RESEARCH PAPER

Design of a Simple, Efficient and Robust IoT Device Authentication and Secret Key Generation Mechanism for IoT Networks

Mr. Malikhan Singh[1], Dr. Meena Chaudhary[2], Dr. Anshu Kumar Dwivedi[3]

[1] Research Scholar, Department of Computer Engineering and Application, Mangalayatan University, Aligarh, Uttar Pradesh, India. Institute of Engineering and Technology. Email: malikhan.amu@gmail.com

[2] Assistant Professor, Dept. of Computer Engineering and Application, Institute of Engineering and Technology, Mangalayatan University, Aligarh, Uttar Pradesh, India. Email: meena.chaudhary@mangalayatan.edu.in

[3] Assistant Professor (Senior Grade), School of Computer Science Engineering and Technology, Bennett University, Greater Noida, Uttar Pradesh. Email: anshucse.dwivedi@gmail.com

Received: 12th Mar, 2026 | **Revised:** 24th Mar, 2026 | **Accepted:** 14th Apr, 2026 | **Available Online:** 30th Apr, 2026

ABSTRACT

Recent developments such as the rapid proliferation of Internet of Things (IoT) have given rise to new requirements for secure, lightweight and energy-efficient forms of communication, particularly across heterogeneous and resource-constrained domains. In previous works, there has been considerable concentration on resource optimization; however, robust authentication protocols are also essential in order to protect infrastructure devices including randomly deployed sensor nodes. To this end, we present a simple, efficient and resilient authentication along with session key generation mechanism for IoT networks. The scheme utilizes public key cryptography, one-way hash functions, random numbers, secret keys and timestamps to provide confidentiality, integrity and protection against attacks. This paper presents a simple, efficient, and robust authentication and secret key generation mechanism for IoT networks, designed to minimize energy consumption while maintaining strong security properties. The authentication scheme is designed to be validated by formal verification tools, such as Burrows–Abadi–Needham (BAN) logic and Automated Validation of Internet Security Protocols and Applications (AVISPA). The security analysis is performed by OFMC and CL-Atse backends; the design is realized and evaluated in terms of communications, computations and storage. The proposed hardware implementation also makes it possible to evaluate the power consumption and scalability with other IoT devices. This presents a secure and efficient authentication scheme with dynamic session key establishment for IoT-based WSN. The mechanism offers an efficient way of securing IoT devices in distributed and resource-constrained settings, paving the way for secure IoT applications and services in this space.

Keywords: IoT Networks, Automated Security System, AVISPA, Smart Networks, Wireless Sensor Networks, Burrows Abadi Needham (BAN) Logic.

How to cite this article: Singh M, Chaudhary M, Dwivedi AK. Design of a Simple, Efficient and Robust IoT Device Authentication and Secret Key Generation Mechanism for IoT Networks. Int J Drug Deliv Technol. 2026;16(40s): 166-173. DOI: 10.25258/ijddt.16.40s.18

Source of support: Nil.

Conflict of interest: None

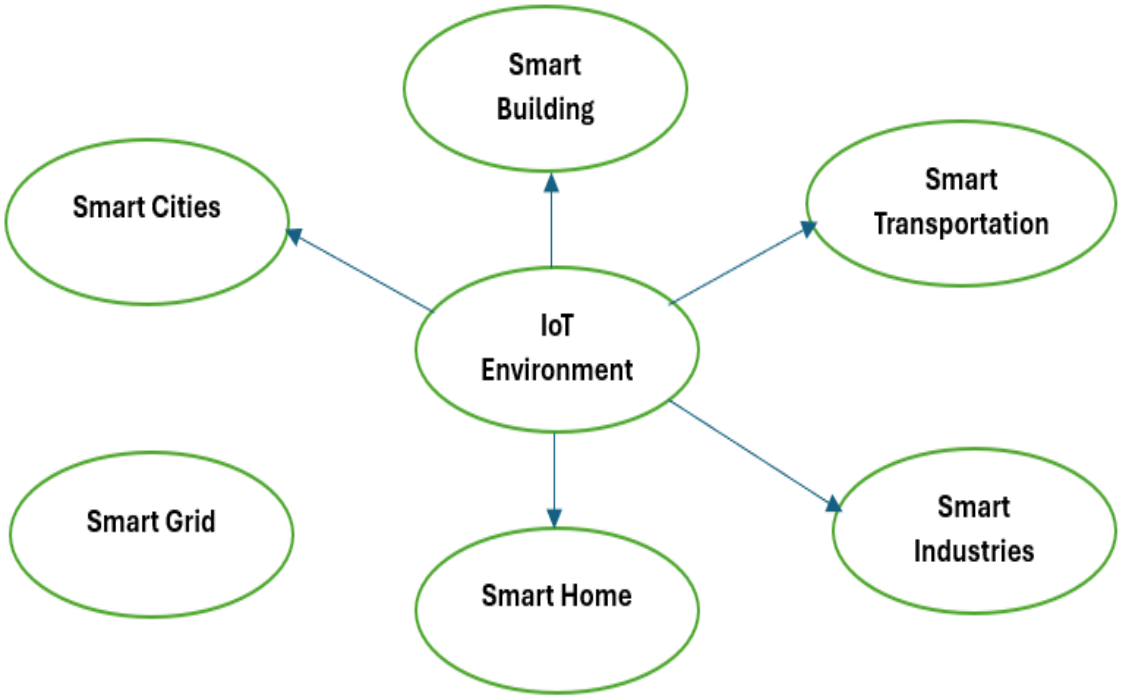

Fig. 1: Different applications of IoT environment.

IoT environments encompass a wide range of applications, including smart cities, health monitoring, personal, smart industries, smart transportation systems, smart agriculture and many more (as shown in Fig. 1). These applications rely on wireless networks to collect and transmit data, utilizing modern communication technologies such as Wi-Fi, Wi-Sun, ZigBee, and Z-Wave, which offer improved performance over traditional infrared-based communication systems [7], [8], [9]. Nevertheless, the adoption of such technologies introduces significant communication and computational overheads.

The advancements of machine-to-machine (M2M) communication has changed the way devices interact, observe, and analyze data. Within this context, the internet communication infrastructure is essential for enabling secure communication between IoT devices [10], [11], [12], [13]. IoT devices, which are electronic devices capable of collecting environmental data and interacting with other devices, generate large amounts of data through M2M communication. This mechanism results in increased demands for bandwidth, storage capacity, and computational resources. According to projections by CISCO, the number of IoT devices connected to the internet was expected to exceed with potential growth to 500 billion by 2030, collectively generating hundreds of zettabytes of data. This unprecedented scale of data transmission raises critical security issuess that must be considered.

The major challenges in IoT environments are resource limitations, heterogeneity, and security. Devices within these environments are expected to ensure secure data transmission to authenticated receivers, thereby supporting accurate decision-making. Additionally, they must be safeguarded against secret value guessing, replay, Sybil, and masquerade attacks, while also maintaining forward and backward secrecy to ensure the confidentiality of past and future communications.

Although much of the existing research has concentrated on efficient resource utilization in constrained environments, it is equally vital to develop mechanisms that guarantee secure communication with minimal energy consumption. Sensor nodes, often deployed irregularly, require robust authentication mechanisms to support heterogeneous and distributed environments. To address this challenge, the proposed mechanism introduces an authentication protocol for IoT devices. During the registration phase, IoT devices obtain secure credentials from the server. The mechanism incorporates public key cryptography, secret key, one-way hash functions, random number, and timestamps to defend against the aforementioned security threats.

Comprehensive evaluation confirms the authenticity of the proposed protocol. Formal security validation methods, including Burrows–Abadi–Needham (BAN) logic, and Automated Validation of Internet Security Protocols and Applications (AVISPA), demonstrate the mechanism's robustness against prevalent attacks.

Furthermore, hardware implementation results confirm that the protocol achieves security objectives while consuming less energy than existing approaches.

I. RELATED WORK

Security in IoT networks is a major concern due to its large-scale applicability. It attracts many researchers for the finding of the feasible solutions towards ensuring security in IoT networks. The pivot requirements of security are device authentication and key management in IoT networks [14], [15], [16], [17], [18], [19]. Device authentication is about the communication of trusted devices in the IoT networks. In this section, we discusses the related work in the field of IoT security.

In 2017, Li et al. [22] discussed the public key encryption scheme for the authentication of IoT devices. The proposed mechanism is evaluated using Cooja Simulator and proposed mechanism is lightweight by equipping XOR operation. It resists against various attacks eavesdropping, and Distributed Denial-of-Service (DDoS) attacks.

In [21], Kumar et al. designed an authentication and key agreement for Smart Energy Networks (SEN). This mechanism establishes a secure communication between smart meters and unable to resist DDoS and replay attacks. The simulation is done through AVISPA tool.

In [20], Mick et al. proposed an authentication mechanism for smart cities. A pre-shared key extensible authentication protocol (EAP-PSK) was designed to authenticate and route Named Data Networking (NDN) IoT. The proposed mechanism was simulated using NS-3 and this mechanism is insecure against DDoS attack.

In [23], Jaya et al. proposed a mechanism for authentication through Elliptic Curve Digital Signature Algorithm (ECDSA) for IoT networks. Authors have proposed three phases for ensuring the security. The mechanism is insecure against DDoS and Man-in-the-middle attacks.

Li et al. [24] discussed a lightweight authentication protocol based on XOR and hash operations. The simulation is done with NS-3 and AVISPA tools. It is vulnerable to MitM, DDoS, and backward secrecy.

In [25], authors proposed a protocol based on ECC and one-way hash function for the authentication of IoT devices. This protocol is not resistant against backward and forward secrecies.

In [26], Loffi et al. proposed a mutual authentication using public and private key cryptography for IoT devices and fog nodes in IoT environments. It is insecure against node capture, Sybil and DoS attack.

Many mechanisms have proposed for the authentication of IoT devices in IoT environments. But these mechanisms are prone to various attacks like DoS, MitM, Sybil, DDoS and many more. Therefore, we have designed an authentication mechanism for authentication IoT devices in IoT environments.

II. Proposed Mechanism

This section discusses the authentication mechanism with session key generation for the authentication of IoT devices.

3.1 Notations:

Table 1: Notations used for the proposed protocol.

Symbol	Description
N	IoT device
S	Server
PU_s	Public key of S
PU_a	Public key of A
PR_s	Private Key of A
PR_s	Private Key of S
ID_A	Identity of A
MSG_A	Message of A
T_A	Timestamp of A
T_S	Timestamp of S
R	Random number generated by S
S_a	Session key
IN_A	Intermediate message

3.2 The Protocol:

In the proposed mechanism, IoT device ‘N’ wants to authenticate itself with the server ‘S’, then it has to perform the following communications:

M1: N → S: $ID_A, \{MSG_A, T_A\}_{PUs}$

The IoT device ‘N’ stores public key of server ‘PU_s’ in its memory for further communication. The IoT device ‘N’ sends a request message M1 to server for session key. When server receives the request, it verifies the identity of IoT device ‘N’. After the successful verification, server decrypts the message with its private key ‘PR_S’ and gets the timestamp ‘T_A’. Server checks whether the timestamp is a valid timestamp or not. If the timestamp is valid, the server generates a session key ‘S_a’ as shown below. Otherwise the process is aborted.

$S_a = h(ID_A \| ID_S \| R)$

Later it calculates the intermediate message ‘IN_A’ as follows:

$IN_A = MSG_A \oplus S_a$

The server sends a message M2 to the IoT device ‘N’ as shown below:

M2: S → N: $\{IN_A\}_{PUa}$

When IoT device ‘N’ receives this message, it decrypts the message M2 using its private key ‘PR_a’. After the

successful decryption, IoT device will be able to extract the secret key using XOR operation.

$S_a = MSG_A \oplus IN_A$

After calculating the secret key, IoT device 'N' sends an encrypted timestamp 'T_A' using secret key 'S_a' in message M3.

M3: N→ S: $\{T_A\}_{Sa}$

As server receives message M3, it decrypts timestamp using its saved secret key. After its successful decryption, server finds IoT device a legitimate device. Server sends a encrypted message M4 to IoT device 'N' with the received timestamp 'T_A' and a new generated timestamp 'T_S'.

M4: S → N: $\{T_A, T_S\}_{Sa}$

After receiving this message, IoT device acknowledged with the received timestamps.

M5: N → S: $\{T_S\}_{Sa}$

In this way, the IoT device authenticates itself with the help of server and generates secret key successfully. Fig. 2 shows the flow of messages in the proposed mechanism.

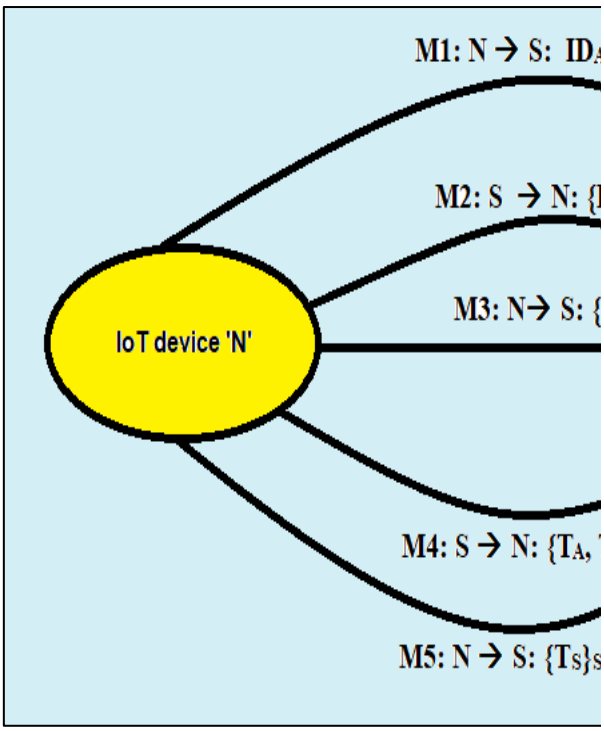

Fig. 2: Flow of messages between IoT device and Server.

III. SECURITY ANALYSIS

Based on the theoretical analysis of our proposed protocol the following attacks are not possible on the protocol:

1. Denial-of-Service (DoS) Attack – In our proposed protocol, we are using identity of IoT device 'ID_A' for authentication, therefore DoS attack is not possible on the protocol.

2. Man-in-the-middle (MITM) Attack - The Proposed protocol is secure against man-in-the-middle attack due to the encryption of all messages. Thus, it is prone to MITM attack.

3. Replay attack – This attack is prevented through the use of timestamps and by ensuring old communications are not reused.

4. Session hijacking attack – In the proposed mechanism, secret key is used to prevent session hijacking attack.

Thus, the proposed protocol attains the security properties and also resilient to some possible attacks.

3.1 Automated Security Analysis using AVISPA:

This section discusses about the modelling of the proposed protocol through AVISPA (Automated Validation of Internet Security Protocol and Analysis) [28], [29], [30]. The proposed protocol is coded with the two roles IoT device 'N' and server 'S'. Dolev-Yao model is the attacker model in this tool [31]. The IoT device 'N' acts an agent A with Sa as session key (secret key in the proposed protocol), PUa as public key of IoT device 'N' and RCV_S, SND_ S as its communication channel. Server 'S' acts an agent S with Sa as session key (secret key in the proposed protocol), PUs as public key of server 'S' and RCV_A, SND_ A as its communication channel.

```
role N(N, S, A: agent,
       pubkS, pubkA: public_key)
played_by N
vars
    IDA, IDS : agent,
    MSGA, INA : message,
    TA, TS, R, Sa : message
fresh
    TA, MSGA

init
    IDA := A
    IDS := S

transition
1. state(0) -> state(1)
   /* IoT device sends IDA and MSGA
   send_1( S, { IDA, crypt( (MSGA,

2. state(1) -> state(2)
   /* IoT device receives {INA} enc
   recv_2( S, crypt( INA, pubkA ) )

3. state(2) -> state(3)
   /* IoT sends timestamp TA protec
   send_3( S, crypt( TA, Sa ) )

4. state(3) -> state(4)
   /* IoT receives {TA, TS} encrypt
   recv_4( S, crypt( (TA, TS), Sa )

5. state(4) -> state(5)
   /* IoT replies with TS protected
   send_5( S, crypt( TS, Sa ) )

end role
```

Fig. 3:Pseudo code of AVISPA 1.1 of IoT device ‘N’

```
role S(N, S, A: agent,
       pubkS, pubkA: public_key)
played_by S

vars
    IDA, IDS : agent,
    MSGA, INA : message,
    TA, TS, R, Sa : message
fresh
    R, TS

init
    IDS := S

transition
1. state(0) -> state(1)
   recv_1( N, { IDA, crypt( (MSGA, TA),
   /* Server computes session key */
   Sa := hash( (IDA, IDS, R) )
   INA := xor( MSGA, Sa )

2. state(1) -> state(2)
   /* Server sends INA encrypted under
   send_2( N, crypt( INA, pubkA ) )

3. state(2) -> state(3)
   /* Server receives TA protected with
   recv_3( N, crypt( TA, Sa ) )

4. state(3) -> state(4)
   /* Server sends {TA,TS} with Sa */
   send_4( N, crypt( (TA, TS), Sa ) )

5. state(4) -> state(5)
   /* Server receives TS back with Sa *
   recv_5( N, crypt( TS, Sa ) )

end role
```

Fig. 4: Pseudo code of AVISPA 1.1 of IoT device ‘S’.

```
role environment()
played_by environment

const
    n, s, a : agent,
    pubkS, pubkA : public_key

intruder_knowledge = { n, s, a, pubkS,

composition
    session1: N(n, s, a, pubkS, pubkA)
    /\ session2: S(n, s, a, pubkS, pub

end role

goal
        authentication_on Sa
end goal
```

Fig. 4: Pseudo code of AVISPA 1.1 of role environment and goals.

Agent ‘A’ starts the communication by initializing on state 0. S adopts request from ‘A’ and it is activated to state 1. ‘S’ adopts request from ‘A’ and is activated to

state 2. 'S' transmits it request to 'A' and it is activated to state 5. Finally, 'A' and 'S' are mutually authenticated in state 5 and 6. The agent's public keys is given under intruder's knowledge. The role environment consists of intruder knowledge, protocol id's, public keys, and agents. The session key is avoided from the knowledge of intruder because it is possible to hold session key as secret between trusted devices (as shown in Fig. 3, 4, 5).

3.2 Goals : authentication_on Sa

```
sonal@ubuntu:~$ avispa protocol1.h
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/sonal/avispa-1.1/testsuite
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.08s
  visitedNodes: 18 nodes
  depth: 4 plies
```

Fig. 6: Analysis using OFMC backend.

IV. RESULTS & DISCUSSION

The security analysis of the proposed protocol shows that the proposed protocol is secure against various security attacks. The proposed protocol is analysed using two backends: CL-Atse and OFMC backends. The OFMC backend discusses the security in terms of demand driven and lazy behaviour. Whereas CL-Atse defines the security analysis in terms of constraint sets and traces out the security attacks. Figures shows that the proposed protocol is found safe and sound through the AVISPA in both backends. The intruder is unable to read or interrupt any message in whole communication process. Hence, the proposed mechanism is free from various potential security attacks like Denial-of-Service attack, Man-in-the-Middle attack, and many more. Fig. 6 and Fig. 7 shows the results of analysis of our proposed protocol for both backends, OFMC and CL-Atse.

```
[redacted]:~$ avispa protocol1.hlpsl --c

SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
  BOUNDED_SEARCH_DEPTH

PROTOCOL
  /home/sonal/avispa-1.1/testsuite/results

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 40 states
  Reachable  : 11 states
  Translation: 0.12 seconds
  Computation: 0.00 seconds
```

Fig. 6: Analysis using CL-Atse backend

V. PERFORMANCE ANALYSIS

In this section, different overheads like communication cost, computation cost and storage cost of our proposed protocol are calculated.

Communication cost is the number of bits transmitted during whole authentication and secret key generation process in our proposed protocol. The computation cost is the time consumed by the protocol to successfully authenticate the IoT devices in the IoT networks. The storage overhead is related to the number of bits stored in the IoT device's memory before initiating the communication.

To calculate the communication cost and storage cost, we consider the size of the identity of server and device is 1 bytes, the size of random number and timestamp is 4 bytes, the size of MSG_A and intermediate message IN_A is 4 bytes, the size of public-private key pair is 32 bytes, and the size of secret key is 16 bytes. The size of public key encrypted message is 20 bytes, and the secret key encrypted message is 16 bytes. Total five messages are transmitted in our proposed protocol. The total communication cost of transmitting messages is

(24 bytes + 20 bytes + 16 bytes + 16 bytes + 16 bytes) = 92 bytes.

The storage cost of IoT device is consistent with the identity of server and IoT device, public-private key pair of IoT device and public key of server. The total storage cost is (1 bytes + 1 bytes + 32 bytes + 16 bytes) = 50 bytes.

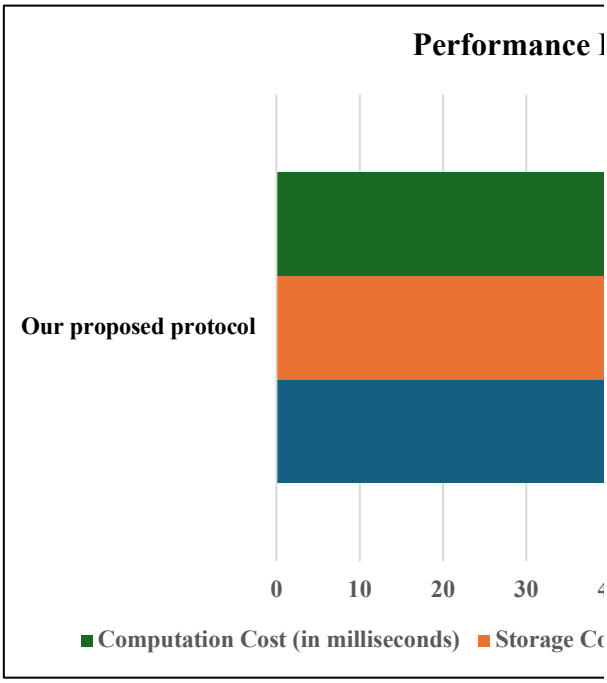

Fig. 7: Performance evaluation of the proposed protocol.

To calculate the cost of computation, the computation cost of hash function is 37.76 milliseconds (ms), asymmetric encryption or decryption is 3 ms, symmetric encryption or decryption is 3 ms, symmetric encryption or decryption is 3.6 ms. The cost of XOR and concatenation operations are negligible. Our proposed mechanism performs 2 asymmetric encryption, 3 symmetric encryption, 1 hash function, 1 XOR and 1 concatenation operation to ensure the security of IoT device. The total cost of computation for our proposed protocol is (2*3ms + 3*3.6ms + 1*37.76ms) = 54.56ms.

Fig. 7 depicts the cost of communication, storage and computation cost of our proposed protocol.

VI. CONCLUSION

As we know that the security is the key concern in IoT environment because this network is consisted of large number of devices. The IoT devices are resource constrained with less energy efficient. Therefore, there is a need of an authentication mechanism which authenticates devices over the network and generate a secret key for secure communication with less resource consumption. Our proposed mechanism is very simple, efficient and robust due to the smaller number of messages are transmitted to authenticate IoT device. The proposed protocol is based on public key cryptography, hash function and XOR operation. Any IoT device when entered the network, it has public key pair of itself with the public key of server, and it acquires the secret key from the server for secure communication in future. The proposed mechanism is analysed using AVISPA tool and validates the security of the proposed protocol.

References

[1] A. B. Kathole, K. N. Vhatkar, and S. D. Patil, "IoT-enabled pest identification and classification with new meta-heuristic-based deep learning framework," Cybern. Syst., vol. 55, no. 2, pp. 380–408, Feb. 2024.

[2] S. Kumbhare, S. A. Ubale, G. Dharmale, N. Mhala, and N. Gandhewar, "IoT-enabled agricultural waste management for sustainable energy generation," Int. J. Intell. Syst. Appl. Eng., vol. 12, no. 13s, pp. 477–482, 2024.

[3] A. B. Kathole, K. N. Vhatkar, S. Kumbhare, J. Katti, and V. V. Kimbahune, "IoT-based smart agriculture for onion plant disease management: A comprehensive approach," Int. J. Intell. Syst. Appl. Eng., vol. 12, no. 13s, pp. 472–476, 2024.

[4] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The Industrial Internet of Things (IIoT): An analysis framework," Comput. Ind., vol. 101, pp. 1–12, Oct. 2018.

[5] A. Hazra, M. Adhikari, T. Amgoth, and S. N. Srirama, "A comprehensive survey on interoperability for IIoT: Taxonomy, standards, and future directions," ACM Comput. Surv., vol. 55, no. 1, pp. 1–35, Jan. 2023.

[6] S. Schneider, "The Industrial Internet of Things (IIoT) applications and taxonomy," in Internet of Things and Data Analytics Handbook. Hoboken, NJ, USA: Wiley, 2017, pp. 41–81.

[7] S. Vitturi, C. Zunino, and T. Sauter, "Industrial communication systems and their future challenges: Next-generation Ethernet, IIoT, and 5G," Proc. IEEE, vol. 107, no. 6, pp. 944–961, Jun. 2019.

[8] M. Tanveer, A. A. A. El-Latif, A. U. Khan, M. Ahmad, and A. A. Ateya, "LEAF-IIoT: Lightweight and efficient authentication framework for the Industrial Internet of Things," IEEE Access, vol. 12, pp. 31771–31787, 2024.

[9] S. F. Tan and A. Samsudin, "Recent technologies, security countermeasure and ongoing challenges of Industrial Internet of Things (IIoT): A survey," Sensors, vol. 21, no. 19, p. 6647, Oct. 2021.

[10] G. Rathee, F. Ahmad, N. Jaglan, and C. Konstantinou, "A secure and trusted mechanism for

industrial IoT network using blockchain,'' IEEE Trans. Ind. Informat., vol. 19, no. 2, pp. 1894–1902, Feb. 2023.

[11] T. Gebremichael, L. P. I. Ledwaba, M. H. Eldefrawy, G. P. Hancke, N. Pereira, M. Gidlund, and J. Akerberg, ''Security and privacy in the Industrial Internet of Things: Current standards and future challenges,'' IEEE Access, vol. 8, pp. 152351–152366, 2020.

[12] H. Vargas, C. Lozano-Garzon, G. A. Montoya, and Y. Donoso, ''Detection of security attacks in industrial IoT networks: A blockchain and machine learning approach,'' Electronics, vol. 10, no. 21, p. 2662, Oct. 2021.

[13] M. Wang, Y. Sun, H. Sun, and B. Zhang, ''Security issues on Industrial Internet of Things: Overview and challenges,'' Computers, vol. 12, no. 12, p. 256, Dec. 2023.

[14] C. Lupascu, A. Lupascu, and I. Bica, ''DLT based authentication framework for industrial IoT devices,'' Sensors, vol. 20, no. 9, p. 2621, May 2020.

[15] E. Lara, L. Aguilar, M. A. Sanchez, and J. A. García, ''Lightweight authentication protocol for M2M communications of resource-constrained devices in Industrial Internet of Things,'' Sensors, vol. 20, no. 2, p. 501, Jan. 2020.

[16] C. Patel, A. K. Bashir, A. A. AlZubi, and R. Jhaveri, ''EBAKE-SE: A novel ECC-based authenticated key exchange between industrial IoT devices using secure element,'' Digit. Commun. Netw., vol. 9, no. 2, pp. 358–366, Apr. 2023.

[17] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, ''Challenges and opportunities in securing the Industrial Internet of Things,'' IEEE Trans. Ind. Informat., vol. 17, no. 5, pp. 2985–2996, May 2021.

[18] M. Agrawal, J. Zhou, and D. Chang, ''A survey on lightweight authenticated encryption and challenges for securing industrial IoT,'' in Security and Privacy Trends in the Industrial Internet of Things. Cham, Switzerland: Springer, 2019, pp. 71–94.

[19] X. Yu and H. Guo, ''A survey on IIoT security,'' in Proc. IEEE VTS Asia–Pacific Wireless Commun. Symp. (APWCS), Aug. 2019, pp. 1–5.

[20] T. Mick, R. Tourani, and S. Misra, ''LASeR: Lightweight authentication and secured routing for NDN IoT in smart cities,'' IEEE Internet Things J., vol. 5, no. 2, pp. 755–764, Apr. 2018.

[21] P. Kumar, A. Gurtov, M. Sain, A. Martin, and P. H. Ha, ''Lightweight authentication and key agreement for smart metering in smart energy networks,'' IEEE Trans. Smart Grid, vol. 10, no. 4, pp. 4349–4359, Jul. 2019.

[22] N. Li, D. Liu, and S. Nepal, ''Lightweight mutual authentication for IoT and its applications,'' IEEE Trans. Sustain. Comput., vol. 2, no. 4, pp. 359–370, Oct. 2017.

[23] J. Singh, A. Gimekar, and S. Venkatesan, ''An efficient lightweight authentication scheme for human-centered Industrial Internet of Things,'' Int. J. Commun. Syst., vol. 36, no. 12, pp. 1–13, Nov. 2019.

[24] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, and K. R. Choo, ''A robust and energy efficient authentication protocol for Industrial Internet of Things,'' IEEE Internet Things J., vol. 5, no. 3, pp. 1606–1615, Jun. 2018.

[25] Lohachab A, Karambir. ECC based inter-device authentication and authorization scheme using MQTT for IoT networks. J Inf Sec Appl. 2019;46:1-12.

[26] Zhang Y, Cheng K, Khan F, Alturki R, Khan R, Rehman AU. A mutual authentication scheme for establishing secure device-to-device communication sessions in the edge-enabled smart cities. J Inf Sec Appl. 2021;58:102683.

[27] Loffi L, Westphall CM, Grüdtner LD, Westphall CB. Mutual authentication with multi-factor in IoT-fog-cloud environment. J Netw Comput Appl. 2021;176:102932.

[28] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. H. Drielsma, P. C. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, and L. Vigneron, ''The AVISPA tool for the automated validation of Internet security protocols and applications,'' in Proc. 17th Int. Conf. Comput.-Aided Verification, Scotland, U.K. Cham, Switzerland: Springer, Jul. 2005, pp. 281–285.

[29] L. Viganò, ''Automated security protocol analysis with the AVISPA tool,'' Electron. Notes Theor. Comput. Sci., vol. 155, pp. 61–86, May 2006.

[30] J. A. Hurtado Alegría, M. C. Bastarrica, and A. Bergel, ''AVISPA: A tool for analyzing software process models,'' J. Softw., Evol. Process, vol. 26, no. 4, pp. 434–450, Apr. 2014.

[31] I. Cervesato, ''The Dolev–Yao intruder is the most powerful attacker,'' in Proc. 16th Annu. Symp. Log. Comput. Sci. (LICS, vol. 1, 2001, pp. 1–2.