International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 01 | January - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

TRANSACTORY AUTHENTICATION USING KERBEROS

Thejaswini C S[1], Vinay Kumar K M[2], Sophiya Fathima[3], Vinod Kumar H M[4], Mahesh S[5]

[1]Thejaswini C S, ISE, Vidya Vikas Institute of Engineering & Technology Mysore
[2]Vinay Kumar K M, ISE, Vidya Vikas Institute of Engineering & Technology Mysore
[3]Sophiya Fathima, ISE, Vidya Vikas Institute of Engineering & Technology Mysore
[4]Vinod Kumar H M, ISE, Vidya Vikas Institute of Engineering & Technology Mysore
[5]Mahesh S, ISE, Vidya Vikas Institute of Engineering & Technology Mysore

ABSTRACT: The paper introduces a novel transactional authentication framework for distributed environments, built upon the established Kerberos protocol. This framework tackles the security vulnerabilities inherent in multi-client and server interactions during transactions, ensuring robust authentication, data integrity, and confidentiality. By utilizing the Key Distribution Center's (KDC) trusted third-party function in Kerberos, the framework provides clients with time-limited session tickets, eliminating the requirement for repeated authentication during a transaction. This novel strategy promotes a distributed system's transactional environment that is safer and more effective.

Key Words: Kerberos, Key Distribution Center's (KDC), Ticket, Pre-Authentication, Token, Security Authentication, Authorization.

1. INTRODUCTION: In the complex landscape of interconnected systems, guaranteeing secure communication and identity verification is paramount, especially when sensitive data and transactions flow. Enter Kerberos, a robust authentication protocol named for the mythical three-headed dog, developed by MIT in the 1980s. Now a widely trusted solution, Kerberos safeguards networks, distributed systems, and cloud environments. Kerberos empowers mutual authentication between clients and servers, safeguarding access and data from malicious manipulation. Its core lies in "tickets," secure cryptographic credentials that prove identity, enabling users and services to interact confidently without exposing passwords or other sensitive information.

The presented framework incorporates a three-step authentication mechanism encompassing the client, server, and Key Distribution Center (KDC). In the first step, the client undergoes authentication with the KDC, obtaining a session ticket containing a unique session key. This approach serves a dual purpose: firstly, it minimizes the computational burden associated with recurrent authentication, facilitating streamlined transaction processing. Secondly, it guarantees the privacy of critical transactional information by implementing encryption methods utilizing the session key. Furthermore, the framework exhibits scalability and interoperability by aligning with the established and widely accepted Kerberos standard. Because Kerberos supports single sign-on (SSO), it simplifies the user authentication procedure, which is a major advantage. Users obtain a ticket-granting ticket (TGT) upon successful authentication with the Key Distribution Center (KDC).

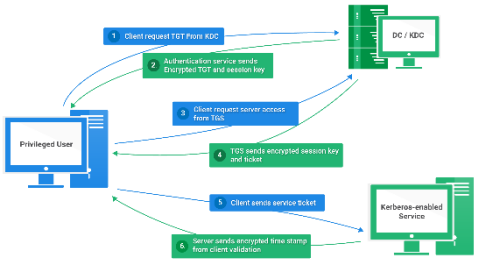

Fig 1.
Kerberos Fundamentals

They can now access a variety of network services without having to repeatedly enter their credentials thanks to this TGT. This streamlines access control management and enhances user experience. Users show their TGT to the KDC in order to receive a service ticket, which contains session keys that provide safe communication between the client and the service, when they wish to access a particular service. Kerberos provides an additional layer of security to transactional systems by facilitating identity verification and trust formation between clients, servers, and intermediates. This improves overall transaction security by thwarting impersonation attempts, unauthorized access, and data manipulation.

2. AUTHENTICATION PROCEDURES:

2.1 DIFFIE-HELLMAN ALGORITHM

When exchanging data over a public network, the Diffie-Hellman algorithm is used to establish a shared secret that can be used for secret communications. The secret key is obtained by negotiating a large prime number n with B, where m is the modulus n's origin. The elliptic curve is used to generate points.

A and B can negotiate the two certificates even if the path is dangerous because they don't have to be secret. They are usable for multiple users at once.

The value of mxy mod n is the same for both d and d'. Even the people listening in on the other end of the line are unable to determine the value; all they know is n, m, x, and y. It will be meaningless until they compute the discrete logarithm and have a recovery of x and y. Consequently, d is the secret key between A and B that was independently determined.

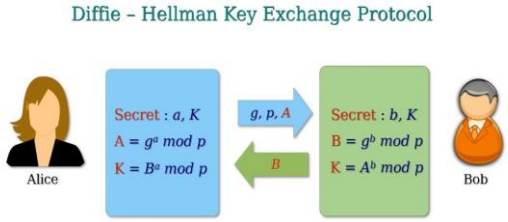

Fig 2. Diffie-Hellman protocol for key exchange

2.2 TOKEN

In identity management systems, a token serves as a system construct embodying the claimed subject or identity, encapsulating various identity attributes. One widely adopted and meticulously defined token format is the JSON Web Token (JWT). JWT establishes fundamental principles and structures for tokens, while the JSON Web Encryption (JWE) standard outlines the procedures for encrypting and decrypting JWT tokens. The method of signing a JWT token and then validating the signature is outlined in the JSON Web Signature (JWS) specification. Furthermore, the cryptographic algorithms and keys used by JWE and JWS are defined by the JSON Web Algorithms (JWA) and JSON Web Key (JWK) standards, respectively.

Based on how they are presented, there are two main categories of tokens: Holder-of-Key tokens and Bearer tokens. Additionally, tokens are divided into Identity Tokens and Access Tokens schemes according to their respective purposes. This all-inclusive architecture guarantees a clear and safe method for using and maintaining tokens in identification systems.

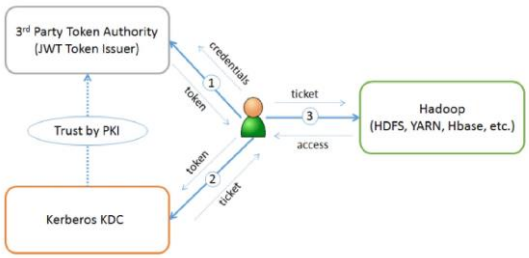

Fig 3. Token authentication based on Kerberos

2.3 WATERMARK EMBEDMENT TO BIOMETRICS

In the proposed BKAP (Biometric Key Authentication Protocol), smartphones with adequate computing capabilities and internal cameras are assumed to be available to users. The authentication process involves the use of both user fingerprints and smartphone information. The KDC (Key Distribution Center) database securely stores fingerprint references linked to mobile numbers and hashed serial numbers

The hashed mobile serial number is used to create a watermark, which is used to link the user's fingerprint to the mobile device. This watermark is embedded into the fingerprint during image acquisition, with the entire process, including fingerprint acquisition, watermark generation, and embedding, being performed using the internal functions of smartphones. The watermark embedding key is derived from the session key generated by the KDC. Any sufficiently secure and unobtrusive watermark technology can be employed for this purpose.

It is essential that the fingerprint features are significantly corrupted by the presence of the watermark. In case of a positive match, the watermark needs to be accurately removed from the watermarked image using the valid key. Incorrect removal of the watermark can result in a different set of fingerprint features. Consequently, if the data needed to remove the watermark is inaccurate or insufficient, the fingerprint matching procedure may be jeopardized and a positive match cannot be obtained.

50 fingerprint images from FVC2002 database are chosen randomly as host images. A 32bit number corresponding to the first 32 bits of the SHA-2 hash of a mobile serial number and timestamp is converted into binary, then used as watermark embeds to the host images. One fingerprint is shown in Figure (a), a watermark is shown in (b). The watermarked fingerprint is shown in (c). If detecting watermark with the valid key, the same watermark as that in (b) will be obtained. Otherwise, a completely different watermark will be detected without the correct key, this is shown in (d).

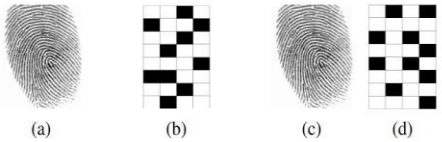

Fig 4. (a) Fingerprint (b) Watermark (c) Watermarked fingerprint (d) Watermark detected without correct key

2.4 TH-KBBA FOR SECURED DATA ACCESS

In the realm of Cloud computing, the security of data access is a critical concern, primarily due to the potential risk of unauthorized users gaining access to sensitive information. To address this issue, a robust authentication mechanism known as THKBBA (Three-Phase Key-Based Biometric Authentication) has been introduced, aiming to elevate the overall security level during data retrieval from the cloud server.The TH-KBBA mechanism involves three key entities: a multitude of users, an Authentication Server (AS), and a Cloud Server (CS). The process unfolds as follows: users initiate requests to access cloud data from CS. Assuming responsibility for user verification, AS makes sure that access is only allowed to authenticated users. After the authentication process is completed, CS gives the user the services they have requested.

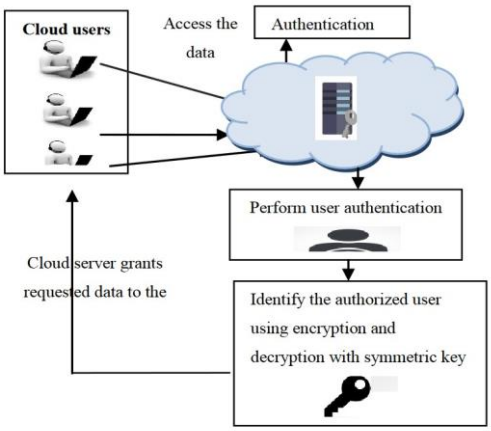

Fig 5. Flow process of TH-KBBA

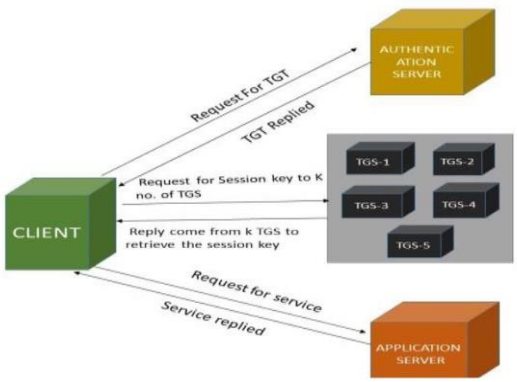

Fig 6. Threshold Cryptography

In second phase, AS verifies user as authenticated or unauthorized. Finally CS grants user requested services through ticket generation. The three phases are described as follows,

Registration phase: In order for the TH-KBBA Mechanism to proceed, the user must register his or her details with the server during this initial step.

2.5 Threshold Cryptography

Threshold cryptography provides increased security by chunking sensitive data. This approach splits the data D into n segments, where the secret information D needs to be reconstructed from at least m segments (where m < n). Segments smaller than m can't figure out what the secret is. This kind of configuration is sometimes called a (m, n) threshold scheme.

The cornerstone of threshold cryptography is a threshold cryptosystem, which encrypts data and distributes it around a robust computer network to protect it. A public key is used to encrypt the message, and the relevant private key is distributed to the allowed parties. In a threshold cryptosystem, multiple parties (exceeding a predefined threshold) must collaborate in the decryption or signature protocol to decrypt an encrypted message or sign a message.

Our protocols are designed to ensure security in the presence of an adversary corrupting at most t servers, where t is less than n/3. Although it's feasible to enhance fault-tolerance to t < n/2, we've prioritized simplicity over achieving the optimal threshold. Threshold cryptography stands out as one of the most secure techniques for conducting cryptographic operations. In the realm of computer science, cryptography focuses on securely accessing and transferring information among multiple parties, free from external interference. The significance of cryptography extends beyond the virtual realm into the real world, emphasizing the importance of safeguarding information and secrets from potential adversaries. In practical terms, cryptographic techniques contribute to establishing secure ecosystems capable of functioning reliably, whether or not trusted entities are actively involved.

3. Technological advancements:

Transactional authentication with Kerberos has advanced technologically to meet the growing cybersecurity threats. An additional layer of protection is added when Multi-Factor Authentication (MFA) is integrated with Kerberos, requiring users to authenticate themselves using different ways. By safely storing Kerberos tickets,

smart card integration improves authentication, and single sign-on (SSO) solutions provide a seamless and safe user experience across several services. Advanced Encryption Standards (AES) are used to ensure that Kerberos tickets are securely encrypted. Secure authentication across several domains is made possible by identity federation technologies like OAuth and SAML. A secure authentication environment must be maintained by patching and updating the Key Distribution Center (KDC) software on a regular basis, putting in place systems for continuous monitoring and logging, and adhering to secure coding practices. A comprehensive and robust security posture is further enhanced by the integration of privilege management technologies and token-based authentication for online services. Adopting a zero-trust security paradigm highlights the significance of maintaining constant watchfulness, authenticating users and devices, and following the least privilege principle in transactional authentication systems.

4. Advantages:

There are many benefits associated with Kerberos when it comes to transactional authentication. First of all, it presents Single Sign-On (SSO), which improves user comfort and overall security by simplifying user access to several services following a single authentication event. Strong encryption techniques are used by the protocol to safeguard login credentials and reduce the possibility of eavesdropping and unwanted access. In order to reduce the amount of time that potential attackers are exposed, Kerberos uses a ticket-based system to issue time-limited tickets for particular service access.

Additionally, Kerberos guarantees mutual authentication, confirming the legitimacy of the client and server's identities and lowering the possibility of man-in-the-middle attacks. A dedicated authentication server makes centralized management easier by streamlining the maintenance of user accounts and access limitations. Credential delegation is supported by Kerberos, enabling services to safely access resources on behalf of users. It also supports cross-realm authentication, which allows for seamless access between various Kerberos realms. Particularly in enterprise-level deployments, Kerberos is a flexible and broadly applicable solution for secure transactional authentication because of its scalability, open standards compliance, and connection with Active Directory. Nevertheless, cautious setup, administration, and observance of security best practices are necessary for a successful deployment.

5. Future trends:

In the dynamic landscape of transactional authentication, upcoming trends are expected to center around heightened security measures, incorporating cutting-edge technologies like biometrics, multi-factor authentication (MFA), and adaptive authentication to bolster the authentication process against evolving cyber threats. The adoption of the Zero Trust security model is likely, emphasizing continuous verification and the imperative for authentication in all transactions, even within trusted networks. Blockchain technology may be integrated into transactional authentication systems to enhance security and transparency. Cloud integration is anticipated to rise, providing scalability and flexibility, while efforts to enhance user experience aim to streamline authentication processes. The Kerberos protocol is likely to undergo improvements to address vulnerabilities and align with modern technologies. Ongoing standardization efforts will ensure interoperability, and risk-based authentication mechanisms will be implemented to dynamically adjust security levels based on transaction-specific risks. Machine

learning and artificial intelligence will play a crucial role in analyzing user behavior, while compliance with evolving data protection regulations and compatibility with emerging technologies, such as the Internet of Things and edge computing, will shape the trajectory of transactional authentication in the future.

6. CONCLUSION:

In summary, Kerberos-based transactional authentication presents a reliable and well-established approach to fortifying security in transactional settings. Through the implementation of mutual authentication and the use of cryptographic tickets, it establishes a secure trust relationship between entities, safeguarding sensitive data during communication. This overview delves into the foundational aspects of Kerberos and its application in transactional scenarios, underscoring its significance in today's security-focused landscape.

To conclude, the authentication framework for transactions utilizing Kerberos provides a robust and scalable solution tailored for securing transactions in distributed environments. Capitalizing on the inherent strengths of the Kerberos protocol, this framework ensures potent authentication, integrity, and confidentiality measures, all while mitigating computational overhead and ensuring smooth transaction processing. The proposed framework stands as a valuable contribution to elevating the security and efficiency of networked systems, rendering it suitable for diverse applications that demand secure transactional communication.

REFERENCES:

1. G. Thawre, N. Bahekar and B. R. Chandavarkar, "Use Cases of Authentication Protocols in the Context of Digital Payment System," *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Kharagpur, India, 2020, pp. 1-6, doi: 10.1109/ICCCNT49239.2020.9225428.

2. K. Zheng and W. Jiang, "A token authentication solution for hadoop based on kerberos pre-authentication," *2019 International Conference on Data Science and Advanced Analytics (DSAA)*, Shanghai, China, 2019, pp. 354-360, doi: 10.1109/DSAA.2019.7058096.

3. K. M. Prabha and P. V. Saraswathi, "TIGER HASH KERBEROS BIOMETRIC BLOWFISH USER AUTHENTICATION FOR SECURED DATA ACCESS IN CLOUD," *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on*, Palladam, India, 2018, pp. 145-151, doi: 10.1109/I-SMAC.2018.8653713.

4. M.R. Sutradhar, N. Sultana, H. Dey and H. Arif, "A New Version of Kerberos Authentication Protocol Using ECC and Threshold Cryptography for Cloud Security," *2018 Joint 7th International Conference on Informatics, Electronics & Vision (ICIEV) and 2018 2nd International Conference on Imaging, Vision & Pattern Recognition (icIVPR)*, Kitakyushu, Japan, 2018, pp. 239-244, doi: 10.1109/ICIEV.2018.8641010.

5. M. Jaiganesh and B. Ramdoss, "Security management in Kerberos V5 for GSM network," *2018 International Conference on Computing, Communication and Networking*, Karur, India, 2018, pp. 1-7, doi: 10.1109/ICCCNET.2018.4787777.

- 6. S. T. F. Al-Janabi and M. A. -s. Rasheed, "Public-Key Cryptography Enabled Kerberos Authentication," *2017 Developments in E-systems Engineering*, Dubai, United Arab Emirates, 2017, pp. 209-214, doi: 10.1109/DeSE.2017.16.
- 7. F. Han, M. Alkhathami and R. Van Schyndel, "Biometric-Kerberos authentication scheme for secure mobile computing services," *2017 6th International Congress on Image and Signal Processing (CISP)*, Hangzhou, China, 2017, pp. 1694-1698, doi: 10.1109/CISP.2017.6743949.