DYNAMIC MULTI-KEY AUTHENTICATION FOR IOT SYSTEM USING SECURE VAULTS

Prof. Vinay M G[1], Firdushahin[2], Madan L[3], Mahesh Chandru C[4]

[1] *Assistant Professor, In science and Engineering, Vidya Vikas Institute of Engineering & Technology, Karnataka, India*
[2] *Student, Information science and Engineering, Vidya Vikas Institute of Engineering & Technology, Karnataka, India*
[3] *Student, Information science and Engineering, Vidya Vikas Institute of Engineering & Technology, Karnataka, India*
[4] *Student, Information science and Engineering, Vidya Vikas Institute of Engineering & Technology, Karnataka, India*
[5] *Student, Information science and Engineering, Vidya Vikas Institute of Engineering & Technology, Karnataka, India*

ABSTRACT

The Internet of Things (IoT) is rapidly advancing, bringing with it the need for robust and scalable security frameworks. This paper presents a novel Dynamic Multi-Key Authentication (DMKA) system, which uses secure vaults to enhance authentication in IoT environments. In this framework, users register with an authority node, which verifies the registration, generates a certificate, and creates multiple encryption keys using SHA and RSA algorithms. These certificates are stored in a secure cloud and accessed via Raspberry Pi-based systems. Upon request, the user presents the certificate and receives an OTP encrypted with a public key. If verified, a session key is issued to access the IoT device.

This system addresses major security issues like information leakage, unauthorized access, and poor reliability found in existing protocols. The approach is validated through a working prototype and systematic testing, demonstrating its reliability and efficiency.

This paper also explores future enhancements including AI-based threat detection and post-quantum cryptography integration.

Keyword: - IoT, Dynamic Multi-Key Authentication, Secure Vault, SHA, RSA, Certificate-Based Security

1. INTRODUCTION

The Internet of Things (IoT) refers to a network of physical objects embedded with electronics, software, sensors, and connectivity enabling them to collect and exchange data. Its vast applications span from healthcare and agriculture to smart cities and energy management. However, with such expansion comes a heightened concern over data security, privacy, and system reliability.

1. DYNAMIC MULTI-KEY AUTHENTICATION SYSTEM

1.1 About Internet of Things (IoT)

IoT systems allow devices to be sensed and controlled remotely, integrating physical systems into computer-based frameworks. By embedding technologies such as RFID, NFC, and cloud platforms, IoT has improved efficiency and accuracy while reducing human intervention.

1.2 Applications of IoT

IoT applications are categorized into consumer, enterprise, and infrastructure types. Examples include smart homes, industrial monitoring, agriculture automation, environmental sensing, and urban planning.

Growing IoT Ecosystem: The Internet of Things (IoT) connects billions of devices globally, ranging from sensors to smart appliances.Ensuring secure communication and authentication among these devices is a critical challenge.

Security Challenges in IoT: IoT devices often have limited computational power and storage, making traditional security solutions unsuitable.Static keys and centralized authentication mechanisms are prone to compromise, spoofing, and key theft.

Need for Advanced Authentication: Dynamic key-based approaches offer improved security by rotating keys regularly or based on behavior.Using multiple keys reduces the risk of single-point failures and key compromise.

Role of Secure Vaults: Secure Vaults are tamper-resistant storage modules that protect cryptographic materials inside IoT devices.They enable safe storage, usage, and lifecycle management of dynamic keys.

Proposed Approach: The dynamic multi-key authentication model uses a key engine to generate and manage multiple ephemeral keys.These keys are stored in Secure Vaults and used for mutual authentication between devices and servers.

2. METHODOLOGY

This section outlines the systematic approach followed in the design and implementation of a Dynamic Multi-Key Authentication as shown in Figure 1:

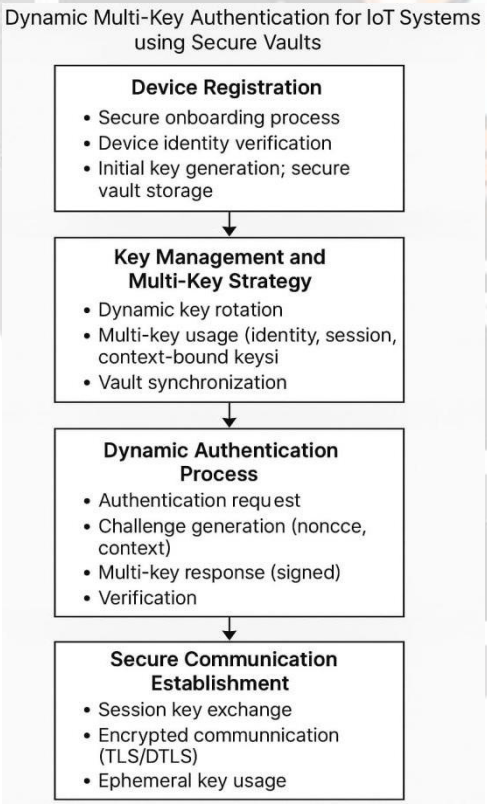


Fig -1: METHODOLOGY OF DYNAMIC MULTI-KEY AUTHENTICATION FOR IOT SYSTEM USING SECURE VAULTS

i. Device Registration and Initialization*

Each IoT device is initially registered within the system through a secure onboarding process. The process includes:

Device Identity Verification:* Unique identifiers (UUIDs or hardware-based identifiers) are used to register devices.

Initial Key Generation:* Upon registration, the system generates a set of cryptographic keys.

Key Management and Multi-Key Strategy

ii.Key Management and Multi-Key Strategy

Dynamic Key Rotation:* Keys are periodically rotated based on configurable policies (time interval, access frequency, behavioral metrics).

Multi-Key Usage:* Each authentication session uses a combination

iii.Dynamic Authentication Process.

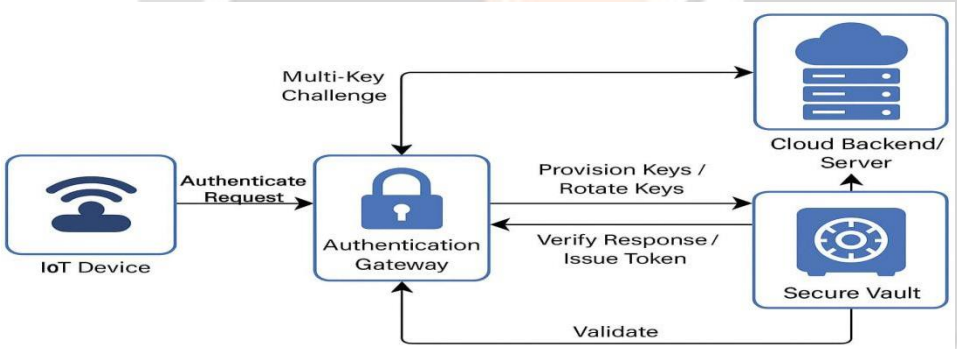
Authentication Request: The IoT device initiates an authentication request with a token or certificate.

Challenge Generation:The server generates a challenge including a nonce, timestamp, and contextual data (e.g., device location, usage pattern).

Multi-Key Response:* The device responds with a cryptographically signed message using its set of dynamic keys.

3. PROPOSED SYSTEM

The rapid proliferation of IoT devices introduces significant security challenges, especially in authentication Traditional static key mechanisms are insufficient against sophisticated attacks such as replay, impersonation, or key compromise.



3.1 System Architecture Overview

- The system architecture follows a modular design, as shown in Figure 4.1. Users first select an input type—Value- Based Input.
- IoT Devices: Lightweight, resource-constrained nodes (sensors, actuators, etc.)
- Authentication Gateway: Verifies identities and manages key exchanges.
- Secure Vault: Stores and manages cryptographic keys in a tamper-proof environment (e.g., HashiCorp Vault, Azure Key Vault, AWS KMS).
- Cloud Backend / Server: Performs analytics and centralized policy enforcement..

4. CONCLUSIONS AND FUTURE RESEARCH DIRECTIONS

The proposed Dynamic Multi-Key Authentication system leveraging Secure Vaults enhances the security and resilience of IoT environments. By dynamically generating and rotating multiple authentication keys, it significantly reduces the risk of key compromise and session hijacking. Secure Vaults ensure tamper-resistant key storage, providing strong protection even in hostile environments.

Future directions include integrating AI-driven anomaly detection to trigger adaptive key rotations, supporting cross-platform vault compatibility, and optimizing key generation for ultra-low-power IoT devices. Additionally, the approach can be extended to edge computing and federated IoT networks, enhancing security across distributed infrastructures while maintaining scalability and minimal latency.

5. REFERENCES

[1] MQTT based Secure Transport Layer Communication for Mutual Authentication in IoT Network, 2022

[2] Authentication, access control and scalability models in Internet of Things Security: A review, 2024

[3] A study of secure communication scheme in MQTT: TLS vs AES cryptography, 2022

[4] A Secure Network Architecture for Heterogeneous IoT Devices using Role-based Access Control, 2019

[5] Analysis of the Cryptographic Algorithms in IoT Communications, 2023

[6] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A Review," 2012 International Conference on Computer Science and Electronics Engineering, IEEE, 2012.

[7]A. H. Abdmeziem and D. Tandjaoui, "Internet of Things: Concept, Building blocks, Applications and Challenges," Computing, Communications and IT Applications Conference (ComComAp), IEEE, 2014.

[8] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," IEEE Internet of Things Journal, vol. 4, no. 5, 2017.

[9] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," Computer, vol. 44, no. 9, pp. 51–58, 2011.

[10] A. K. Das, "A Secure and Robust Temporal Credential-Based Three-Factor Authentication Scheme for Wireless Sensor Networks," Peer-to-Peer Networking and Applications, vol. 8, pp. 60–79, 2015.

[11] C. Bormann, A. P. Castellani, and Z. Shelby, "CoAP: An Application Protocol for Billions of Tiny Internet Nodes," IEEE Internet Computing, vol. 16, no. 2, pp. 62–67, 2012.

[12] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[13] Z. Yan, P. Zhang, and A. V. Vasilakos, "A Survey on Trust Management for Internet of Things," Journal of Network and Computer Applications, vol. 42, pp. 120–134, 2014.