Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 8, August : 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] Associate Professor in the department of MCA at QIS College of 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.

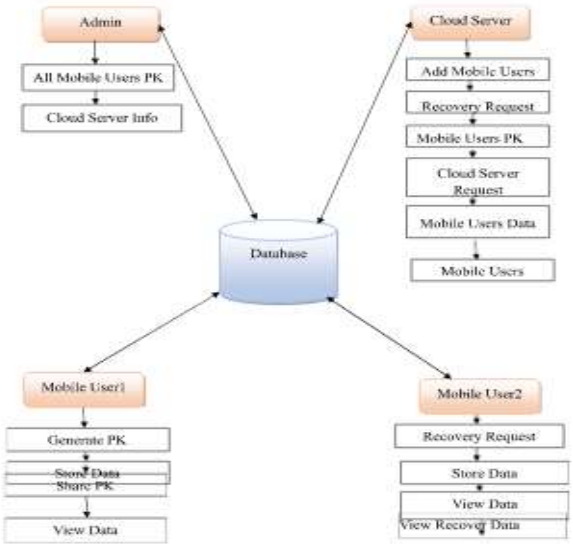
INTRODUCTION:

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.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 8, August : 2024

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.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 8, August : 2024

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:

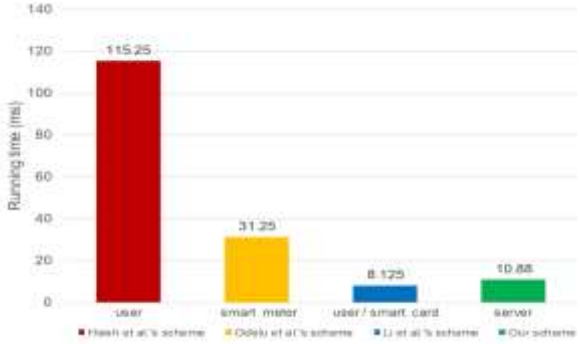
1. Anonymous Credentials: Users obtain credentials from an issuer without revealing their identity.
2. Anonymous Authentication: Users authenticate using their credentials without revealing their identity.

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

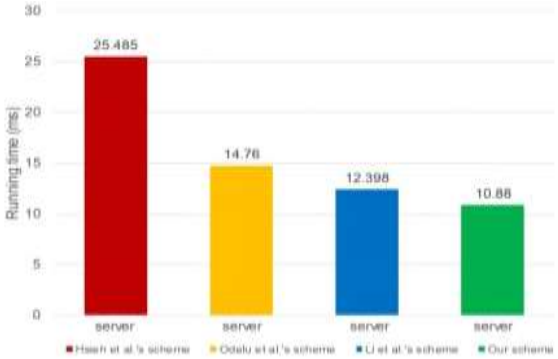
1. Anonymous Credentials (AC) protocol
2. Public-Key Cryptography (PKC) protocol
3. Secure Multi-Party Computation (SMPC) protocol
4. Zero-Knowledge Proof (ZKP) protocol

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

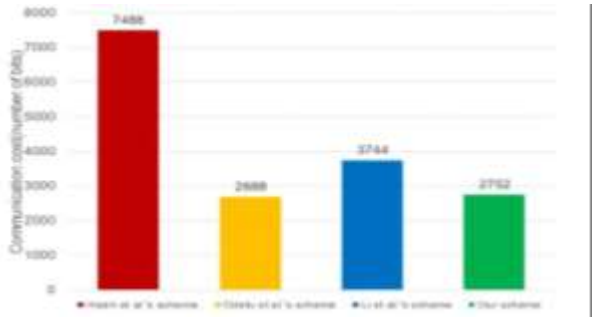


Computational costs comparison Sponsor side



Computational costs comparison Responder side

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 8, August : 2024



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. M. Bellare and P. Rogaway, "Entity authentication and key distribution," in Advances in Cryptology - EUROCRYPT'93, Springer-Verlag, 1994.
2. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology - CRYPTO'84, Springer-Verlag, 1985.
3. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Advances in Cryptology - CRYPTO'2001, Springer-Verlag, 2001.
4. D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Communications of the ACM, vol. 24, no. 2, pp. 84-88, 1981.
5. M. Blaze, "Divertible protocols and atomic proxy cryptography," in Proceedings of the 1998 IEEE Symposium on Security and Privacy, IEEE Computer Society, 1998.
6. B. Parno, J. Howell, C. Gentry, and M. Raykova, "Pinocchio: Nearly practical verifiable computation," in Proceedings of the 2013 IEEE Symposium on Security and Privacy, IEEE Computer Society, 2013.
7. Y. Dodis and A. Yampolskiy, "A verifiable random function with short proofs and keys," in Advances in Cryptology - EUROCRYPT'05, Springer-Verlag, 2005.
8. J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in Proceedings of the 2001 International Conference on the Theory and Applications of Cryptographic Techniques, Springer-Verlag, 2001.
9. J. Benaloh and M. de Mare, "One-way accumulators: A decentralized alternative to digital signatures," in Advances in Cryptology - EUROCRYPT'93, Springer- Verlag, 1994.
10. D. Beaver, S. Micali, and P. Rogaway, "The round complexity of secure protocols," in Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, ACM Press, 1990.
11. M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in Proceedings of the 1st ACM Conference on Computer and Communications Security, ACM Press, 1993.
12. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in Advances in Cryptology - CRYPTO'86, Springer- Verlag, 1987.
13. Libert, T. Peters, and M. Yung, "Scalable anonymous group communication in the asynchronous and adaptive adversary model," in Proceedings of the 2010 IEEE Symposium on Security and Privacy, IEEE Computer Society, 2010.
14. Cachin, K. Kursawe, and V. Shoup, "Random oracles in Constantinople: Practical

asynchronous Byzantine agreement using cryptography," in Proceedings of the 19th Annual ACM Symposium on Principles of Distributed Computing, ACM Press, 2000.

15. G. Brassard, D. Chaum, and C. Crepeau, "Minimum disclosure proofs of knowledge," Journal of Computer and System Sciences, vol. 37, no. 2, pp. 156- 189, 1988.

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 Languag es.

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