Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 7, July : 2024

ANONYMOUS IDENTITY BASED AUTHENTICATION AND KEY AGREEMENT

[1] ELLINENI ANANTHALAKSHMI, [2] MR. K. JAYA KRISHNA
[1] PG Scholar in the department of MCA at QIS College of Engineering & Technology (AUTONOMOUS), Vengamukkapalem, Ongole- 523272, Prakasam Dt., AP., India.
[2]Professor in the department of MCA at QIS Collegeof Engineering & Technology (AUTONOMOUS), Vengamukkapalem, Ongole- 523272, Prakasam Dt., AP., India.

ABSTRACT:

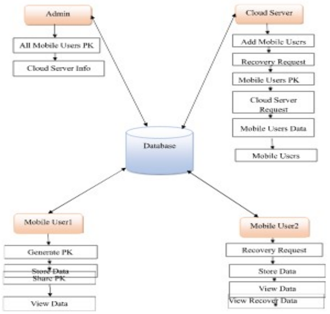
Anonymous identity-based authentication and key agreement (AIBAKA) is a cryptographic protocol designed to provide secure and privacy-preserving communication between parties in a networked environment. Unlike traditional authentication schemes that require users to disclose their identities, AIBAKA allows users to authenticate themselves to each other without revealing their identities to third parties. This is achieved through the use of identity-based cryptography, where users' identities are derived from publicly known information such as email addresses or usernames. Additionally, AIBAKA facilitates the establishment of shared secret keys between authenticated parties, enabling secure communication channels while preserving anonymity. This paper presents an overview of the AIBAKA protocol, its security properties, and its applications in various networked environments, highlighting its effectiveness in ensuring confidentiality, integrity, and anonymity in communication systems.

INDEX:AIBAKA protocol, identity, based, encryption.

INTRODUCTION:

In today's interconnected world, ensuring secure and private communication is paramount to safeguarding sensitive information and maintaining user privacy. Traditional authentication and key agreement protocols often require users to disclose their identities during the authentication process, raising concerns about privacy and anonymity. In response to these challenges, anonymous identity-based authentication and key agreement (AIBAKA) protocols have emerged as a promising solution for enabling secure communication while preserving user anonymity. AIBAKA protocols allow users to authenticate themselves to each other without revealing their actual identities to third parties or intermediaries, thereby enhancing privacy and confidentiality in communication systems. The proliferation of digital communication channels has led to increased concerns regarding user privacy and data security. Traditional authentication mechanisms typically rely on users' identities, such as usernames or public keys, to verify their authenticity. However, this approach often entails the disclosure of sensitive information, compromising user privacy and anonymity. AIBAKA protocols address this challenge by decoupling identity verification from actual identity disclosure, allowing users to authenticate themselves based on derived identity strings without revealing their true identities. This not only enhances user privacy but also mitigates the risk of identity theft and unauthorized access to sensitive information. Moreover, anonymity plays a crucial role in various applications where users seek to communicate without revealing their identities, such as whistleblowing, anonymous feedback systems, and privacy-preserving social networks.

SYSTEM ARCHITECTURE :



METHODOLOGY :

The development of anonymous identity-based authentication and key agreement (AIBAKA) involves several key modules designed to facilitate secure and privacy-preserving communication between parties in a networked environment. These modules include:

Identity Setup: In this module, a trusted authority or key generation center is responsible for generating public and private parameters and assigning unique identity strings to users. This process typically involves the creation of a master secret key and the derivation of users' identity strings from publicly known information such as email addresses or usernames.

Authentication: The authentication module enables users to prove their identities to each other without disclosing their actual identities to third parties or intermediaries. Users authenticate themselves based on their identity strings, which are derived from publicly known information, eliminating the need for pre-registered public keys or certificates.

Key Agreement: The key agreement module facilitates the establishment of shared secret keys between authenticated parties, enabling secure communication channels while preserving anonymity. Authenticated users derive shared secret keys based on their identity strings and the public parameters generated during the setup phase.

Anonymous identity-based authentication and key agreement are crucial in secure communication, especially in privacy-preserving applications. Here's a high-level overview of the methodology:

Anonymous Identity-Based Authentication:

1. Public Key Cryptography: Each user has a public-private key pair.
2. Identity-Based Encryption: A trusted authority generates a private key based on the user's identity (e.g., username or email).
3. Zero-Knowledge Proofs: The user proves ownership of the private key without revealing their identity.

Key Agreement:

1. Diffie-Hellman Key Exchange: Users exchange public keys to establish a shared secret key.
2. ** Elliptic Curve Cryptography**: Uses the difficulty of the elliptic curve discrete logarithm problem to ensure security.

Anonymous Authentication Protocols:

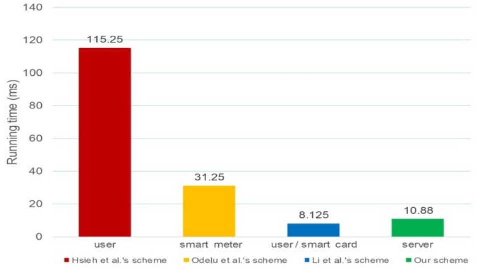
1. Anonymous Credentials: Users obtain credentials from an issuer without revealing their identity.
2. Anonymous Authentication: Users authenticate using their credentials without revealing their identity.

Some popular protocols that achieve anonymous identity-based authentication and key agreement include:

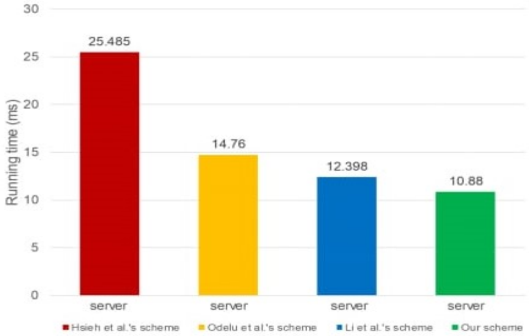
1. Anonymous Credentials (AC) protocol
2. Public-Key Cryptography (PKC) protocol
3. Secure Multi-Party Computation (SMPC) protocol
4. Zero-Knowledge Proof (ZKP) protocol

These protocols ensure secure authentication and key agreement while maintaining user anonymity. However, it's important to note that implementing these protocols requires expertise in cryptography and security.

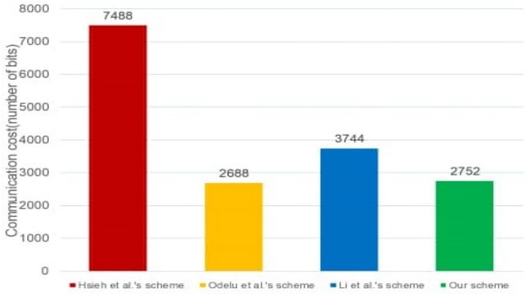
RESULTS ANALYSIS :



Computational costs comparisonSponsor side



Computational costs comparisonResponder side



Communication cost comparison

CONCLUSION :

In conclusion, anonymous identity-based authentication and key agreement (AIBAKA) protocols represent a significant advancement in the field of secure communication, offering a practical solution for balancing the conflicting requirements of authentication and privacy. Through the decoupling of identity verification from actual identity disclosure, AIBAKA protocols enable users to authenticate themselves and establish secure communication channels without revealing their identities to third parties or intermediaries. This not only enhances user privacy and confidentiality but also mitigates the risk of identity theft and unauthorized access to sensitive information, making AIBAKA protocols well-suited for deployment in diverse networked environments. Furthermore, the adoption of AIBAKA protocols has the potential to foster a more transparent and trustworthy communication ecosystem, where users can interact with confidence knowing that their privacy and confidentiality are protected. By providing users with greater control over their identities and personal information, AIBAKA protocols empower individuals to engage in secure and private communication, thus contributing to the overall security and resilience of digital communication systems. Moving forward, continued research and development in AIBAKA protocols are essential to address emerging threats and challenges in communication security, ensuring that users can communicate safely and anonymously in an increasingly interconnected world.

FUTURE ENHANCEMENT :

Zero-Knowledge Proof Integration: Integrate zero-knowledge proofs (ZKPs) to enhance privacy in authentication. ZKPs allow one party (the prover) to prove to another party (the verifier) that a statement is true without revealing any information beyond the validity of the statement itself. This could enable users to authenticate themselves without disclosing their actual identities.
Attribute-Based Authentication: Enhance the AIBAK system to support attribute- based authentication, where access decisions are based on specific attributes of the user rather than their identity. This can provide finer-grained access control and better privacy protection.

Revocation Mechanisms: Implement efficient mechanisms for revoking access in AIBAK systems. This could include the ability to revoke anonymous credentials or keys in case of compromise or loss, without revealing the user's identity.

Distributed Ledger Technology (DLT) Integration: Explore the use of distributed ledger technology (e.g., blockchain) to securely store and manage anonymous credentials or keys. DLT can provide tamper-resistant storage and decentralized management, enhancing security and trust in the AIBAK system.

Scalability Improvements: Develop techniques to improve the scalability of AIBAK systems, especially in scenarios with a large number of users or devices. This could involve optimizing cryptographic operations, reducing communication overhead, or leveraging distributed computing resources.

Post-Quantum Security: Research and implement post-quantum cryptographic primitives to ensure the long-term security of AIBAK systems against quantum attacks. As quantum computing advances, it's important to future-proof the system's cryptographic algorithms.

Interoperability Standards: Define and promote interoperability standards for AIBAK systems to facilitate seamless integration with existing authentication frameworks and protocols. This can simplify deployment and interoperability across different platforms and environments.

User-Centric Design: Focus on user-centric design principles to improve the usability and user experience of AIBAK systems. This includes intuitive interfaces, clear feedback mechanisms, and support for accessibility features.

Continuous Authentication: Explore continuous authentication techniques that continuously monitor user behavior and dynamically adjust authentication levels based on risk factors. This can enhance security while minimizing user friction.

Formal Verification: Apply formal verification techniques to rigorously analyze the security properties of AIBAK systems and ensure their correctness with respect to specified security requirements. This can provide strong guarantees against potential vulnerabilities or attacks.

Privacy-Preserving Protocols: Research and develop privacy-preserving protocols for AIBAK systems that minimize the amount of sensitive information exposed during authentication and key agreement processes. This can help protect user privacy against unauthorized access or surveillance.

By incorporating these future enhancements, AIBAK systems can become more secure, scalable, privacy-preserving, and user-friendly, addressing the evolving needs and challenges of modern authentication and key agreement scenarios.

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, June 2023, 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.

21. 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.

22. Veldandi Srikanth, et al. "Human-AI Interaction Using 3D AI Assistant" International Conference on Emerging Advances and Applications in Green Energy (ICEAAGE-2024), 15, Feb 2024, https://www.researchgate.net/publication/380971799_ICEAAGE-2024_Conference_Proceedings_Final

23. Veldandi Srikanth, et al. "Voice Based Assistance for Traffic Sign Recognition System Using Convolutional Neural Network"

International journal of advance and applied research (IJAAR) ISSN – 2347-7075, 4th, April 2024, https://ijaar.co.in/wp-content/uploads/2021/02/Volume-5-Issue-4.pdf

24. Veldandi Srikanth, et al. "Convolutional Neural Network Based Heart Stroke Detection" International journal of advance and applied research (IJAAR) ISSN – 2347-7075, 4th, April 2024, https://ijaar.co.in/wp-content/uploads/2021/02/Volume-5-Issue-4.pdf

25. Srikanth veldandi, et al. "Data Analytics Using R Programming Lab | IOK STORE." IOK STORE, ww.iokstore.inkofknowledge.com/product-page/data-analytics-using-r-programming-lab.

26. Srikanth veldandi, et al. "Data Structures Laboratory Manual | IOK STORE." IOK STORE, www.iokstore.inkofknowledge.com/product-page/data-structures-laboratory-manual.

27. Srikanth veldandi, et al. "Cyberspace and The Law: Cyber Security | IOK STORE." IOK STORE, iokstore.inkofknowledge.com/product-page/cyberspace-and-the-law.

AUTHOR PROFILE:

Mr. K. Jaya Krishna, currently working as an Associate Professor in the Department of Master of Computer Applications, QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He did his MCA from Anna University, Chennai, M.Tech (CSE) from JNTUK, Kakinada. He published more than 10 research papers in reputed peer reviewed Scopus indexed journals. He also attended and presented research papers in different national and international journals and the proceedings were indexed IEEE. His area of interest is Machine Learning, Artificial intelligence, Cloud.Computing.and.Programming Languages.

Ms. EllineniAnanthalakshmi, currently pursuing Master of Computer Applications at QIS College of engineering and Technology (Autonomous), Ongole, Andhra Pradesh. She Completed B.Sc. in Physics from AbhyudayaMahila Degree College, Guntur, Andhra Pradesh. Her areas of interest are Cloud computing. & Java.