# ROBUST KEY AGREEMENT FRAMEWORK USING DYNAMIC IDENTITY-BASED AUTHENTICATION

[1]*Pranay Kumar,*[2]*Sarojini.P,*[3]*Sravana Bhargavi*
[123]*Students*
*Department Of Computer Science And Engineering*

**ABSTRACT**

With the exponential growth of interconnected systems and remote communications, ensuring secure and authenticated data exchange is a critical concern in modern digital infrastructures. This paper presents a robust key agreement framework based on dynamic identity-based authentication, designed to provide lightweight, efficient, and scalable security in distributed environments such as IoT, wireless sensor networks, and mobile cloud systems. The proposed protocol leverages dynamic identities and session-based key generation to enhance user privacy, prevent identity theft, and resist various attacks, including replay, impersonation, and man-in-the-middle attacks. Formal security analysis and performance evaluation demonstrate that the framework achieves strong mutual authentication, forward secrecy, and low computational overhead, making it suitable for real-time, resource-constrained applications. The scheme is further validated using formal verification tools to ensure its provable security properties, establishing it as a practical solution for secure key exchange in decentralized systems.

## I. INTRODUCTION

In today's hyper-connected digital landscape, secure communication and identity verification are foundational to the protection of user data, system integrity, and privacy. Traditional static identity-based authentication schemes have proven vulnerable to various security breaches, such as identity spoofing, session hijacking, and replay attacks. As a result, dynamic identity-based authentication has emerged as a promising solution, providing users with changing pseudonymous credentials that improve security without compromising performance.

Key agreement protocols, which allow two or more parties to securely establish a shared secret key over an insecure channel, are essential for enabling encrypted communication. However, the challenge lies in developing protocols that are not only secure but also lightweight and resistant to modern cryptographic attacks—particularly in low-power, real-time environments like IoT networks, mobile platforms, and smart grid systems.

This paper introduces a robust key agreement framework that incorporates dynamic identity-based authentication to enhance user anonymity and strengthen resistance against common attack vectors. The proposed protocol focuses on mutual authentication, forward secrecy, and efficient session key generation, using minimal cryptographic operations to ensure computational feasibility. The system is designed to scale well in diverse network environments and complies with current security standards. A comprehensive analysis of the protocol's security features, computational efficiency, and resistance to known attacks is also presented.

## II. SYSTEM ANALYSIS

### EXISTING SYSTEM

Despite the many research efforts done for the DIDAKA protocols, designing a protocol that can fulfil both desired efficiency and security features is still a challenging task. In 2004, Das et al. [15] proposed a dynamic ID-based remote user authentication scheme using smart card. In 2009, Wang et al. [16] indicated that [15] does not provide mutual authentication and is susceptible to the impersonation attack.

Accordingly, they proposed an enhanced scheme. However, in 2011, Khurram Khan et al. [17] showed that [16] does not provide anonymity and session key agreement and does not support smart card revocation. Another DIDAKA scheme presented by Liao and Wang [18] in 2009 for multiserver environments.

However, at the same year, Hsiang and Shih [19] indicated that [18] suffers from the insider and masquerade attacks and fails to provide mutual authentication. Afterwards, they proposed an improved protocol; nonetheless, in 2011, Lee et al. [20] demonstrated that [19] cannot resist the masquerade attack and cannot provide mutual authentication. In 2012, Wen and Li [21] presented another ID-based AKA protocol. However, Tang and Liu [22] demonstrated the susceptibility of [21] against the offline password guessing and impersonation attacks. In 2013, Li et al. [23] showed that [20] still cannot provide mutual authentication and is susceptible to some attacks. Further, in 2013, Qu and Zou [24] indicated that [21] does not provide anonymity and perfect forward secrecy. In 2014, Islam and Biswas [25] presented another ID-based AKA protocol. Nevertheless, in 2015, Sarvabhatla and Vorugunti [26] indicated that [25] cannot resist the impersonation and offline password guessing attacks. Additionally, an efficient DIDAKA scheme presented by Lin [27] in 2014; nevertheless, their scheme fails to provide the desired security features, such as perfect forward secrecy.

In 2015, Shunmuganathan et al. [28] showed that [23] is vulnerable to both the offline password guessing and stolen smart card attacks and accordingly, they presented an enhanced protocol. However, recently, Jangirala et al. [29] have indicated that [28] also fails to withstand the offline password guessing, impersonation, and stolen smart card attacks and cannot provide perfect forward secrecy. Furthermore, Chaturvedi et al. [30] proposed an enhanced DIDAKA protocol; nonetheless, careful consideration of their work indicates that it cannot totally provide the desired security properties. Recently, Xie et al. [14] have presented a novel DIDAKA protocol with an extended security model. Nonetheless, we found that their scheme cannot resist the known session-specific temporary information, denial of service, and key compromise impersonation attacks.

**Disadvantages**

- ❖ An existing methodology doesn't implement Authenticating server and checking message integrity method.
- ❖ The system not implemented Key Compromise Impersonation Attack (KCIA).

**Proposed System**

In order to double check the resistance of the proposed DIDAKA protocol against the various attacks, such as impersonation, key compromise impersonation (KCI), known session-specific temporary information (KSSTI), modification, injection, replay, and offline password guessing attacks and further, to verify the provision of the strong anonymity and perfect forward security (PFS), in this section, we take the advantage of a powerful tool called ProVerif [40]. This tool not only is able to check the "reachability properties," but also can validate the "correspondence assertions" or "observational equivalences."

As a result, it has grasped noticeable attention from the academia. Nonetheless, most scholars just use its very basic capabilities. Fig. 4 illustrates the implementation of the proposed protocol in the ProVerif input language besides the obtained results. As can be seen in the proposed system, unlike the previous works that have just employed the basic capabilities of ProVerif, we have utilized its advanced features.

In the proposed system, the first result is the result of a reachability query, which proves the secrecy of the generated session key; the second

one is the result of an observational equivalence query, which corroborates the strong anonymity of user; the third one indicates the resistance against the offline password guessing attack; and eventually, the fourth and fifth ones are the results of two injective correspondence assertions that prove the replay, impersonation, and modification attacks resistance of the proposed protocol. Moreover, to demonstrate that the proposed protocol can provide the PFS and resist the KSSTI attack, respectively, we have made the long-term and ephemeral secrets available to attacker. Following, for the both cases, we have reran the model and checked the result of the first query, i.e., query attacker.SK• :

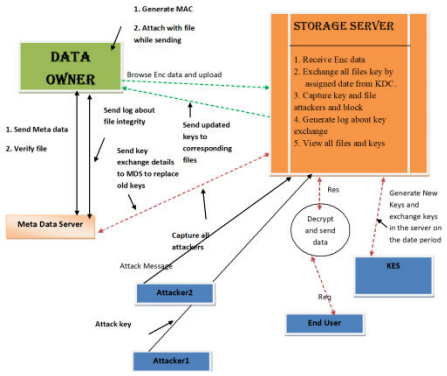
The results were again true that show the secrecy of session key will be still preserved in case of long-term or ephemeral secrets leakage. Finally yet significantly, in order to ensure the resistance against the KCI attack, we have disclosed the secrets of server to attacker. Since the fourth result was again true for this case, we become sure that in case of server secret keys leakage, an attacker cannot still impersonate user and hence, our scheme is resilient to the KCI attack.

**Advantages**

- ❖ The proposed system implements DYNAMIC ID-BASED AUTHENTICATED KEY AGREEMENT SCHEME method.
- ❖ The system implemented authenticating server and checking message integrity method.

## III. SYSTEM DESIGN

**SYSTEM ARCHITECTURE**




## IV. IMPLEMENTATION MODULES

**Data Owner**

In this module, client browse a file encrypt and upload to the router. Generates a mac address for the particular file while uploading and Sends meta data to meta data server

**Storage Server**

Receive encrypted data from client. Exchange all files key by assigned date from KES and Send updated keys to corresponding files, Send key exchange details to meta data server to replace old keys. Capture key and file attackers and block. Generate log about key exchange and View all files and keys, Decrypts the data and sends to the receiver

**KES**

Generate New Keys and exchange keys in the server on the date period

**Meta Data Server**

Data owner send meta data to keep copy of the file and Send log about file integrity and Capture all attackers

**Receivers—End User**

Request secret key and available files in the router, Request and receive decrypted files

**Attacker**

**Type-1** attacks secret key

**Type-2** injects malicious data and corrupts original file.

## V. CONCLUSION

The proposed robust key agreement framework using dynamic identity-based authentication addresses several critical security requirements for modern distributed systems. By dynamically updating user identities and employing lightweight cryptographic techniques, the protocol ensures mutual authentication, forward secrecy, resistance to replay and impersonation attacks, and low communication overhead.

Performance analysis and formal security verification confirm that the scheme is well-suited for resource-constrained environments such as IoT devices, wireless networks, and cloud-connected platforms. Additionally, the modular design allows for future integration with biometric systems, blockchain architectures, or quantum-resilient cryptographic primitives.

In conclusion, this dynamic ID-based approach offers a scalable, secure, and efficient solution for key agreement in decentralized and high-risk communication settings. Future work may involve deploying the protocol in real-world environments and enhancing it with AI-based anomaly detection to further secure communication channels.

## REFERENCES

[1] D. Abbasinezhad-Mood and M. Nikooghadam, “An Anonymous ECC-based Self-certified Key Distribution Scheme for the Smart Grid,” IEEE Transactions on Industrial Electronics, vol. 65, no. 10,
pp. 7996–8004, 2018.

[2] M. Masdari and S. Ahmadzadeh, “A Survey and Taxonomy of the Authentication Schemes in Telecare Medicine Information Systems,” Journal of Network and Computer Applications, vol. 87, pp.
1–19, 2017.

[3] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, “Authentication Protocols for Internet of Things: A Comprehensive Survey,” Security and Communication Networks, vol. 2017, 2017.

[4] D. Alrababah, E. Al-Shammari, and A. Alsuht, “A Survey: Authentication Protocols for Wireless Sensor Network in the Internet of Things; Keys and Attacks,” pp. 270–276, 2017.

[5] K.-A. Shim, “Basis: A Practical Multi-user Broadcast Authentication Scheme in Wireless Sensor Networks,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 7, pp. 1545–1554,
2017.

[6] H. Xiong and Z. Qin, “Revocable and Scalable Certificateless Remote Authentication Protocol with Anonymity for Wireless Body Area Networks,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 7, pp. 1442–1455, 2015.

[7] M. Masdari and S. Ahmadzadeh, “Comprehensive Analysis of the Authentication Methods in Wireless Body Area Networks,” Security and Communication Networks, vol. 9, no. 17, pp. 4777–4803,
2016.

[8] N. Saxena and B. J. Choi, “Authentication Scheme for Flexible Charging and Discharging of Mobile Vehicles in the V2G Networks,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 7, pp. 1438–1452, 2016.

[9] D. Abbasinezhad-Mood and M. Nikooghadam, “Design and Hardware Implementation of a Security-enhanced Elliptic Curve Cryptography Based Lightweight Authentication Scheme for Smart Grid Communications,” Future Generation Computer Systems, vol. 84, pp. 47–57, 2018.

[10] N. Saxena, B. J. Choi, and R. Lu, “Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 5, pp. 907–921, 2016.