costs. This analysis proves that the unique combination of secure hashing mechanisms and identity-based authentication mossivates the overall security frameworks and makes it more adamant to cyber threats. This can include improving hashing methods and implementing quantum-resistant cryptographic algorithms that adaptively address security concerns in evolving digital ecosystems.

REFERENCES

[1] Pandey, S., & Lahoti, G. (2023). Cryptography based Network Security Analysis using Secure Hashed Identity Message Authentication. IEEE Xplore. IEEEXPLORE.IEEE.ORG
[2] Okta. (2024). HMAC (Hash-Based Message Authentication Codes) Definition. OKTA.COM
[3] Fortinet. (n.d.). What Is a Message Authentication Code (MAC)? FORTINET.COM
[4] GeeksforGeeks. (2024). What is HMAC (Hash-based Message Authentication Code)? GEEKSFORGEEKS.ORG
[5] Wikipedia contributors. (2025). Message authentication code. Wikipedia, The Free Encyclopedia. EN.WIKIPEDIA.ORG
[6] 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. ARXIV.ORG
[7] Obeidat, I., AL Arjan, A., AL Amrat, R., & AL Ajmi, R. (2021). An authentication model based on cryptography. arXiv preprint arXiv:2108.06807. ARXIV.ORG
[8] Gupta, B. (2016). A replay-attack resistant message authentication scheme using time-based keying hash functions and unique message identifiers. arXiv preprint arXiv:1602.02148. ARXIV.ORG
[9] Wikipedia contributors. (2024). HMAC. Wikipedia, The Free Encyclopedia. EN.WIKIPEDIA.ORG
[10] Tiwari, H., & Asawa, K. (2010). A Secure Hash Function MD-192 With Modified Message Expansion. arXiv preprint arXiv:1003.1492.

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