Global and Stochastic Analysis
Vol. 13 No. 1 (2026)

http://dx.doi.org/10.64837/GSA.13.1.6

Received: 20th October 2025 *Revised: 10th January 2026* *Accepted: 21st th January 2026*

A GLOBAL STOCHASTIC PERSPECTIVE ON IOT DEVICE AUTHENTICATION USING DIGITAL CERTIFICATE MECHANISM FOR INTERNET OF THINGS (IOT) DEVICES

MALIKHAN SINGH, MEENA CHAUDHARY, AND ANSHU KUMAR DWIVEDI*

Abstract. The increased deployment of Internet of Things (IoT) has revolutionized global connectivity through applications such as smart cities, smart industries, healthcare systems, and industrial automation. However, resource-constrained IoT devices face severe security challenges, particularly in device authentication. Traditional authentication mechanisms based on symmetric and asymmetric cryptography introduce excessive communication and computation overhead, making them unsuitable for constrained IoT environments.

In this paper, we propose a secure and lightweight device authentication mechanism based on digital certificates from a global stochastic perspective. The proposed framework considers the dynamic and uncertain behavior of IoT networks while ensuring secure identification and communication. The protocol employs asymmetric cryptography, hash functions, nonces, and timestamps to prevent impersonation, replay, and device capture attacks. The security properties of the proposed protocol are formally verified using the AVISPA tool under the Dolev-Yao attacker model. Performance evaluation demonstrates low communication, storage, and computational overhead, making the proposed mechanism suitable for Industrial IoT, smart cities, defense systems, and other mission-critical IoT applications.

1. Introduction

The Internet of Things (IoT) has emerged as a transformative technology that interconnects billions of heterogeneous devices, enabling intelligent communication, automation, and data-driven decision-making. IoT applications span across smart cities, healthcare, home automation, industrial control systems, and defense environments.

Despite its rapid growth, IoT networks face significant security challenges due to limited computational resources, constrained memory, and low power availability of IoT devices. Among various security concerns, device authentication is a critical requirement to ensure that only legitimate devices participate in network communication.

Existing authentication schemes based on traditional symmetric and asymmetric cryptography often introduce high computational and communication overhead. Lightweight authentication schemes reduce overhead but may compromise security or trust management.

To overcome these limitations, this paper proposes a certificate-based authentication mechanism from a global stochastic perspective. The proposed solution enhances trust, scalability, and resilience in IoT ecosystems while maintaining lightweight operational requirements.

2. Related Work

Device authentication in IoT has been widely studied to address security and resource constraints.

Implicit certificate schemes such as ECQV reduce certificate size and computational overhead. Lee and Lee (2020) proposed lightweight authentication mechanisms using implicit certificates. However, revocation and trust management remain complex.

Hammi et al. (2017) introduced lightweight mutual authentication protocols based on symmetric cryptography. Although computationally efficient, these approaches lack strong non-repudiation properties.

Key words and phrases. IoT Security, Device Authentication, Digital Certificates, Lightweight Cryptography, AVISPA Analysis, Smart IoT Applications.

*Corresponding author.

Thungon et al. (2023) developed a certificate-based authentication scheme for 6LoWPAN IoT environments using ECC. While more efficient than RSA-based approaches, certificate handling and verification still impose overhead.

Garba et al. (2023) proposed LightCert4IoTs using blockchain-based certificate validation. However, blockchain dependency introduces latency and connectivity challenges.

Hummen et al. proposed TinyOSCP using Bloom filters for certificate revocation in constrained devices. Although energy efficient, it compromises detailed revocation information.

These limitations highlight the need for a simple, scalable, and secure certificate-based authentication mechanism tailored for IoT environments.

3. Proposed Mechanism

The proposed authentication framework consists of two phases:

- Registration Phase
- Authentication Phase

Notations.

- ID_{D1}, ID_{D2} : Identities of IoT devices
- S : Server
- PU_S, PR_S : Server public and private keys
- PU_{D1}, PR_{D1} : Keys of device $D1$
- PU_{D2}, PR_{D2} : Keys of device $D2$
- CD_1, CD_2 : Certificates
- N_1, N_2 : Nonces
- T_1 : Timestamp
- $h(\cdot)$: One-way hash function

3.1. **Registration Phase.** When a new IoT device joins the network, it must first register with the server(S) to obtain a digital certificate for secure communication and future authentication. This is done in the following way:

When IoT device (D1) sends the request to generate the certificate to the server (S). The request IoT device (D1) includes the Identity (ID_1) of the device, its public key (PU_{D1}) and the timestamp (T1), and these three elements are encrypted using the public key of the server (PUs). In addition, the public key of the server (PUs) was preloaded into the IoT device (D1) as a hardware key during deployment.

$$M_1 : D1 \rightarrow S : \{ID_{D1}, PU_{D1}, T_1\}_{PU_S} \tag{1}$$

The server decrypts the request with its private key. If it decrypts successfully, this means that the request was captured from a valid IoT device currently on the IoT server's network. The server will then generate a custom digital certificate (CD1) for the requesting IoT device 'D1'. The certificate will contain the identity of the IoT device (D1), the public key of the IoT device (PUD1), the issuer name (S), and the expiry (date and time) (EXP). The server signs the certificate with its private key.

$$CD_1 = (ID_{D1}, PU_{D1}, S, EXP)_{PR_S} \tag{2}$$

The server will then return the generated certificate (CD1) along with the updated (T1+1) encrypted with the server's private key to the original requesting node. In addition, the server will send the hash of the received timestamp encrypted with the IoT device's public key.

$$M_2 : S \rightarrow D1 : \{CD_1, T_1 + 1\}_{PR_S}, \{h(T_1)\}_{PU_{D1}} \tag{3}$$

The IoT device will decrypt the received message, compute the hash for the original timestamp (T1), and compare it to the hash that was encrypted for the returning timestamp (T1+1). If both hashes are the same, this guarantees that the certificate was created by the server. The IoT device will then store the certificate to use with the authentication phase, allowing the device to securely communicate with other IoT devices.

Therefore, all devices must go through the registration phase with the server to be able to get a valid digital certificate before they are aware of or authenticate any other devices in the network (as seen in Fig.1). This helps to ensure that only registered and legitimate devices access the IoT network.

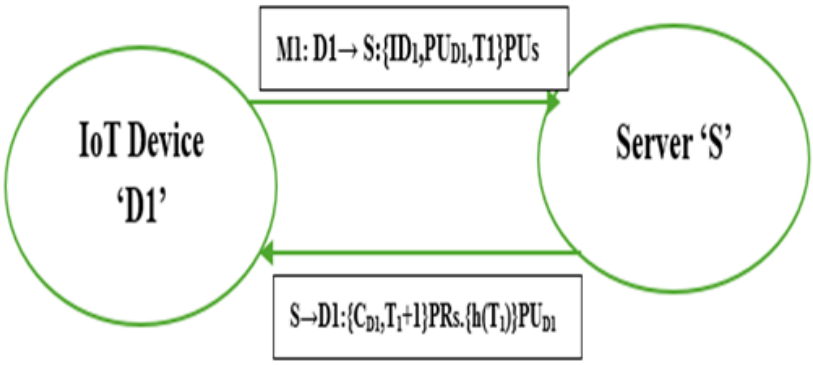

FIGURE 1. Registration Phase of Proposed Protocol

3.2. **Authentication Phase.** After completing the registration phase, IoT devices authenticate each other using the digital certificates issued by the server. The mutual authentication process between two IoT devices (D1 and D2) proceeds as follows:

IoT device 1 'D1' sends its identity (ID_1), its digital certificate (C_{D1}), and the current nonce (N_1), where N_1 is signed (encrypted) with D1's private key.

$$M_3 : D1 \rightarrow D2 : ID_{D1} \parallel CD_1 \parallel \{N_1\}_{PR_{D1}} \tag{4}$$

IoT Device 2 'D2' verifies the identity of D1. IoT device 2 decrypts C_{D1} using the server's public key (PUs). If successful, this represents that the certificate is generated by server only. IoT device 2 checks the expiry of the digital certificate. IoT device 2 extracts D1's public key from the certificate and decrypts the nonce (N_1) to confirm freshness and prevent replay attacks. Once verification is successful, D2 is assured that D1 is a registered and legitimate IoT device of the network. Later, IoT device D2 then responds with its own identity (ID_2), its certificate (C_{D2}), and its current nonce (N_2), where N_2 is signed with D2's private key.

$$M_4 : D2 \rightarrow D1 : ID_{D2} \parallel CD_2 \parallel \{N_2\}_{PR_{D2}} \tag{5}$$

IoT Device 1 verifies the identity of D2. It decrypts C_{D2} using the server's public key (PUs) and checks the expiry of the certificate. IoT Device 1 uses IoT device 2's public key (from C_{D2}) to decrypt nonce (N_2), confirming freshness and protection against replay attacks (as shown in Fig. 2). This ensures IoT device D2 is a legitimate and registered device of the IoT network.

After the registration phase, IoT devices will mutually authenticate each other using the digital certificates that the server has previously issued them from a stochastic perspective, accounting for dynamic and uncertain network interactions [21], [22], [23]. The mutual authentication between two IoT devices (D1 and D2) will have the following process: IoT device 1 "D1" sends its identity (ID1), its digital certificate (CD1), and the current nonce (N1), where N1 has been signed (encrypted) with D1's private key. Upon receipt of any authentication message, the IoT device performs the following checks:

- Identity Check: the receiver confirms that the ID in the certificate matches the identity claimed by the sender
- Expiry Check: the receiver IoT device checks whether the certificate is still valid
- Certificate Authority Check: the receiver IoT device validates the signature on the certificate using the server's public key to ensure the certificate was issued and signed by a trustworthy authority server.

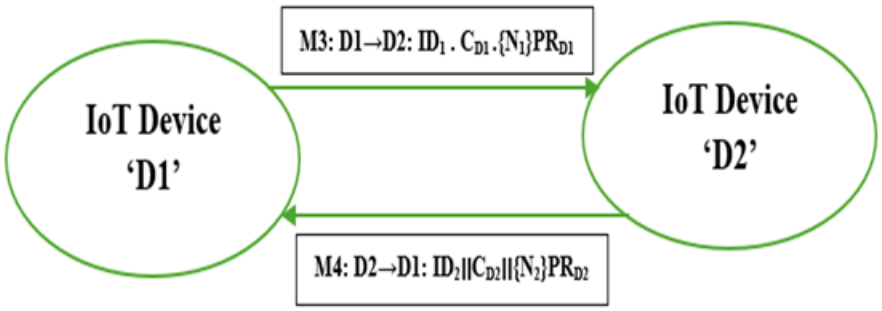

FIGURE 2. Authentication Phase

In this way, IoT devices D1 and D2 securely authenticate each other using digital certificates via asymmetric key cryptography. The proposed protocol ensures protection against impersonation, replay, and unauthorized access, making it suitable for securing IoT networks against both active and passive attacks.

4. Security Analysis

Impersonation Attack. This attack is about the disguising by an attacker after capturing the identity of the legitimate entity. In the proposed mechanism, identity of the devices is transmitted with certificate to avoid the impersonation attack.

4.1. **Replay Attack.** In this attack, an attacker replays the old messages to prove it is an authentic entity of the system. To avoid this attack, we have used nonce with each message transmission.

Device Capture Attack. This attack is about the compromising of the device by an attacker. To avoid this attack, hash functions are employed in the proposed protocol.

Automated Security Analysis using AVISPA. AVISPA tool is used to analyse the security of the proposed mechanism. In this section, three agents are defined for IoT device 'D1', IoT device 'D2' and server as D1, D2 and S respectively. This model uses Dolev-Yao attacker model [24], [25], [26], [27], [28]. Each agent uses a channel for communication among different agents SND, and RCV channel. The agent 'D1' sends the certificate request for the agent 'S'. Agent 'S' generates a certificate and sends the encrypted certificate to the agent 'D1'. Agent 'D1' verifies the received message and sends authentication request to another agent 'D2'. After successful authentication of agent 'D1', agent 'D2' responses with its own certificate. Agent 'D1' verifies the received certificate and in this way, both devices authenticate successfully. Fig. 1, 2, 3, and 4 shows the pseudo code for the proposed protocol.

Goals:

$$\texttt{secrecy\_of}\ CD_1$$

$$\texttt{secrecy\_of}\ CD_2$$

$$\texttt{authentication\_on}\ N_1$$

$$\texttt{authentication\_on}\ N_2$$

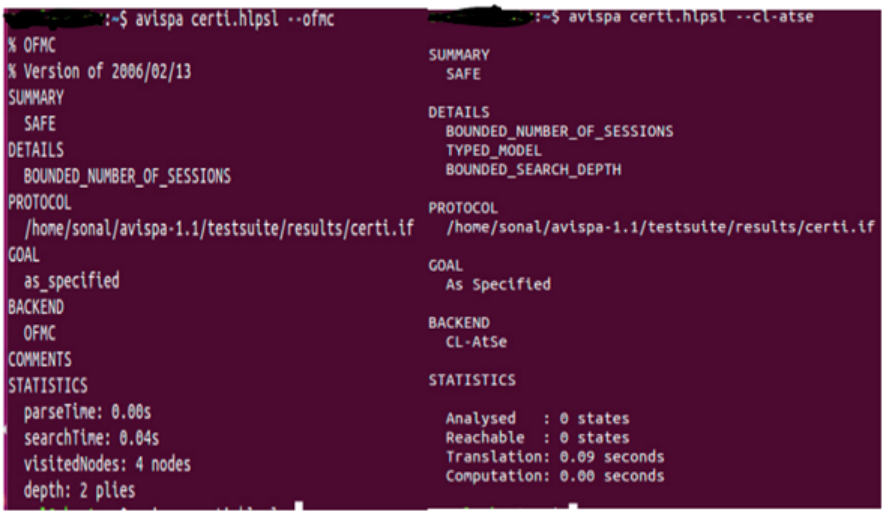

FIGURE 3. AVISPA Analysis Output

5. PERFORMANCE EVALUATION

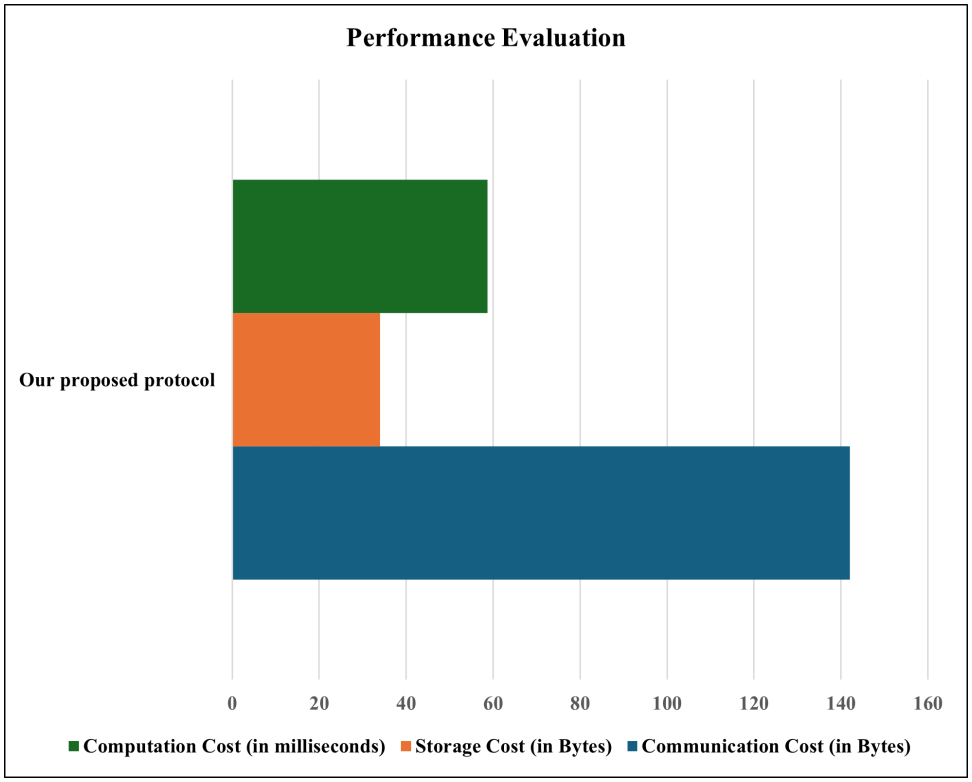

FIGURE 4. Performance Evaluation

In this part, we have discussed the cost of different parameters. These parameters' size has been used in this part too. The size of the certificate of IoT device are 32 bytes.

In our proposed protocol, message 1 is of size 20 bytes due to only one encrypted message using one asymmetric encryption. The size of message 2 is 20 bytes and 20 bytes respective for 2 encryptions. The size of message 3 and message 4 are consisted of the identity of device, certificate of device and encrypted nonce. The communication cost of our proposed protocol is (20 bytes + 40 bytes + 41 bytes + 41 bytes) = 142 bytes.

The storage cost of each IoT device consists of identity of IoT device, server and certificate. The total storage cost of each IoT device is (1 byte + 1 byte + 32 bytes) = 34 bytes.

The computation cost of the proposed protocol is comprised of 8 asymmetric encryption/decryption and 1 hash function. The total computation cost is (7 * 3ms + 1 * 37.76ms) = 58.76ms of our proposed protocol.

6. Conclusion

As we know, the IoT networks have crucial concern of security and privacy of data. These networks contain large amount of data to transmit which is related to specific application. Therefore, the accessibility and reachability of the data to legitimate entity or devices is our prime concern. In this part we have proposed a device authentication mechanism which uses digital certificate to authenticate each other. Our proposed mechanism provides security against replay, impersonation, and device capture attacks from a global stochastic perspective, considering the dynamic and uncertain behavior of IoT networks. The proposed mechanism is analysed for its security using AVISPA. The performance evaluation shows the different overheads of our proposed mechanism. This mechanism can be applied for many applications like military, industry for secure communication among different IoT devices.

References

[1] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W., A survey on internet of things: architecture, enabling technologies, security and privacy, and applications, *IEEE Internet Things J.* **4**(5) (2017), 1125–1142.

[2] Zhou, W., Jia, Y., Peng, A., Zhang, Y., Liu, P., The effect of IoT new features on security and privacy, *IEEE Internet Things J.* **6**(2) (2018), 1606–1616.

[3] Ni, J., Zhang, K., Lin, X., Shen, X., Securing fog computing for internet of things applications, *IEEE Commun. Surv. Tutor.* **20**(1) (2017), 601–628.

[4] Ma, X., Luo, W., The analysis of 6LoWPAN technology, In: *IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, 2008, 963–966.

[5] Hennebert, C., Dos Santos, J., Security protocols and privacy issues into 6LoWPAN stack, *IEEE Internet Things J.* **1**(5) (2014), 384–398.

[6] Verma, A., Ranga, V., Security of RPL-based 6LoWPAN networks in IoT, *IEEE Sens. J.* **20**(11) (2020), 5666–5690.

[7] Sowjanya, K., Dasgupta, M., Survey of symmetric and asymmetric key management schemes in IoT healthcare, In: *ICPC2T*, IEEE, 2020, 283–288.

[8] Henriques, M.S., Vernekar, N.K., Using symmetric and asymmetric cryptography to secure IoT communication, In: *ICIOT*, IEEE, 2017, 1–4.

[9] Hummen, R., Ziegeldorf, J.H., Shafagh, H., Raza, S., Wehrle, K., Towards viable certificate-based authentication for IoT, In: *ACM Workshop on Hot Topics on Wireless Network Security*, 2013, 37–42.

[10] Malani, S., Srinivas, J., Das, A.K., Srinathan, K., Jo, M., Certificate-based anonymous device access control scheme, *IEEE Internet Things J.* **6**(6) (2019), 9762–9773.

[11] Goldwasser, S., Micali, S., Rivest, R.L., A digital signature scheme secure against adaptive chosen-message attacks, *SIAM J. Comput.* **17**(2) (1988), 281–308.

[12] Mughal, M.A., Luo, X., Ullah, A., Ullah, S., Mahmood, Z., Lightweight digital signature-based security scheme, *IEEE Access* **6** (2018), 31630–31643.

[13] Lee, D.H., Lee, I.Y., Lightweight authentication and key agreement schemes for IoT, *Sensors* **20**(18) (2020), 5350.

[14] Hammi, M.T., Livolant, E., Bellot, P., Serhrouchni, A., Minet, P., Lightweight mutual authentication protocol for IoT, In: *Int. Conf. Mobile and Wireless Technology*, 2017, 3–12.

[15] Serhrouchni, A., Minet, P., Lightweight mutual authentication protocol for IoT, *Proc. ICMWT* **425** (2017), 3.

[16] Thungon, L.C., Sahana, S.C., Hussain, M.I., Lightweight certificate-based authentication for 6LoWPAN IoT, *J. Supercomput.* **79** (2023), 12523–12548.

[17] Garba, A. et al., LightCert4IoTs: Blockchain-based lightweight certificates authentication, *IEEE Access* **11** (2023), 28370–28383.

[18] Höglund, J., Furuhed, M., Raza, S., Lightweight certificate revocation for low-power IoT, *J. Inf. Secur. Appl.* **73** (2023), 103424.

[19] Patel, C., Bashir, A.K., AlZubi, A.A., Jhaveri, R., EBAKE-SE: ECC-based authenticated key exchange, *Digit. Commun. Netw.* **9**(2) (2023), 358–366.

[20] El-Hajj, M., Fadlallah, A., Chamoun, M., Serhrouchni, A., Survey of IoT authentication schemes, *Sensors* **19**(5) (2019), 1141.

[21] Chevalier, Y., Compagna, L., Cuellar, J., Drielsma, P.H., Mantovani, J., Mödersheim, S., Vigneron, L., High-level protocol specification language, In: *SAPS'2004*, Austrian Computer Society, 2004, 13.
[22] Fan, K., Li, H., Wang, Y., Security analysis of Kerberos using BAN logic, In: *IEEE Int. Conf. Information Assurance and Security*, 2009, 467–470.
[23] Burrows, M., Abadi, M., Needham, R.M., A logic of authentication, *Proc. Royal Soc. London A* **426**(1871) (1989), 233–271.
[24] Nessett, D.M., Critique of the Burrows-Abadi-Needham logic, *ACM SIGOPS Oper. Syst. Rev.* **24**(2) (1990), 35–38.
[25] Sharma, D., Kumar, G., Sharma, R., Analysis of heterogeneous data storage using M/M/c model, *Int. J. Cloud Appl. Comput.* **11**(3) (2021), 58–71.
[26] Belopolskaya, Y., Stochastic models for forward Kolmogorov equations, *J. Appl. Data Anal. Mod. Stoch. Model.* **1**(2) (2024), 64–86.
[27] Gliklikh, Y., Ryazantsev, M., Completeness of flow generated by stochastic algebraic-differential equation, *J. Appl. Data Anal. Mod. Stoch. Model.* **1**(1) (2024), 1–6.
[28] Ilolov, M., Rahmatov, J.Sh., Inverse problems of geothermics, *J. Appl. Data Anal. Mod. Stoch. Model.* **1**(2) (2024), 87–93.

Department of Computer Engineering and Application, Mangalayatan University, Aligarh, Uttar Pradesh, India
Email address: malikhan.amu@gmail.com

Department of Computer Engineering and Application, Mangalayatan University, Aligarh, Uttar Pradesh, India
Email address: meena.chaudhary@mangalayatan.edu.in

School of Computer Science Engineering and Technology, Bennett University, Greater Noida, Uttar Pradesh, India
Email address: anshucse.dwivedi@gmail.com