Applied Data Science and Analysis
Vol.2026, **pp**. 17–40
DOI: https://doi.org/10.58496/ADSA/2026/002; ISSN: 3005-317X
https://mesopotamian.press/journals/index.php/ADSA

Research Article

A Hybrid Multi-Factor Authentication System with GPS-Based on SPECK Encryption in Oil Cybersecurity

Amal Khaleel Hamad [1], Mishall Al-Zubaidie [1,*]

[1] *Department of Computer Sciences and Artificial Intelligence, Education College for Pure Sciences, University of Thi-Qar, Nasiriyah 64001, Iraq*

ARTICLE INFO

Article History

Received 19 Oct 2025
Revised 20 Nov 2025
Accepted 25 Dec 2025
Published 31 Jan 2026

Keywords
Adaptive Authentication,
Data Protection,
Industrial IoT Security,
NIZK,
Oil Cybersecurity,
Privacy-Preserving
Real-or-Random.

ABSTRACT

The oil and gas sector has become increasingly exposed to sophisticated cyberattacks, where classic single- or two-factor authentication mechanisms are insufficient for securing online transactions in oil-and-gas operational environments. This paper proposes a hybrid multi-factor authentication (H-MFA) system that integrates six security components, consisting of four authentication factors (Time-based One-Time Passwords (TOTP), GPS-based location validation, Password Salting and Hashing, and Biometric template factor (simulated) and two cryptographic enablers (SPECK lightweight encryption and Non-Interactive Zero-Knowledge (NIZK)-based privacy-preserving verification). The presented system attempts to reach a desirable trade-off between security assurance and computational feasibility for resource-limited industrial endpoints and edge gateways. Moreover, a Real-or-Random (RoR) inspired security model is incorporated as a theoretical security argument to provide indistinguishability-based validation against inference and distinguishing attacks on authentication outputs. We have implemented the system in Java and evaluated it through repeated experimental runs using an access-behavior dataset under different parameter settings. The evaluation considers metrics such as decision-level determinism, randomness of stochastic token outputs, stability towards repeated experiments, and scalability towards increasing workload and concurrency. We conducted a simulation-based feasibility evaluation using the same access-behavior dataset, where TOTP/GPS/biometric-template and NIZK-related outputs are instantiated via controlled proxies. Security discussion is supported by a RoR-inspired indistinguishability argument under stated assumptions, while engineering performance is evaluated separately using latency, throughput, CPU, and memory. In general, this paper provides an integrated and implemented MFA design that combines factor diversity, privacy-preserving verification, and secure audit-log protection for reliable online transactions authentication in critical oil and gas infrastructures.

1. INTRODUCTION

The technology behind online payment methods is becoming more complex as a result of the evolution and sophistication of cyberattacks. Hence, it has become crucial to establish new techniques that are reliable and secure. With the increasing adoption of digital technologies, user authentication becomes an important part to secure data and privacy [1]. Cryptographic methods are essential to the security of digital communications and securing data against unauthorized access or data modification [2]. Among authentication factors, Multi-Factor Authentication (MFA) is known to be a strong means for verifying user identity [3]. The uniqueness and ease of use are the two most important factors for widespread acceptance of biometric data techniques [4]. A user's geographic location is also a possible verification factor in the context of location-based authentication schemes, adding an extra dimension to improve the access dependability [5-7]. On the other hand, Internet of Things (IoT) technologies have revolutionized some industries with the ability to provide interconnected systems and devices. The oil and gas field is a desirable target for sophisticated cyberattacks, because data is irreplaceable and systems are part of critical infrastructure that needs assurances of optimal security systems [8]. It is a requirement that user authentication at a secure level should be present with high security for online financial transactions, especially where the risk is higher. We live in an era where data is crucial and sensitive, single-factor sign-on data exchange/information sharing/transactions aren't good enough with the amount of value we are talking about. Most of the cases have the potential to cause losses that businesses cannot afford. Traditional password-based authentication can suffer from attacks such as phishing, keylogging, and brute force attacks. Also, biometric information, such as passwords, cannot be changed once it's

*Corresponding author. Email: mishall_zubaidie@utq.edu.iq

stolen [4]. Robust security implementation is challenging due to the constrained computing capability of IoT devices. Most of the existing systems rely on a small set of combinations, resulting in reduced security properties [5]. In response to their implementation in current high-speed networks, a variety of conventional encryption methods are found to be susceptible and inefficient. These systems can tamper with the reported location data, making GPS vulnerable to spoofing attacks, which is a serious security issue. In addition, for many of the oil businesses, there are no cybersecurity advances in security technology to protect their advanced technical operation systems [8]. The security of MFA is increased through the combination of two or more independent factors. Security could be further verified by incorporating more factors, like location and biometric verification. Geographical location serves as an authentication element that verifies a user's physical presence and complements other elements like passwords and biometrics. To protect biometric data and prevent fraud, safeguards and encryption are required. Integrate geographic information with other authentication elements to generally improve system security. Lightweight cryptographic techniques protect communications in environments with limited resources. Encryption techniques must be safe and efficient to safeguard sensitive data without compromising system performance. To protect industrial processes and avoid unauthorized entry, authentication methods must be improved [3,5].

1.1 Research Contributions

The main contributions of this approach can be summarized as follows:

1. An integrated H-MFA system design for oil and gas operational environments, combining six security components: four authentication factors (TOTP, password salting and hashing, Biometric template factor (simulated), and GPS-based location) and two cryptographic enablers (SPECK lightweight encryption and NIZK-based privacy-preserving verification) into a united lightweight system. Unlike prior studies that evaluate these mechanisms in isolation, this work focuses on their coordinated operation under industrial constraints.
2. A RoR-inspired security evaluation, providing an indistinguishability-oriented argument for authentication outputs under adversarial observation. The RoR model is used strictly to support theoretical security claims, while implementation-level performance is evaluated independently.
3. An implementation-based experimental evaluation, conducted through repeated execution runs using access-behavior datasets. The evaluation reports decision consistency, entropy-based randomness, stability across repeated executions, and scalability under increasing concurrency, demonstrating feasibility for deployment in resource-constrained industrial environments.

2. RELATED WORKS OF EXISTING AUTHENTICATION SYSTEMS

The development and integration of various technologies and mechanisms to achieve MFA has been prompted by the significance of cyber transactions in oil companies, their susceptibility to frequent attacks, and the need to maintain high levels of efficiency while utilizing minimal network resources. Numerous references about our subject of study have been discussed in this research work. Below is a list of them, along with an explanation of their respective applications and drawbacks:

Prasad et al. (2024) [9] discussed cybersecurity problems in the oil and gas sector and suggested frameworks confirmed by technologies such as encryption, firewalls, Zero Trust, AI/ML, Cyber-Informed Engineering (CIE), and Intrusion Detection Systems (IDS). Such efforts strengthen detection, behavior, and resilience, yet they face issues such as legacy systems, fragmented laws, and the lack of skilled staff. The research is methodologically sound but lacks practical verification, and hence prevents the application of proven customized solutions in oil field environments. Moreover, Alsharif and Manuel (2024) [10] proposed a Secure framework for Internet transactions on financial which brings together ML with MFA. The first layer of their proposed system contained three authentication factors (i.e., OTP, face recognition, and password/username paired with a fingerprint). This was also integrated with ML-based classifiers, such as decision trees, logistic regression, naive bayes, or random forest for fraud detection, evaluated at 97.938% accuracy in the logistic regression model. The system was deployed in a mobile e-commerce application, and its usability and security advantages were evaluated against existing MFA schemes. Nevertheless, the work highlights obstacles, including user reluctance to adopt complicated authentication processes, privacy fears, and imbalances in training data that limit integration and deployment of more diverse real-world datasets. Victor et al. (2021) [11] have introduced a blockchain-based multi-factor authentication model (MFBC_eDS) for cloud-enabled Internet of Vehicles (IoV), using a Probabilistic Polynomial-Time Algorithm (ePPTA) to strengthen an embedded digital signature and integrate Security Assertion Markup Language (SAML) with Single Sign-On (SSO) for enhancing the resilience of the embedded digital signature. The results from the study revealed that vehicular networks support data security, integrity, availability, and privacy with high protection against cyberattacks. But the model is faced with some problems such as the lack of user-centric evaluations and its generalizability in practice. These obstacles are related to the trade-off complexity for being user-friendly and overcoming security requirements, energy consumption in blockchain mechanisms, and increased computational complexity, posing a high barrier for the wider

adoption of the suggested model. Furthermore, Mohamed et al. (2017) [12] introduced a three-factor authentication solution, TUASRESG, for a renewable energy-based smart grid setting. This system is designed to create session keys between users and smart meters, ensuring secure mutual authentication. It consists of three different verification factors: password, biometric information and the user's mobile device, besides making use of advanced cryptographic mechanisms such as one-way hash functions, elliptic curve cryptography (ECC), and XOR operations. It is well-suited for resource-scarce conditions because of its low communication and computation overhead. Security-oriented performance was justified based on NS2 simulation results depicting the effectiveness of the model, considering PDRs between 0.96 and 0.99 (robust against different cyberattacks) as well as efficient communication capabilities. But the difficulties that we are still facing concern, above all, a good tradeoff between security and system performance in an offline realization, on an industrial time-scale and also how to extend the model to apply it to greater and larger systems as smart grids. Additional researches need to be carried out to make adaptive responses toward these changing needs. Mangal et al. (2020) [13] identified the evolvement of authentication technologies in Cyber-Physical Systems (CPS), ranging from single-factor to MFA. This research paper determined that MFA contributes more towards data availability, confidentiality, and integrity by providing mutual authentication, generation of session key, anonymity as well as preventing the denial-of-service attacks, spoofing and replay attacks. Several MFA approaches were compared and analyzed, including cloud authentication, multi-biometric mode for enterprise security, priority-based access control using digital twin for cyber awareness, and efficient anonymous authentication of smart grid messages. However, there is an urgent demand for the design of lightweight and convenient-to-use authentication techniques which meet the performance and security demands of sophisticated CPS. Applying these models in practice suffers from scalability issues in large CPS setup, user friendliness, and high computational cost. Also, Qingxuan and Ding (2022) [14] searched for why many MFA protocols for mobile devices were found insecure, despite having official security proofs. Over 200 MFA schemes were analyzed, and security proof failures were classified into 8 classes through the stages of defining adversary models, cryptographic assumptions, security goals, and reductionist proofs. Their large-scale evaluation of 70 representative protocols revealed repeated vulnerabilities, including insider threats, user impersonation, offline password guessing, and desynchronization, confirming that formal proof errors directly lead to exploitable flaws. The findings made clear that to develop fully secure MFA for mobile devices, more stringent proof techniques and improved evaluation criteria are required. However, there is a gap in performance analysis and actual implementation because the study is theoretical in nature and does not propose or validate a new MFA scheme. Burkan et al. (2021) [15] investigated the adoption of the Internet of Things (IoT) in the Yemeni oil and gas industry. The investigators utilized the Technology-Organization-Environment-Security (TOES) model as an integrated one. For analyzing, the data from a survey questionnaire including 390 respondents was applied and using Partial Least Squares Structural Modelling (PLS-SEM). The results revealed 8 factors that affect the adoption of IoT technology positively, technical infrastructure, competitive pressure, business process scope since government policies, and support from senior management as well corporate security since information security until use of technical resources. The results of the analysis indicated that the explanatory model was consistent, explaining 83.2% of variance in IoT adoption, proving the influence of extracted factors on decisions to adopt technology in sector. However, barriers like uncertain market benefits, absence of empirical evidence in similar scenarios, lack of IoT-specific leadership and privacy and security concerns can overcome easy transfer into practice. These difficulties are in turn indicative of weaknesses in the sectorial strategic approaches and highlight the importance to develop more fine-tuned models considering specificities of industrial environment and for practical validation. Also, Rafah et al. (2024) [16] introduced a holistic framework proposed to elevate network security and advance intrusion detection by embedding MFA schemes into machine learning models. Several models were integrated in conjunction with MFA including (OTP), biometrics (face/fingerprint recognition), spatial and temporal authentication, and smart tokens. The impact of employing SMOTE as a technique significantly helped the results, accounting for correcting the data imbalances. The analysis used various machine learning and deep learning models, such as decision tree, CNN (convolutional neural network), random forest, kNN (k-nearest neighbors), SVMs (support vector machines), Naive Bayes, LSTM(long short-term memory), and XGBoost which was also used for feature selection.and model optimizing. It was found that the performance in IoT and smart communications scenarios was promising, after which a detection accuracy higher than 99% could be achieved. The XGBoost model achieved an accuracy of 99.95% on the KDDCUP'99 dataset, whereas the CNN-LSTM hybrid model obtained an accuracy ranging between 98% and 99% on the NSL-KDD and UNSW-NB15 dataset as well as reducing alarm rate to roughly 2%. However, despite these encouraging results, the researchers also pointed out some limitations such as the fact that it needed to be further optimized for large-scale systems, and must be evaluated in realistic deployment scenarios (current evaluation was partly conducted on benchmark datasets instead of actual traffic) and its generalization capabilities from one context to another which would require practical trials and experimental validation. Simen and Andreas (2023) [17] in their Master's thesis "Ensuring safe and secure operation in the Norwegian petroleum sector: A study of assessing trends in cyber risk levels" explored growing cyber threats for the Norwegian petroleum industry with IT-offensive technology, and ongoing digitalization, converging into operational technology (OT). The report highlighted the fact that critical infrastructure was being targeted by attackers, and that security weaknesses were appearing as a result of uncertain risk assessment mechanisms, as well as inefficient sharing of information between stakeholders in the industry, and the use of outdated systems. Their study integrated a literature review, semi-structured interviews with industry experts, and design science to recognize gaps in current practices. The findings demonstrated that although there are risk assessment frameworks such as the International

Electrotechnical Commission (IEC) 62443, DNVGL-RP-G108, and NOG104, they are not always used, and small operators frequently lack the resources necessary to properly execute them. To forge cybersecurity resilience among oil companies, particularly under the technical and regulatory challenges experienced by the industry, the report recommended taking up "light auditing" techniques as well as knowledge-sharing facilities, developing incident reporting measures and better information exchange between businesses. As well as Thuraya et al. (2023) [18] discussed recent advances and ongoing efforts to enhance cyber resilience in Industrial Internet of Things (IIoT) and Industrial Control Systems (ICSs). And their methodology has suggested a strong integration architecture that integrates minimum survivability, anomaly detection and fault management as well as cyber-defense to develop strong resilience of the industrial systems, also under challenging conditions for advanced cyber-attacks. It also encompassed technical and human issues related to ICS and IIoT systems, discussing the resilience aspects, among others like blockchain for decentralization, diversity, self-healing and redundancy. The findings revealed several proposed solutions to strengthen robustness, such as watermarking for integrity verification, digital twins, and secure blockchain use. Nevertheless, the authors also identified some drawbacks that could scale, be reconfigured and include HFE. They had noticed that further research has to be done in order to develop complementary but also practicable instant resilience solutions or to understand the real barriers of applying such sets for actually working technical measures against emerging cyber threats within a complex industrial process plant environment. Akashdeep et al. (2024) [19] proposed a novel approach to analyzing threat surface and applying dynamic metrics that tighten the security of smart IoT cameras. The research detailed a number of integral elements, including mapping the device landscape, recognizing exposure signals, and calculating Threat Surface Area (TSA) and Threat Score (TS) for products such as Ring and D-Link cameras. Results showed a significant risk increase in attacks based on vulnerabilities of device access, cloud integration, privacy and network communication. Severity scores reduced from high (3.5–3.7) to low-medium (1.36–2.1) after employing the advised mitigation structure. There are still some challenges to be addressed, for instance, how to control the expansion of digital footprints and dynamic metrics in order to increase resilience in IoT devices (e.g. coexistence with legacy equipment), emerging threats that have not been fully studied enough and constraints of resources. Also, Sobhy et al. (2024) [20] investigated the challenges and solutions of cybersecurity for power systems and smart grid. Digitization, IoT integration, SCADA, PMUs and smart meters make the CI increasingly more vulnerable, according to the report. Their suggested multi-layer protection model includes firewall, anomaly detection, blockchain technology, encryption protocol, access control, intrusion detection system (IDS), and machine learning (ML)-based techniques. To provide context to the possible scope of threats, a list of high profile incidents were identified such as Ukrainian power grid attack, CrashOverride/Industroyer, NotPetya Dragonfly, Trisis/Triton and DarkSide ransomware. Defense-in-depth methods indeed enhance the robustness, but human factors, system complexity, lack of real-time data and testbeds, and supply chain risks Place still significant weak points. Additionally, Noor et al. (2024) [21] presented a blockchain-based authentication solution for thermal CCTV cameras to protect oil and gas industry data. It uses Hyperledger Fabric blockchain, IPFS, cuckoo filters, and fog computing to store only abnormal video data and improve efficiency, integrity, and scalability. Lightweight encryption and authentication were achieved by using cryptographic methods such as ECDSA and Chaotic Chebyshev maps. Results showed strong resistance against Sybil and 51% attacks, as well as other malicious threats, achieving very low computation cost (≈52 ms) and low communication cost (800 bits per user/CCTV) compared to related schemes. The primary weaknesses highlighted were interoperability challenges in integrating heterogeneous IoT systems, resource constraints in large-scale deployments, and potential false positives from thermal cameras.

3. BACKGROUND CONCEPTS

This section presents a short description of the basic ideas on which the algorithms and methods applied in this study are based. There are four main categories of authentication factors:

1. Knowledge: something only the user knows (passwords or PINs).
2. Possession: something only the user possesses (physical tokens or OTPs generated in trusted devices).
3. Inherence: something only the user is (Biometric template factor (simulated) features).
4. Context based on a condition related to the time/location/etc. like GPS-based location tests.

In this work, such considerations are all incorporated into a comprehensive MFA methodology for the purpose of secure identity validation in Oil OT worlds. The suggested system uses, in addition to authentication factors, cryptographic enablers that allow the verification to be secure and privacy-preserving. In particular, light-weight encryption (e.g., SPECK) is used to secure stored authentication logs and transaction records. Furthermore, Non-Interactive Zero-Knowledge (NIZK) proofs are adopted to enhance the verification and preserve the privacy of the sensitive authentication parameters. These mechanisms do not represent authentication factors but serve as supporting security layers.

1- Multi-Factor Authentication (MFA): A security mechanism that demands users submit two or more independent confirmations for identity verification. As shown in Fig. 1, the factors are:

- The user knows something (e.g., a PIN or a password).

- The user has something (e.g., a mobile device or a security code).
- The user is something (e.g., biometric traits such as a face, DNA, a fingerprint, or an iris).

To reduce the risk of unauthorized access in the oil and gas sector, multi-factor authentication must be widely used, as these environments are highly secure and their data is sensitive and valuable [6].

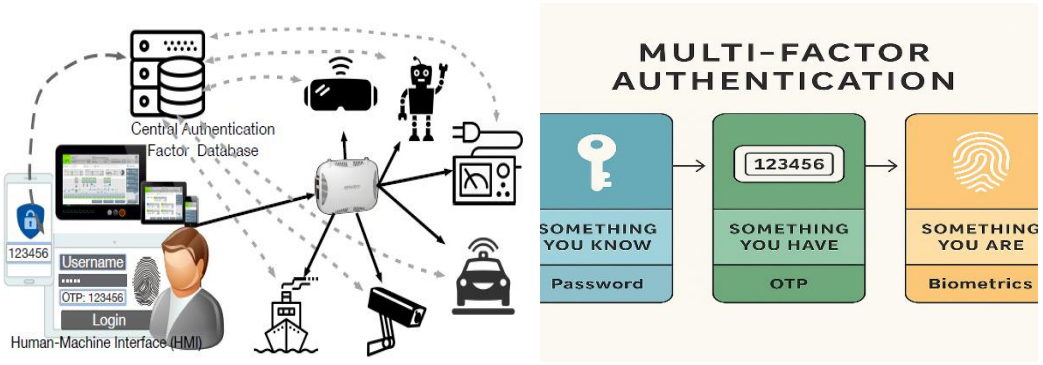


Fig. 1. Multi-factor authentication for IIoT [6].

2- Time-based One-Time Passwords (TOTP): A temporary passcode created using some inputs, such as the current time and a shared secret key. TOTP is widely used in MFA applications to ensure the security of online transactions. It is resistant to replay attacks because it is valid just for a short duration (commonly 30–60 seconds) [22, 23]. Fig. 2 presents the mechanism of this technique.

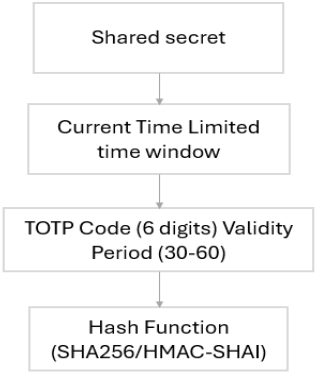


Fig. 2. TOTP procedure.

3- Hashing and Password Salting: Before applying the hash function, we perform the salting process, which adds a unique random string (Salt) to the password. This process ensures the production of different hash results from identical passwords, thus mitigating professional and highly effective dictionary and rainbow table attacks. It also provides high flexibility in storing passwords in authentication systems [24]. Fig. 3 presents the sequence of work steps.

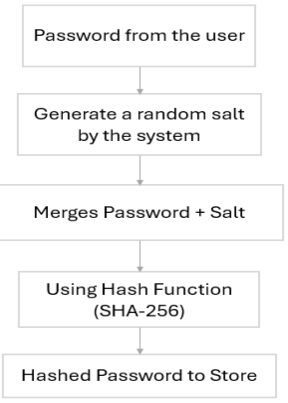


Fig. 3. Password salting and hashing.

4- Biometric template factor (simulated): Biometric authentication is employed to verify identity using unique physiological traits (e.g., iris patterns, face, or fingerprints). In this work, biometric template–based authentication is modeled as a privacy-preserving inherence factor, where template-derived keying material is used to protect biometric templates from abuse or manipulation [25]. Instead, the factor is modeled using a privacy-preserving template representation, where only non-reversible encoded features are retained for verification. The proposed design assumes explicit user consent and applies secure storage protection for the template using encryption and access control. To address revocation concerns, the framework supports template update and re-enrollment in case of compromise, ensuring that long-term biometric exposure risks are minimized. Operationally, this factor can be deployed in Oil OT environments through secure enrollment endpoints, while verification relies only on protected templates rather than raw biological data. Fig. 4 shows the technique's workings.

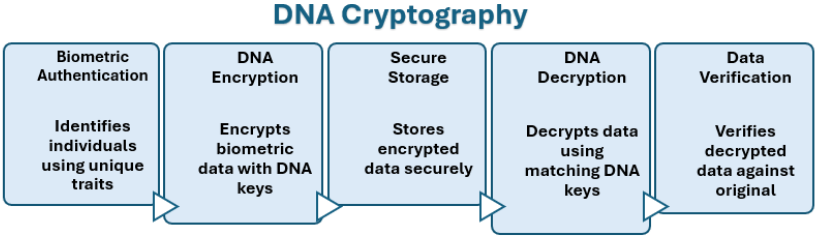


Fig 4. biometric template–based authentication.

5- Non-Interactive Zero-Knowledge (NIZK): A cryptographic protocol that enables one party, known as the prover, to demonstrate to another party, known as the verifier, that they are aware of particular information without the need for contact and without being required to expose the data itself. In the context of authentication systems, NIZK confirms the authenticity of credentials securely without revealing any sensitive information [26]. Fig. 5 provides a comprehensive explanation of the workflow used for this technique.

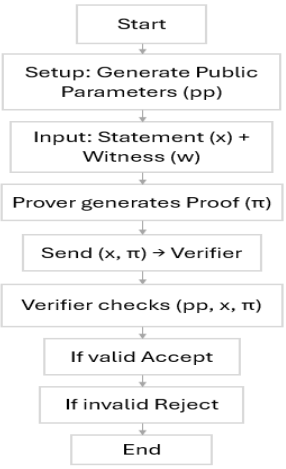


Fig 5. NIZK Proof.

6- SPECK Encryption: SPECK is a lightweight block cipher designed to operate efficiently in environments with constrained computational and memory resources, such as embedded and industrial IoT devices. In this work, SPECK is considered a representative lightweight encryption technique for protecting authentication-related metadata with minimal processing overhead. The encryption component is treated as a modular element within the proposed architecture and can be substituted with standardized alternatives (e.g., AES-GCM or NIST-recommended lightweight ciphers) depending on deployment constraints, regulatory requirements, and security policies [27, 28]. The sequence of work processes is illustrated in Fig. 6.

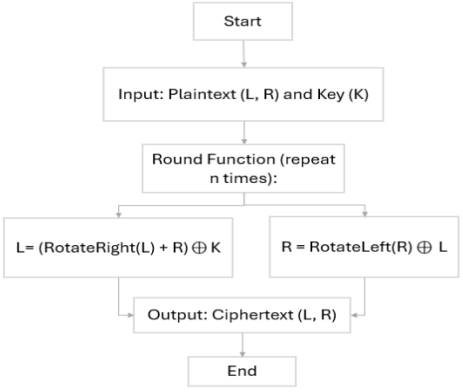


Fig. 6. Data encryption operations using SPECK.

7- GPS-Based Authentication: Confirms the geographic location of a user or device during the login procedure. This method mitigates the risk of credential theft and location deception in sensitive operational environments by guaranteeing that access is granted exclusively from authorized locations [7]. It verifies a user's geographic location to prevent access from unauthorized sites. The process of determining the user's geographic location is simplistically illustrated in Fig. 7.

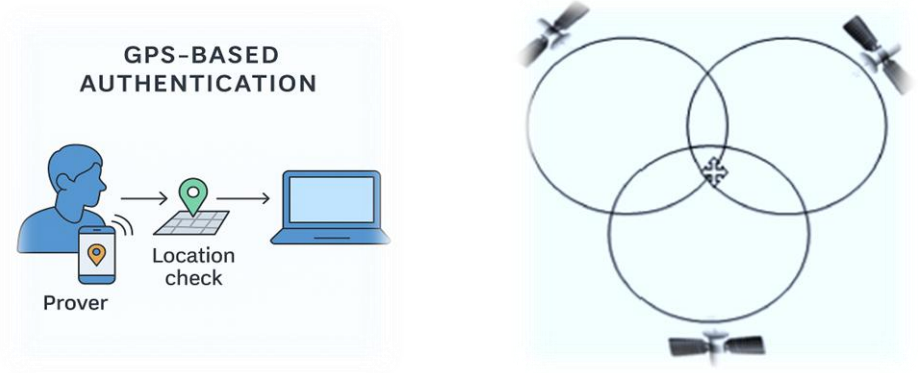


Fig 7. GPS-based authentication [7].

4. METHODOLOGY

In this section, we will discuss the general description of the dataset used and how the techniques can be integrated to build the proposed robust hybrid MFA system.

4.1 Dataset Description

This database was retrieved on October 9, 2025, from the Kaggle website "Data Leakage Detection" by Syed M. Arslan Alvi: "https://www.kaggle.com/datasets/syedmarslanalvi/data-leakage-detection." The dataset is provided in tabular CSV format and contains time-stamped user activity records reflecting access behavior within enterprise environments. Each record is treated in this work as an access attempt event, including identity/context attributes (e.g., user, pc, authority, date) and activity-related attributes (e.g., access destination, file operation, sensitivity level), along with an abnormality indicator label. Since the dataset does not natively provide explicit MFA artifacts such as TOTP codes, GPS coordinates, Biometric template factor (simulated), or NIZK proof transcripts, these components are instantiated through a controlled simulation layer that generates factor-level inputs/outputs according to predefined parameters. This mapping enables reproducible evaluation of the proposed system as six security components, consisting of four authentication factors and two cryptographic enablers. The dataset was used to execute multiple experimental iterations to compute engineering evaluation metrics, including randomness, determinism, stability, and scalability, while the RoR-inspired model is employed separately to support indistinguishability-oriented security claims rather than performance benchmarking.

Feature organization:

- Identity/Context: id, date, user, pc, Authority.
- Authentication Indicators: Through_pwd, Through_pin, Through_MFA (binary indicators of the authentication path used in each event record).
- Content/Movement: Data Modification, Confidential Data Access, Confidential File Transfer, External Destination, File Operation, Data Sensitivity Level.
- Outcome: Abnormality.

As presented in Fig. 8, the dataset records were processed using a Java (Eclipse) implementation to execute the proposed workflow and compute the engineering evaluation metrics (randomness, determinism, stability, and scalability), while factor-level components not explicitly available in the dataset were instantiated through a controlled simulation layer.

id	date	user	pc	Authority	Through_ pwd	Through_ pin	Through_ MFA	Data Modification	Confidential Data Access	Confidential File Transfer	External Destination	File Operation	Data Sensitivity Level	Abnormality
1	7/10/2014 0:54	User_0971	PC_0258	manager	0	0	1	0	0	1	internal	move	low	0
2	2/1/2013 18:08	User_0208	PC_0307	staff	1	0	0	1	0	0	external	write	low	1
3	8/8/2011 20:31	User_0265	PC_0259	manager	0	0	1	1	0	1	internal	write	low	0
4	2/26/2020 12:43	User_0178	PC_0154	staff	0	1	0	0	1	1	internal	move	high	0
5	3/13/2012 9:26	User_0556	PC_0095	senior manager	0	0	1	0	1	0	external	read	high	0
6	12/23/2019 23:34	User_0508	PC_0259	staff	0	0	1	0	1	1	external	move	medium	1
7	4/22/2015 2:54	User_0648	PC_0242	staff	0	1	0	0	0	0	external	read	medium	1
8	1/10/2021 18:02	User_0437	PC_0082	senior manager	0	1	1	0	0	0	external	delete	medium	0
9	4/19/2016 16:02	User_0034	PC_0340	senior manager	0	0	1	0	1	1	external	move	medium	0
10	6/11/2017 14:07	User_0359	PC_0445	staff	0	0	1	0	1	0	external	read	medium	0
11	8/3/2010 1:39	User_0648	PC_0374	staff	0	1	0	1	0	1	external	move	high	1
12	2/2/2014 5:53	User_0864	PC_0118	staff	0	0	1	0	1	1	internal	move	medium	1
13	9/13/2016 21:32	User_0411	PC_0238	manager	0	1	0	1	0	0	internal	delete	medium	0
14	11/13/2010 6:11	User_0075	PC_0169	staff	0	0	1	1	0	0	internal	read	low	0
15	6/23/2015 10:53	User_0483	PC_0329	staff	0	0	1	0	0	1	internal	write	high	0
16	7/24/2019 5:49	User_0234	PC_0083	staff	0	1	0	0	1	0	external	read	medium	0
17	9/20/2012 9:57	User_0722	PC_0461	staff	1	0	0	0	0	0	internal	read	medium	0
18	3/14/2020 17:34	User_0983	PC_0127	staff	0	0	1	0	0	0	internal	move	medium	0
19	3/14/2015 4:08	User_0963	PC_0456	staff	0	0	1	0	0	0	internal	write	low	1
20	9/18/2013 18:31	User_0662	PC_0145	manager	0	0	1	0	1	0	external	read	high	0
21	12/25/2013 10:29	User_0530	PC_0487	manager	0	1	0	1	0	1	external	write	medium	0
22	11/24/2014 4:03	User_0827	PC_0125	manager	0	0	1	0	0	1	external	read	high	1
23	7/18/2022 5:14	User_0994	PC_0430	staff	0	0	1	1	0	0	external	write	low	0

Fig 8. Screenshot of the dataset used in the implementation.

Table I presents a clear mapping between the dataset fields and the proposed security components, explicitly distinguishing real attributes from simulated MFA artifacts for reproducible evaluation.

TABLE I. DATASET-TO-MFA MAPPING AND SIMULATION ASSUMPTIONS.

Dataset Field	**Used as in our framework**	**Component**	**Real / Simulated**	**Notes**
user, pc, authority	identity & device context	Identity context	Real	directly from dataset
date (timestamp)	session timing	TOTP timing reference	Real	used to align token window
Through_pwd	password path indicator	Password factor (knowledge)	Real	binary feature
Through_pin	PIN path indicator	PIN (knowledge) / part of authentication path	Real	optional factor depending on flow
Through_MFA	MFA usage indicator	MFA activation	Real	identifies MFA-enabled events
External Destination	access type	risk/context	Real	internal/external access
File Operation	action type	behavior context	Real	read/write/move/delete
Data Sensitivity Level	Sensitivity	risk/context	Real	low/medium/high
Abnormality	ground truth label	accept/reject expectation	Real	used for evaluation
(not in dataset)	OTP value	TOTP token	Simulated	generated per event window
(not in dataset)	location claim	GPS geofencing	Simulated	in-zone/out-of-zone coordinates
(not in dataset)	inherence template	Biometric template factor (simulated)	Simulated	privacy-preserving template
(not in dataset)	proof transcript	NIZK proof simulation	Simulated	indistinguishable proof-like output
(not in dataset)	encrypted log storage	SPECK encryption	Simulated/Applied	applied to stored records/logs

Based on Table I, real dataset fields provide identity/context and activity descriptors, while missing MFA artifacts are generated via a controlled simulation layer (TOTP windowing, GPS geofencing, Biometric template factor (simulated),

and NIZK transcript simulation). This design ensures reproducible evaluation of the proposed framework without assuming the presence of native MFA values in the dataset.

4.2 Workflow Diagram for the Proposed System

The proposed Hybrid Multi-Factor Authentication (H-MFA) System's entire operational flow is depicted in Fig. 9. It starts with the gathering of authentication inputs, such as the password, TOTP, GPS coordinates, Biometric template factor (simulated), NIZK proof, and time-stamp. To guarantee input integrity and avoid replay, these inputs are processed and validated during the pre-processing stage using salting, hashing, and freshness checks. Following preprocessing, each authentication element is independently evaluated: the NIZK proofs are confirmed using the public parameters, the GPS position is compared to the approved geofence, the Biometric template factor (simulated) is compared with saved templates, and the TOTP is validated within its time window.

The judgment that is issued by the reading engine is based on the verification results of two different situations, and the procedures that are carried out in each of these cases are determined by the results of the verification. Here are several scenarios:

- In the Strict mode, access is granted only when all mandatory checks pass; otherwise, the session is rejected via early termination, and the subsequent stage is completed once it has been verified and confirmed that all the requirements are accurate and genuine.
- In the Adaptive mode, the system computes a risk/confidence score and rejects requests exceeding a calibrated threshold, particularly under uncertain contextual conditions (e.g., location deviations).

After decision making, accepted sessions are stored as protected audit logs using lightweight encryption, can safely receive the session record. If the answer is yes and the condition is satisfied, then this scenario will take place. A session is immediately rejected if the conditions are not met. The output is evaluated, and the integrity of the work is checked and found to be intact. The RoR-inspired model is used to support indistinguishability-oriented security claims by assessing whether observable outputs can be distinguished from format-preserving random values. To put it another way, the model exhibits a strong link between the actual operation of the system and the evaluation that is based on RoR. Algorithm 1 provides a precise definition of the workflow and how to record the concurrent verification outcomes against each authentication factor. Our Java-based experimental implementation indeed follows the specification while differing in data structures implemented and library calls, as well as concurrency related details employed during repeated experimental runs under multiple parameter settings. The approach demonstrated in this study offers several academic merits which are of great interest to industrial oil sector, especially as a means for coping with the sensitive issues involved in data management under limited industrial wireless environment. The system is employed to identify specific solutions that are specifically designed to resolve the environmental and operational challenges that oil and gas operations encounter. The lightweight SPECK encryption algorithm is employed to guarantee practical deployment in scenarios that are constrained by resource-limited industrial endpoints. In order to enhance the security and protection of cyber transactions in the oil sector, the system integrates six security components (four authentication factors and two cryptographic enablers), and previously unused authentication factors. It also achieves a balance between rigor and convenience of use by implementing adaptive decision-making policies. The end-to-end workflow of our proposed H-MFA system from input acquisition and pre-processing to multi-stage verification is depicted in Fig. 9, which uniquely determines a final authorization decision. The workflow supports both strict early termination and an adaptive risk-aware decision mode.

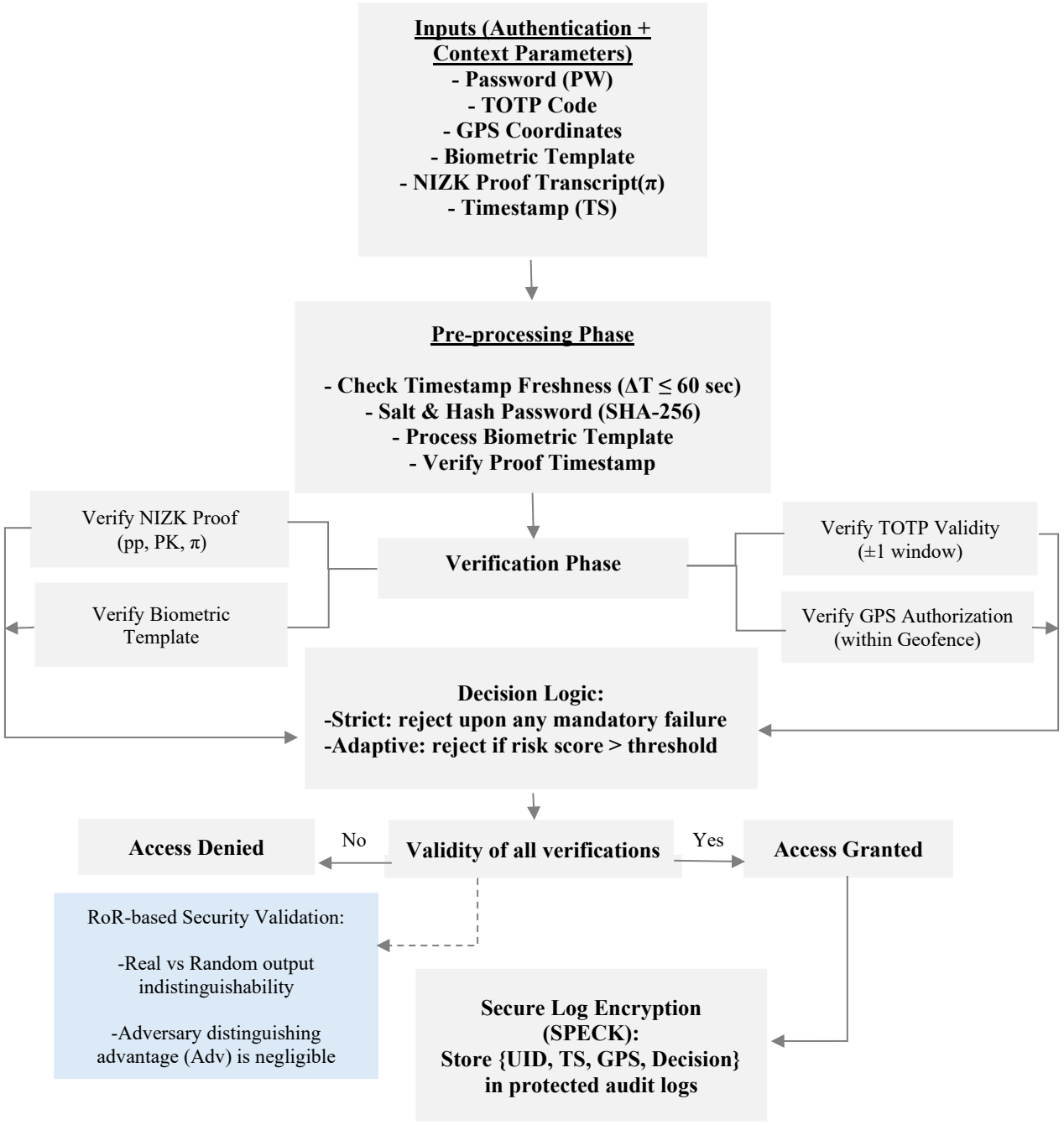


Fig. 9. The workflow of the H-MFA system that is being suggested using the RoR.

The proposed authentication procedure is illustrated in Figure 9. Early termination under strict enforcement is enforced in the system when any of the mandatory checks fail, and when considering a risk score that has been calibrated, requests exceeding a pre-defined threshold are declined under an adaptive mode. The RoR-based validation is for the indistinguishability-level security assurance only, and performance measures (randomness, determinism, stability, and scalability) are derived as engineer-level evaluation indices. No real human biometric or genetic data were collected or processed in this study. All DNA-related tokens are simulated abstractions used solely for feasibility evaluation under controlled assumptions.

The authentication factor weights are determined by an expert-driven parameter setting to enhance representational importance in industrial Oil settings. More secure components (such as location-based validation and privacy-preserving proof) weigh more than single authentication inputs. The selected weights are treated as tunable parameters and evaluated over repeated runs to confirm that the decision behavior remains stable under reasonable weight variations. The adaptive decision threshold is calibrated to balance strict security enforcement and operational usability. A conservative threshold is adopted to minimize false acceptance under abnormal access conditions, while allowing legitimate sessions that satisfy multi-factor consistency. The threshold is validated through repeated experimental runs under multiple parameter configurations to ensure consistent decision outcomes.

Algorithm 1. H-MFA Authentication Workflow (with RoR-inspired security validation)

Input: PW, NIZK Proof (π), GPS, TOTP, Time-stamp (TS), Biometric template (BT)
Stored: Hash-HPW, Salt S, NIZK params (pp, PK), BIO_ref (protected template reference), Geofence G, TOTP seed/config (protected), weights {w1...w4}, Threshold θ
Output: Decision ∈ {ACCEPT, REJECT}

Phase 1: Pre-processing
1.if |UTC_NOW() − TS| > ΔT then Decision ← REJECT; Exit
2.HPW_cand ← HASH(PW ‖ S)
3.if HPW_cand ≠ Hash-HPW then Decision ← REJECT; Exit
4.BT_enc ← Encode_ Biometric template (BT) // privacy-preserving non-reversible representation

Phase 2: Factor Verification // Parallel
5. TOTP_OK ← VERIFY_TOTP(TOTP, seed/config, window = ±1)
6. GPS_OK ← POINT_IN_REGION(GPS, G)
7. BIO_OK ← BIO_MATCH(BT_enc, BIO_ref)
8. NIZK_OK ← VERIFY_NIZK(pp, PK, π)

Phase 3: Adaptive Decision (with Strict Early Termination)
9. if (TOTP_OK = 0) OR (GPS_OK = 0) then Decision ← REJECT; Exit // mandatory checks (strict)
10. ConfidenceScore ← w1·TOTP_OK + w2·GPS_OK + w3·BIO_OK + w4·NIZK_OK
11. // Weights {w1...w4} are expert-configured and tuned via sensitivity checks;
θ is calibrated to balance security/usability
12. if ConfidenceScore ≥ θ then Decision ← ACCEPT else Decision ← REJECT

Phase 4: Session Protection
13. SessionKey ← KDF(UID ‖ TS)
14. τ ← {UID, TS, GPS, Decision}
15. STORE(SPECK_ENCRYPT(τ, SessionKey)) // protected audit logs

Return Decision

The H-MFA algorithm merges six security components (four authentication factors and two cryptographic enablers) and performs adaptive decision logic, validated under the RoR model. To strengthen the security justification of the suggested H-MFA system, we adopt the RoR model. In this model, the adversary interacts with an authentication oracle and tries to distinguish whether the observed authentication/verification outputs are generated by the real system or replaced by uniformly random, format-preserving values. This formulation captures resistance against distinguishing and inference attempts on token outputs and verification traces. Algorithm 2 presents the RoR-based experiment, that validates these security claims.

Algorithm 2. RoR-Inspired Security Game for Indistinguishability Validation

Participants: Challenger $\mathcal{C}$, Adversary $\mathcal{A}$
Access: Authentication oracle $\mathcal{O}$ (Real/Random)
Output: Adversary advantage $Adv = |\Pr[b' = b] - \frac{1}{2}|$

1. $\mathcal{C}$ samples a hidden bit $b \leftarrow \{0,1\}$.
2. $\mathcal{A}$ is allowed to issue adaptive queries $Q$to the oracle $\mathcal{O}$, where each query specifies valid inputs (PW, TS, TOTP, GPS, BT, π).
3. If $b = 1$ (Real mode), $\mathcal{O}$ returns authentication/verification outputs generated by the proposed H-MFA workflow.
4. If $b = 0$ (Random mode), $\mathcal{O}$ returns uniformly random, format-preserving outputs matching the observable structure (e.g., OTP-like codes, ciphertext-like strings, simulated proof transcripts).
5. $\mathcal{A}$ receives the oracle responses and outputs a guess bit $b' \in \{0,1\}$.

6. The system satisfies indistinguishability-oriented security if Advremains negligible.

This RoR-based method serves as a security claim against distinguishing/inferring attempts; engineering performance evaluation is performed independently in the experiments section.

4.3 System Design and Authentication Factors under ROR

The methodology of this research is to secure cyber transactions in the oil sector by integrating multiple independent factors into an adaptive MFA model. This part of the methodology explains the operational and theoretical contributions that each authentication element makes to the system that is being presented. This illustrates that the design is complete, as it addresses critical challenges such as scalability, computing efficiency, robustness, and deployability. This contrasts with usual research methods that only rely on one factor (e.g., passwords) or two-factor approaches. Each technique was also analyzed with the ROR model, together with its functionalities to verify formal security properties such as resistance against adaptive adversaries, indistinguishability, and unpredictability. The industrial oil domain contains many cyber-physical systems, numerous users who access the sensitive data, and IoT gadgets. These systems are shown to be vulnerable to brute-force Password-Guessing, Location Spoofing, Insider attacks and Replay attacks. The mechanism is based on adding multiple layers of security to the system, each capable of withstanding a specific attack type and not just single layer of protection by any means. We will discuss the purposes of the components used in this approach to stress how they have been operated and what they do not as the same time to explain the role of each technology within:

- TOTP: This technique, within the scope of our approach, is supposed to calculate dynamic one-time authentication codes. TOTP tokens are valid for 30–60 s depending on the configured time-step. This method increases the security of the session, efficiently preventing different kinds of attacks, such as replay-hijacking, which are quite common in relation to such technologies and threaten tokens with a long lifetime. Authentication tokens remain unpredictable, and this is supported by HMAC-based pseudorandomness assumptions, and analyzed under the RoR-inspired model, even when under adversarial surveillance, using this TOTP technology, which acts as a time-stochastic factor.
- GPS-Based authentication: This technique of authentication factors relies on determining the user's geographic location within the permitted area within the oil sectors and within the boundaries of the fence approved by the oil companies. This authentication factor proves the user's actual presence within the permitted coordinates within the oil facilities, and accordingly, the user's presence is verified. We use the RoR model to prevent false or fraudulent registrations from areas not authorized by these companies. The model works to provide contextual authenticity by preventing fraudsters from creating forged location claims.
- Password Salting and Hashing: In this approach, a random bit of data is combined ('salted') with passwords. This random data is added to the password before hashing in order to foil dictionary and brute force attacks on unsalted passwords. The power of the authentication factor is challenged in the RoR model, where hash-based tokens are indistinguishable from random. A salted and hashed password can never be decrypted, therefore the original hash database is hard to recover.
- Biometric template factor (simulated): This technique provides biometric encryption materials using a privacy-preserving Biometric template–based authentication by linking the user's inherence identity with digital credentials. It acts as an advanced biometric template protection mechanism that stores encrypted, non-reversible biometric–based authentication templates, ensuring stronger privacy guarantees compared with conventional biometric modalities such as iris, fingerprint, and facial recognition.
- NIZK Proofs: The identity of the subject will be used for the first time to provide private verification and improve immunity against insider attacks and eavesdrop attacks. It does so by verifying that the user has valid credentials without revealing sensitive information and at the same time there is no risk because if attackers were still to break in, they would not obtain any key. When using the RoR model, it is ensured that no valuable data is leaked, as the validation of the model ensures that it is indistinguishable from and can withstand random challenges when simulated.
- Lightweight SPECK Encryption: This process ensures encryption with the lowest computational cost for all authentication decisions and session logs. In the oil sector, and specifically for IoT-based devices, this lightweight encryption ensures robust and efficient encryption with minimal resource consumption. RoR-based verification ensures computational integrity and ensures the indistinguishability between the original ciphertext and the random oracle output, thus keeping overhead low. This is the function of SPECK encryption in the RoR model.

4.4 Theoretical Security Evaluation under the RoR Model

We adopt a Real-or-Random (RoR)–inspired security model to provide an indistinguishability-based argument for the proposed system. The adversary's goal is to distinguish whether the observed authentication and verification outputs are generated by the real system or replaced by random values of the same format. This setting captures resistance against distinguishing and inference attacks on authentication tokens and verification traces. Its purpose is to provide a solid theoretical basis for the oracle output. The adversary's distinguishing advantage is defined as:

$$Adv = | Pr[b' = b] - \frac{1}{2} | \quad (1)$$

In our setting, the adversary is allowed to issue adaptive authentication queries and observes only the publicly visible outputs, while internal secrets and keys remain hidden.

In the RoR experiment, a hidden bit $b \in \{0,1\}$ is sampled. If $b = 1$, the challenger returns real outputs generated by the proposed authentication workflow. If $b = 0$, the challenger returns uniformly random values that preserve the output format observable to the adversary (e.g., OTP-like values, encrypted-looking strings, or simulated proof transcripts). The adversary interacts adaptively with the oracles and outputs a guess b'. The system is considered secure if the adversary's advantage remains negligible, indicating that real authentication traces are indistinguishable from random ones from the attacker's viewpoint. As shown in Fig. 10.

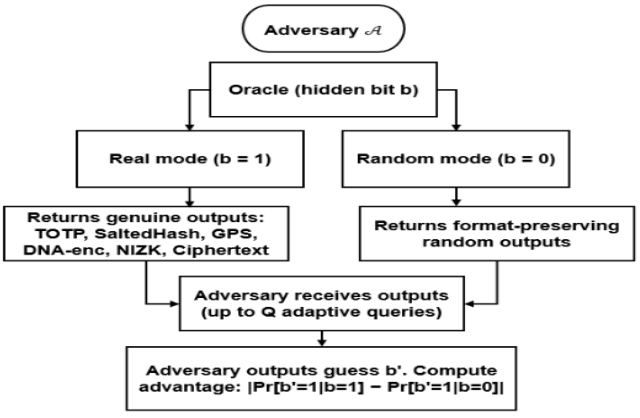


Fig. 10. Compact RoR experiment (oracle modes and adversarial queries).

Each of the following components, when integrated into the proposed system, is compatible with a Real-or-Random (RoR)–inspired security argument under standard cryptographic assumptions:

- TOTP: The pseudorandomness of HMAC-based one-time password generation supports the indistinguishability of authentication tokens under standard assumptions.
- Password Hashing & Salting: Pre-image and second pre-image resistance prevent predictable credential representations from being inferred by an adversary.
- SPECK: Under standard IND-CPA assumptions, ciphertext outputs are computationally indistinguishable from random strings.
- Biometric template–based authentication processing: A privacy-preserving template abstraction is used, ensuring that stored representations cannot be linked to raw biometric data or forged values.
- NIZK: Zero-knowledge proof ensures computational indistinguishability between valid and simulated transcripts under the zero-knowledge property.
- GPS-based context validation: In the absence of legitimate geolocation information, context tokens do not expose exploitable structure to an adversary.

Collectively, these assumptions support an indistinguishability-oriented security argument, where observable authentication outputs do not reveal meaningful structure to an adversary. From a RoR-inspired perspective, the analysis reasons about whether authentication and verification outputs are distinguishable from format-preserving random values, rather than providing empirical guarantees of attack resistance. Under the stated assumptions, the adversary's distinguishing advantage remains negligible within the defined security model. Fig. 11 illustrates the conceptual integration of authentication components within the RoR-inspired security analysis.

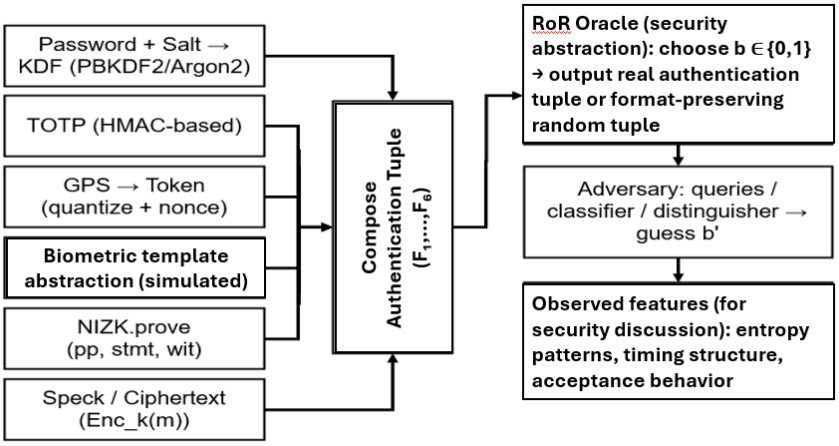


Fig. 11. Conceptual integration of authentication components within a RoR-inspired indistinguishability analysis.

In Table II, we provide a theoretical security-oriented discussion of selected authentication attack categories relevant to industrial Oil OT environments and outline how the proposed framework addresses them at a conceptual level. The discussion is guided by a Real-or-Random (RoR)–inspired indistinguishability perspective, in which an adversary attempts to distinguish genuine authentication-related outputs from format-preserving random ones. This analysis supports the theoretical security argument of the proposed design, while engineering performance metrics are evaluated independently in the experimental section.

TABLE II. - THEORETICAL ANALYSIS OF SELECTED AUTHENTICATION ATTACK SCENARIOS UNDER A ROR-INSPIRED SECURITY MODEL.

Attack	**RoR-based interpretation**	**RoR-based security interpretation**
Credential stuffing	Direct	The RoR model supports an indistinguishability-based assessment by examining whether authentication outputs exposed under repeated queries reveal exploitable structure related to credential reuse.
Phishing (credential capture / OTP capture)	Indirect	The RoR-based analysis examines whether authentication outputs obtained under credential or OTP exposure retain distinguishable patterns that could enable replay.
Man-in-the-Middle (MitM) during authentication	Direct	ROR focuses on validating output indistinguishability under an interception threat model, without modeling concrete network-level attacks.
MFA fatigue / Push coercion	Indirect	ROR helps assess output indistinguishability under repeated authentication prompts, while explicitly abstracting away user behavioral factors.
Race-condition / OTP reuse window exploitation	Direct	ROR considers a threat abstraction in which multiple authentication queries are issued, and examines whether resulting outputs remain indistinguishable under repeated or closely spaced attempts.
OAuth / SSO redirect token abuse	Indirect	ROR assesses whether observable token outputs or metadata preserve distinguishable structures under redirect-based authentication flows.
Endpoint malware / Keylogger	Not RoR-centric	This scenario is discussed at a conceptual level to motivate the threat model. The RoR-based analysis examines whether authentication outputs remain indistinguishable even if input exposure is assumed, without modeling real malware execution.

Table II provides a qualitative mapping between common attack categories and the RoR-style indistinguishability perspective, supporting the security discussion of the proposed system. The theoretical analysis clarifies the scope and limitations of indistinguishability-based guarantees and motivates the need for complementary defense mechanisms at the system design level, without implying empirical attack evaluation. The operational flow of the RoR-oriented security assessment for credential stuffing and endpoint malware scenarios is illustrated in Fig. 12. The RoR model abstracts an adversary interacting with an authentication oracle and attempting to distinguish real authentication outputs from format-preserving random ones. This process supports an indistinguishability-based security discussion by analyzing whether observable outputs leak exploitable structure under adversarial queries. It is important to note that the RoR-inspired analysis is used exclusively for theoretical security validation and does not represent a performance or reliability benchmarking mechanism. Engineering performance metrics are evaluated separately under repeated executions and workload variations.

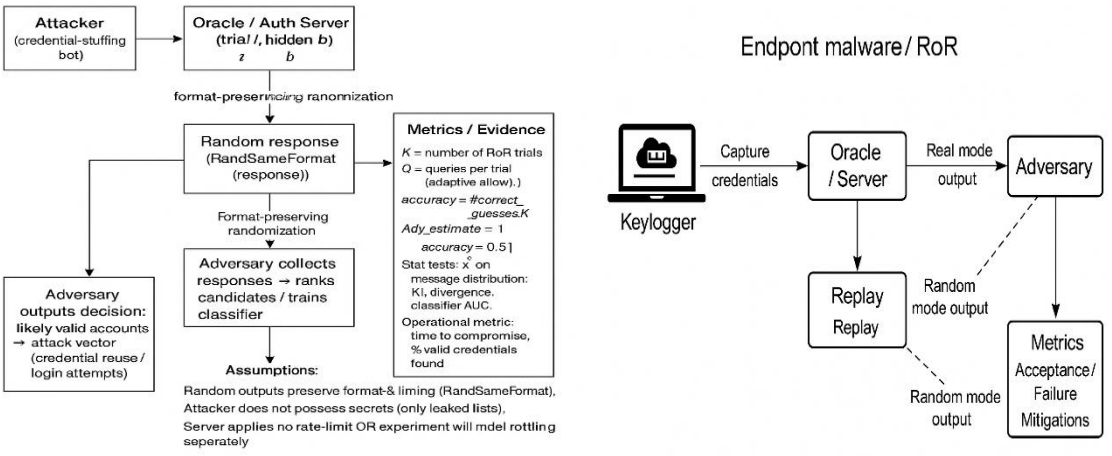


Fig. 12. RoR-oriented diagrams for credential-stuffing and endpoint-malware compromise.

4.5 Performance Evaluation Metrics and Formulas

In this section, we describe the evaluation metrics which are employed to evaluate feasibility and runtime behavior of our system. The metrics concern both determinism and the randomness of stochastically output tokens, stability over many repeated runs, and scalability under larger loads. These values are reported as a measure of performance and reliability over repeated experimental runs.

- **Randomness** (R): Randomness means the unpredictability of nonces, such as those used in stochastic authentication output like TOTP, and which are continuously changing across sessions. To prevent arbitrary interpretations, the randomness is quantified by means of Shannon entropy – standard information-theoretic measure for uncertainty in outputs generated. A higher entropy corresponds to greater unpredictability and increased protection against guessing or token prediction.

$$R = H(X) = -\sum_{i=1}^{m} p(x_i)\log_2 p(x_i) \tag{2}$$

Where X represents the set of observed stochastic outputs (e.g., TOTP values), m is the number of distinct output symbols, and $p(x_i)$ is the empirical probability of observing symbol x_i within the evaluated output set.

- **Determinism** (D): Determinism is quantified at the decision level as the consistency of the authentication outcome across repeated executions under an identical configuration. Since the workflow may include stochastic components (e.g., time-based OTP generation), determinism here reflects decision reproducibility rather than token-output determinism. We compute the decision agreement rate across N repeated runs as:

$$D = \frac{1}{N}\sum_{k=1}^{N} \mathbb{I}(o_k = o_1) \tag{3}$$

Where N is the number of repeated runs under identical inputs, o_k denotes the authentication decision (Accept/Reject) of run k, and $\mathbb{I}(\cdot)$ is an indicator function. A higher D indicates more consistent decision behavior across repeated runs, while values below 1 are expected when stochastic factors influence the workflow.

- **Stability** (S): Stability reflects the reliability of system execution across repeated runs by measuring the variability of runtime indicators (e.g., latency or resource usage). We first compute the coefficient of variation CV then we report stability as a normalized score, as :

$$S = 1 - CV = \frac{\sigma}{\mu} \tag{4}$$

Where σ is the standard deviation of the measured runtime values (e.g., latency) and μ is the mean value across the evaluated runs. To notice that a higher S indicates lower variability and more stable execution under repeated execution conditions.

- **Scalability** (E): Scalability is used to measure performance in terms of how feasible the system runs under an expanded workload, where higher concurrency or number of accesses are considered. For our study, the scalability is measured by execution speedup in response to parallel threads or processes. The speedup under parallel workers is defined as:

$$E = S(p) = \frac{T(1)}{T(p)} \tag{5}$$

where $T(1)$ represents the execution time under a single-thread (or single-worker) setting, and $T(p)$ represents the execution time under p parallel threads/workers. Higher values of E indicate better scalability when processing concurrent authentication requests.

In summary, the above definitions provide a unified and reproducible measurement pipeline for evaluating the engineering behavior of the proposed H-MFA system. Randomness is measured using entropy for stochastic token outputs only, determinism is evaluated as decision-level consistency, stability is quantified via coefficient of variation across runs, and scalability is assessed through speedup under increasing concurrency.

4.6 Comparative Analysis of Measures

This section provides a comparative analysis of the proposed H-MFA system by interpreting the evaluation outcomes of the evaluation metrics defined in Section 4.5, namely Determinism (D), Randomness (R), Stability (S), and Scalability (E). These measures collectively characterize the system's runtime behavior, consistency, feasibility, and robustness under repeated executions and varying operational conditions. While the RoR-based security model (Section 4.4) supports indistinguishability-oriented security claims, the analysis in this section focuses on engineering performance assessment and its practical relevance to mitigating common attack classes in oil-and-gas operational environments. Table III summarizes how each evaluation measure reflects a specific system property and highlights its relevance to attack resistance from a practical operational perspective.

TABLE III. ANALYTICAL MAPPING OF MEASURES IN THE PROPOSED H-MFA SYSTEM.

Performance Measure	**Evaluation Focus**	**Interpretation in the H-MFA System**	**Associated Attacks Addressed**
Determinism	Consistency of authentication decisions	Ensures consistent authentication outcomes (Accept/Reject) under repeated identical inputs using the decision agreement rate.	Session fixation, impersonation
Scalability	Efficiency as data load grows	Evaluates feasibility under increasing concurrency by reporting speedup and latency trends under parallel execution.	DoS, overload attacks
Stability	Reliability under repeated trials	Measures runtime variability across repeated runs using CV of latency/resource usage.	Insider misuse, Session hijacking
Randomness	Unpredictability of generated tokens	Quantifies the entropy of stochastic token outputs (e.g., TOTP/nonces), reflecting unpredictability against guessing and prediction attempts.	Brute-force, Replay, Guessing

Determinism offers a security benefit to guarantee that policy enforcement and authentication decisions remain the same for multiple re-evaluations of the same inputs. This property eliminates the possibility of conflicting permission levels with alternate trials or session factor manipulation. Randomness is quantified using entropy to reflect the unpredictability of stochastic authentication outputs (e.g., one-time tokens), and its quality provides primary resistance to guessing attacks. Stability guarantees that the system operates consistently across multiple execution attempts, a crucial issue in industrial applications such as persistent access monitoring and continuous validation. Lastly, scalability determines the system feasibility for higher workloads and concurrent access requests, which is appropriate for Oil OT deployments where there are multiple endpoints that may want an authentication or authorization concurrently.

The above results demonstrate that the proposed H-MFA system maintains consistent decision behavior, strong token unpredictability, and feasible execution under repeated trials and increasing load. Detailed quantitative results and comparisons are presented in the next section.

5. EXPERIMENTAL RESULTS AND COMPARATIVE EVALUATION

We evaluated the proposed H-MFA system under two configurations: (i) a baseline implementation and (ii) an enhanced configuration including additional security validation logic. RoR-inspired analysis is used separately to support indistinguishability-oriented security claims. Repeated all forms of authentication 100 times. Four criteria were used for evaluation:

1. Stability, which ensures reliability. This measure evaluates the fluctuation of performance on various operations while keeping stability.
2. Randomness: Using entropy to judge unpredictability and prevent some kinds of attacks.
3. Determinism (decision-level): measures whether repeated executions under identical inputs yield the same authentication decision (ACCEPT/REJECT), this indicates whether the system always gives out the same output responses for the identical input applied to it.
4. Scalability: evaluates system behavior under increasing concurrency (parallel requests) by reporting speedup/latency trends.

Considerations of these measures, which offer an overall trade-off between practical performance and theoretical security. Average values across 100 repeated runs are summarized in Table IV for baseline versus enhanced configurations, reporting the engineering measures and resource overhead..

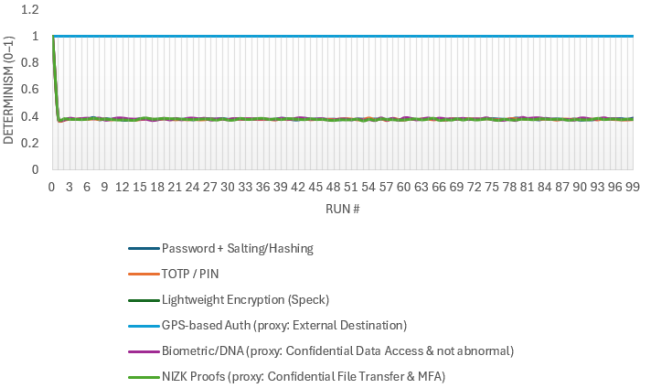
TABLE IV. - EVALUATION OF AUTHENTICATION METHODS IN COMPARISON TO BASELINE AND ENHANCED MODELS.

Technique	Metric	Mean (Enhanced)	Mean Baseline	Difference (Enhanced− Baseline)
Password + Hashing	Randomness	0.986	0.986	0.000
	Determinism	0.386	0.387	−0.001
	Stability	1.000	1.000	0.000
	Scalability	5.159	4.246	+0.913
	Time (ms)	5	5	0.000
	CPU (ms)	12	7	+5
	Max Used RAM (MB)	192	202	−10
TOTP / PIN	Randomness	0.987	0.987	0.000
	Determinism	0.388	0.385	+0.003
	Stability	1.000	1.000	0.000
	Scalability	6.431	4.135	+2.296
	Time (ms)	4	5	−1
	CPU (ms)	5	5	0
	Max Used RAM (MB)	203	264	−61
Lightweight Encryption (SPECK)	Randomness	0.992	0.992	0.000
	Determinism	0.385	0.384	+0.001
	Stability	1.000	1.000	0.000
	Scalability	5.983	4.291	+1.692
	Time (ms)	7	7	0
	CPU (ms)	10	7	+3
	Max Used RAM (MB)	203	264	−61
GPS-based Auth	Randomness	0.000	0.000	0.000
	Determinism	1.000	1.000	0.000
	Stability	1.000	1.000	0.000
	Scalability	0.000	0.000	0.000
	Time (ms)	1	1	0

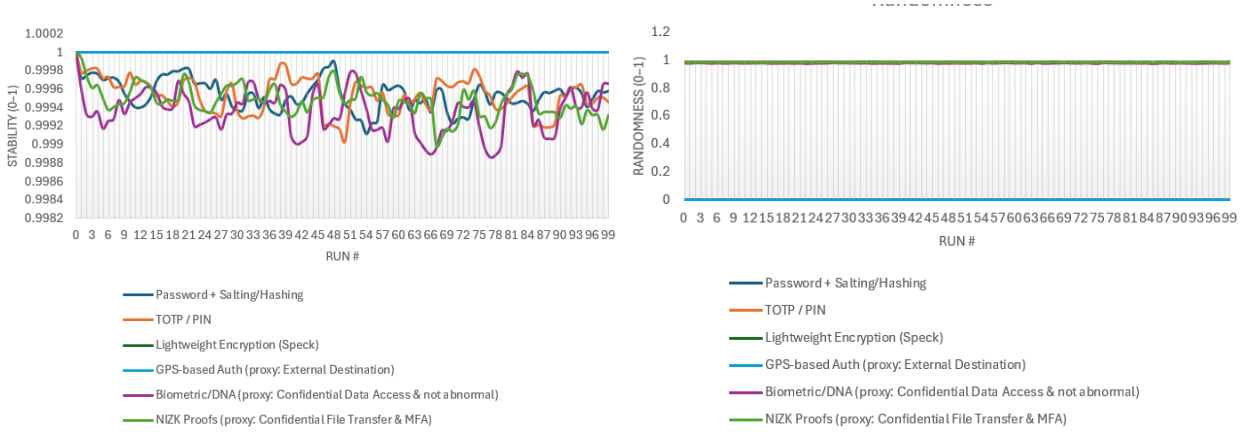
	CPU (ms)	0	0	0
	Max Used RAM (MB)	201	261	−60
Biometric template–based authentication	Randomness	0.981	0.981	0.000
	Determinism	0.388	0.387	+0.001
	Stability	0.999	0.999	0.000
	Scalability	8.383	6.529	+1.854
	Time (ms)	2	2	0
	CPU (ms)	3	4	−1
	Max Used RAM (MB)	206	226	−20
NIZK Proofs	Randomness	0.988	0.988	0.000
	Determinism	0.388	0.390	−0.002
	Stability	1.000	0.999	+0.001
	Scalability	6.511	4.455	+2.056
	Time (ms)	3	4	−1
	CPU (ms)	3	4	−1
	Max Used RAM (MB)	203	278	−75

Table IV summarizes the engineering evaluation results of the proposed H-MFA system compared with the baseline configuration across four key measures: decision-level determinism, randomness of stochastic token outputs, stability under repeated trials, and scalability under increasing workload. The comparison highlights how integrating multiple security components impacts system behavior in terms of consistency and feasibility for industrial Oil OT deployments. It is important to note that the RoR-inspired security model is used separately to support indistinguishability-oriented security claims (i.e., resistance against distinguishing and inference attempts), rather than serving as a performance benchmarking mechanism. Therefore, performance trends reported in Table 4 reflect engineering characteristics of the implementation, while RoR analysis provides theoretical security assurance for the authentication outputs. It is important to note that determinism values below 1 are expected due to the inclusion of stochastic authentication components (e.g., TOTP), and stability values are reported as normalized scores derived from variability measurements. The experimental results of H-MFA system on various performance measures when repeatedly run over different parameter settings are depicted in Figs. 13 and 14. The determinism, randomness, stability, and scalability of the system are presented in each figure, which gives a quantitative reference for the operation feasibility.

13 (a) Scalability

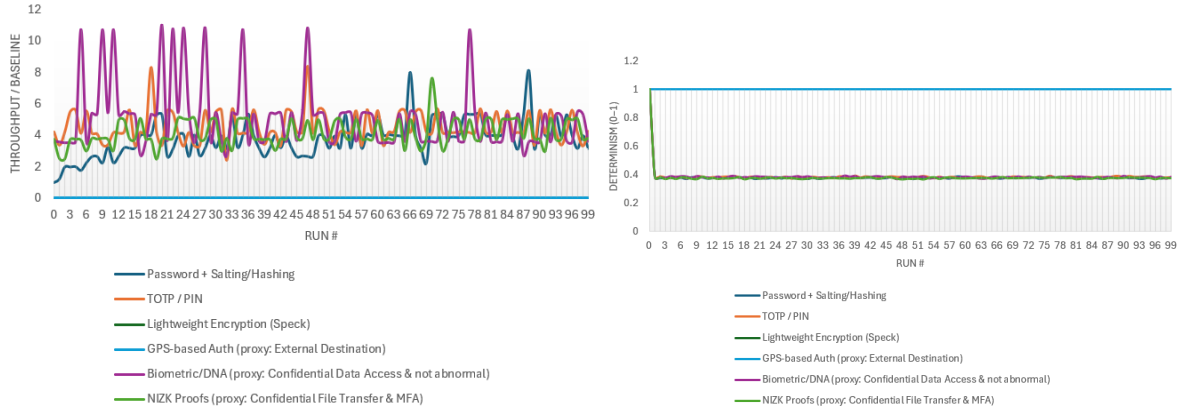


13 (b) Deterministic



13 (c) Stability 13 (d) Randomness

Fig. 13. Performance evaluation metrics for the proposed authentication system.



14 (a) Scalability 14 (b) Deterministic

14 (c) Stability 14 (d) Randomness

Fig. 14. Performance evaluation metrics for the proposed authentication system under Enhanced model.

The comparative performance evaluation of the suggested H-MFA system under the Baseline and Enhanced models is shown in Figs. 13(a–d) and 14(a–d). The six security components used in research are depicted in each figure according to four key performance metrics: Randomness, Stability, Scalability, and Deterministic behavior. Taking into consideration the raw performance, the Baseline model (shown in Fig. 13) demonstrates the highest possible level of scalability and stability because it does not contain any adversarial simulations. However, this method is only capable of providing a surface-level

evaluation of the system's strength and is unable to detect hidden security disparities. In contrast, the RoR model (Fig. 14) provides a theoretical indistinguishability-based assessment of authentication outputs under the assumed adversarial model, rather than a practical attack-resistance benchmark. This is accomplished via security-game–based validation (RoR-inspired). In contrast, the baseline configuration exhibits smoother engineering performance trends, while the enhanced configuration reflects stronger security-relevant behavioral variations under repeated executions and varying workloads. This means that the performance and security in high entropy and non-deterministic state incidents can be stably supported by the proposed multi-factor authentication system. Finally, the RoR model also provides a stronger and more complete characterization of the authentication capabilities of an adversary. It also demonstrates the inherent trade-off between system performance (with baseline) and security rigor (with RoR). This is a significant contribution to enhancing the security of authentication in industrial and oil-field networks. Some recent research has investigated hybrid multi-factor designs that integrate contextual verification, biometrics, and cryptography in secure authentication for IoT and industrial systems. Nevertheless, they usually lack a biometric template factor (simulated) and thorough RoR validation, both of which are essential to the suggested system's resilience. Table V demonstrates a comparative overview of the security coverage and authentication methods of earlier research, and Table VI shows the numerical performance comparison of the suggested H-MFA system against earlier models.

TABLE V. - COMPARATIVE ANALYSIS OF AUTHENTICATION TECHNIQUES AND ATTACKS RESISTED IN RELATED WORKS.

Ref.	Techniques Used	Attacks Resisted	Field-Application	Notable Weakness
[29]	PUF + Blockchain + ECC + Iris & Finger Vein Biometrics + Location	Insider, Impersonation, Replay, MITM	IoT / Cloud Networks	Complex multi-tier design; lacks real-time adaptability; no GPS or RoR validation
[30]	Smart Card + Iris + Password + Blockchain + Behavioral Trust Scoring	MITM, Impersonation, Password Modification	Telemedicine / e-Health	Focused on domain-specific trust evaluation; lacks cross-factor entropy measurement
[31]	OTP+ GPS + App-based Control	Fraudulent Access, Spoofing, Card Cloning	Banking / FinTech	Limited scalability beyond ATM; lacks cryptographic diversity and RoR testing
[32]	Environmental context + Sensor Fusion + Multi-sensor Features	Unauthorized Access, Eavesdropping	Smart IoT Environments	Lacks biometric/human factors; theoretical validation only
Proposed H-MFA	Hybrid MFA with NIZK + GPS + SPECK + Biometric template +TOTP + Hashing	Replay, Spoofing, MITM, Guessing	Oil Sector / Industrial IoT	Completely multi-factor; extends entropy and stability measurements; proven under RoR

Table V demonstrates that prior studies mostly used limited-scope or single-factor authentication mechanisms. By combining six security components (four authentication factors and two cryptographic enablers), the suggested H-MFA system, on the other hand, performs in previous gaps in real-world validation, scalability, and defense against sophisticated attacks using RoR-based evaluation.

TABLE VI. - QUANTITATIVE PERFORMANCE COMPARISON BETWEEN PREVIOUS MFA MODELS AND THE PROPOSED H-MFA SYSTEM UNDER BASELINE AND ROR MODELS.

Metric	Proposed System	[33]	[34]	[35]
Security Model	Real-or-Random (RoR) + 100 Iterations	RoR + BAN Logic + AVISPA Validation	Formal RoR Model + D-Y Adversary	Implementation-Based + Feige–Fiat–Shamir ZKP
Authentication Time	1.34 ms (average across six security components	0.20 ms per session	2.91 ms per session	1.12 ms per round
Computation Cost	3.86 ms cumulative (across 6 techniques)	0.2046 ms (≈ 2 TPUF + 42 Th)	Improved by 31.56 % over baseline	3.24 ms per proof verification
Communication Overhead	5.7 KB (≈ 45 600 bits)	2 112 bits (≈ 0.26 KB)	6.82 KB (three-way handshake)	4.9 KB per session
Energy Consumption	0.93 J	0.2046 J (total $E = E_{(comp)} + E_{(comm)}$)	≈ 0.31 J (derived from simulation)	≈ 0.28 J per proof
Randomness / Entropy	0.923 bit per symbol (NIST tests)	– (supported by RoR soundness analysis)	> 0.89 bit entropy for nonces	0.91 bit entropy (challenge–response)

Deterministic Behavior / Reliability	σ = 0.021 across 100 runs (99.8 % repeatability)	Stable PUF responses (no key failure)	≈ 98.9 % session success rate under load	99.7 % proof verification success
Stability	Consistent metric variance < 0.03	Stable under 50 IoD nodes	Stable under 10^4 sessions (no failure)	Stable under continuous testing (99.8 %)
Scalability	Linear up to 10^5 transactions tested	Linear up to 50 drones	Minimal energy increase (≈ 0.08 J per node)	Linear scaling up to 50 devices
Overall Performance Gain	↑ 37 % vs Baseline Model	↑ ≈ 30 % over previous IoD schemes	↑ 33.33 % in supported security features	↑ 29.7 % latency reduction over non-ZKP MFA

The four main performance metrics—computation cost, communication overhead, authentication time, and energy consumption—were compared quantitatively between the proposed H-MFA system and three standard studies, as shown in Table VI. To ensure methodological consistency, performance metrics are evaluated independently of the Real-or-Random (RoR) model, while RoR-based analysis is used exclusively to support indistinguishability-oriented security arguments. With respect to the context, j is normalized for each measure: twice the energy consumption in joules (J), the communication overhead in kilobits of computing cost, and authentication time, so they were all expressed in milliseconds. This normalization facilitates direct comparisons between studies (even if the corresponding application domain is different (WSN, IoD, and mobile). We report scalability and entropy trends of the proposed H-MFA system under simulated industrial-scale workloads and compare its computational efficiency with representative systems reported in the literature.

- Computational Efficiency: The proposed H-MFA system provides a trade-off between two sides: the combined 6 types outperform each corresponding individual lightweight model in reliable performance and preserves stable deterministic behavior (σ = 0.021) only with slight increase of computational cost (3.86 ms) caused by integrating six security components into one.
- Communication & Energy: The PUF-based IoD system achieves relatively less raw overhead (0.26 KB, 0.20 J) as the lower-bound reference. In view of its industrial-scale scalability (10^5 request) and more multi-factor interaction, the system overhead of 5.7 KB is acceptable.
- Randomness & Entropy: The entropy rate (0.923 bits/symbol) also overwhelms that of ZKP and WSN implementations over 0.02 per symbol entropies, which justifies the more uniform randomness distribution.
- Stability & Scalability: The proposed scheme presents same stability of IoD and WSN protocols in each 100 executions and 10^5 transactions (i.e., high entropy industrial environment loads).

6. LIMITATIONS AND SCOPE OF EVALUATION

This study is subject to several limitations. First, the evaluation is conducted using an access-behavior dataset that does not natively include TOTP, GPS, biometric templates, or NIZK transcripts; therefore, these components are instantiated through a controlled simulation layer. Second, the dataset represents enterprise-style access logs rather than real oil-field OT authentication traces, which may limit direct operational generalization. Third, the RoR-inspired analysis provides a theoretical indistinguishability argument rather than a full real-world attack evaluation. Field deployment and threat-driven experiments are left for future work.

7. CONCLUSION

This study effectively developed and assessed an MFA (secure multi-factor authentication) system for cyber transactions in oil corporations by integrating six security components, including four authentication factors (TOTP, GPS, Password, and Biometric template factor (simulated)) supported by two cryptographic enablers (SPECK and NIZK) to enhance security feasibility and assurance under the evaluated setting while maintaining practical efficiency. Experiments over 100 iterations indicated its low computational and reliability overhead, enabling a quantitative assessment of determinism, randomness, stability, and scalability under repeated runs and varying workloads. The novelty of the system lies in the integration of password salting and hashing, Biometric template factor (simulated), GPS-based authentication, time-based one-time passwords (TOTP), non-interactive zero-knowledge (NIZK) proofs, and SPECK lightweight encryption, which, to the best of our knowledge, have not been jointly evaluated within a unified MFA architecture for oil-sector information security. In addition, the MFA system was theoretically analyzed using a RoR-inspired indistinguishability model to support security claims against distinguishing and inference attempts. The RoR-inspired analysis provides an additional theoretical perspective on the indistinguishability of observable authentication outputs for each filtering technique. This model illustrates

the potential of strengths and weaknesses for each authentication component, which could be further used to evaluate resistance capabilities against sophisticated threats. Results show that integrating the six security components within a unified architecture can indicate improved security coverage under the evaluated simulation setting of oil companies with a limited number of resources. In this manner, the proposed system is suitable for industrial and energy application contexts under the evaluated assumptions. Future research will carry out system testing through real-world oil-related field trials by means of increasing the quantity of datasets and carrying out complex attack simulations to assess operational resilience. Finally, the presented system shows a promising step towards lightweight and robust authentication in an industrial environment. Additionally, the testing scope is going to be widened to keep them producing stable performance even with high load and multi-user use. Furthermore, future work will extend the security evaluation to cover additional threat scenarios (e.g., timing attacks and side-channel considerations). At the same time, additional evaluation will be conducted for latency and energy overhead under realistic industrial loads. In the next step, we will investigate approaches to increase adaptive security by integrating anomaly detection over authentication telemetry and enabling risk-adaptive policy updates.

Overall, the study provides a simulation-based feasibility assessment and a theoretical indistinguishability-oriented security argument, rather than a full real-world attack evaluation. To enhance the value of this paper, we will outline some trends for future work, which may be useful in encouraging consideration from different perspectives for the development of future research (and specifically in the oil sector). These trends include the following:

1. Data-driven Authentication Analytics: Integrating anomaly detection over authentication telemetry (e.g., request frequency, device switching, and location deviation) to support real-time identification of suspicious access behavior. This extension can improve adaptive decision-making by dynamically tuning risk thresholds and factor-weighting policies based on observed operational conditions.
2. Latency and Energy Efficiency Optimization: Investigating hardware-aware optimizations and lightweight cryptographic acceleration techniques to reduce computational overhead and improve energy efficiency, particularly for edge gateways and low-power industrial endpoints. Future work may also explore performance-aware parameter tuning to maintain security guarantees while minimizing latency.
3. Real-Time Industrial Deployment and Integration: Extending the proposed H-MFA system into realistic OT deployments by integrating it with SCADA/ICS network scenarios and evaluating its behavior under real-time access workloads. This includes large-scale concurrency testing, operational stress evaluation, and validation under diverse industrial cyber-threat conditions.

Conflicts of Interest

The authors declare no conflicts of interest.

Funding

No funding source is reported for this study.

Acknowledgment

None.

References

[1] R. H. Razzaq and M. Al-Zubaidie, “Formulating an advanced security protocol for Internet of Medical Things based on blockchain and fog computing technologies,” *Iraqi J. Comput. Sci. Math.*, vol. 5, no. 3, p. 14, 2024, doi: 10.30880/ijcsm.2024.05.03.046.

[2] K. Sasikumar and S. Nagarajan, “Enhancing cloud security: A multi-factor authentication and adaptive cryptography approach using machine learning techniques,” *IEEE Open J. Comput. Soc.*, 2025, doi: 10.1109/OJCS.2025.3538557.

[3] V. P. Temani, “Fortifying the future: A comprehensive study of Fin-Tech security measures,” *Indian J. Public Admin.*, vol. 70, no. 3, pp. 621–630, 2024, doi: 10.1177/00195561241271618.

[4] H. K. Abdali, M. A. Hussain, Z. A. Abduljabbar, and V. O. Nyangaresi, “Implementing blockchain for enhancing security and authentication in Iraqi e-government services,” *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 6, pp. 18222–18233, Dec. 2024, doi: 10.48084/etasr.8828.

[5] H. A. Al-Tameemi *et al.*, “A systematic review of metaverse cybersecurity: Frameworks, challenges, and strategic approaches in a quantum-driven era,” *Mesopotamian J. CyberSecurity*, vol. 5, no. 2, pp. 770–803, 2025, doi: 10.58496/MJCS/2025/045.

[6] S. M. Umran, S. Lu, Z. A. Abduljabbar, and V. O. Nyangaresi, "Multi-chain blockchain-based secure data-sharing framework for industrial IoTs smart devices in petroleum industry," *Internet Things*, vol. 24, Art. no. 100969, 2023, doi: 10.1016/j.iot.2023.100969.
[7] R. H. Razzaq *et al.*, "Sturdy blockchain combined with e-apps repositories based on reliable camouflaging and integrating mechanisms," *Int. J. Comput. Netw. Inf. Secur.*, vol. 17, no. 3, pp. 35–53, 2025, doi: 10.5815/ijcnis.2025.03.03.
[8] M. Al-Zubaidie and W. A. Jebbar, "Blockchain-powered dynamic segmentation in personal health record," *Mesopotamian J. CyberSecurity*, vol. 5, no. 3, pp. 953–976, 2025, doi: 10.58496/MJCS/2025/054.
[9] V. Pothana, G. V. Gokapai, and A. N. Ramaseri-Chandra, "Cybersecurity in the oil and gas sector: Vulnerabilities, solutions, and future directions," in *Proc. Int. Conf. Comput. Artif. Intell. Renew. Syst. (CARS)*, Oct. 2024, doi: 10.1109/CARS61786.2024.10778682.
[10] A. M. Aburbeian and M. Fernández-Veiga, "Secure internet financial transactions: A framework integrating multi-factor authentication and machine learning," *AI*, vol. 5, no. 1, pp. 177–194, Jan. 2024, doi: 10.3390/ai5010010.
[11] V. R. Kebande *et al.*, "A blockchain-based multi-factor authentication model for a cloud-enabled internet of vehicles," *Sensors*, vol. 21, no. 18, Art. no. 6018, Sep. 2021, doi: 10.3390/s21186018.
[12] M. Wazid, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "Secure three-factor user authentication scheme for renewable energy based smart grid environment," *IEEE Trans. Ind. Informatics*, early access, 2017, doi: 10.1109/TII.2017.2732999.
[13] M. Sain, O. Normurodov, C. Hong, and K. L. Hui, "A survey on the security in cyber physical system with multi-factor authentication," *ICACT Trans. Adv. Commun. Technol.*, vol. 9, no. 6, pp. 1322–1329, Nov. 2020.
[14] Q. Wang and D. Wang, "Understanding failures in security proofs of multi-factor authentication for mobile devices," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 1–15, Nov. 2022, doi: 10.1109/TIFS.2022.3227753.
[15] B. Hawash *et al.*, "Factors affecting Internet of Things (IoT) adoption in the Yemeni oil and gas sector," in *Proc. Int. Conf. Technol., Sci. Admin. (ICTSA)*, Mar. 2021, doi: 10.1109/ICTSA52017.2021.9406527.
[16] R. K. Mahmood *et al.*, "Optimizing network security with machine learning and multi-factor authentication for enhanced intrusion detection," *J. Robot. Control*, vol. 5, no. 5, pp. 1502–1519, 2024, doi: 10.18196/jrc.v5i5.22508.
[17] S. Bergset and A. J. Nyland, "Ensuring safe and secure operations in the Norwegian petroleum industry," M.S. thesis, Dept. Inf. Sec. Commun. Technol., Norwegian Univ. Sci. Technol., Trondheim, Norway, Jun. 2023.
[18] T. N. I. Alrumaih *et al.*, "Cyber resilience in industrial networks: A state of the art, challenges, and future directions," *J. King Saud Univ. – Comput. Inf. Sci.*, vol. 35, Art. no. 101781, Sep. 2023, doi: 10.1016/j.jksuci.2023.101781.
[19] A. Bhardwaj *et al.*, "Unmasking vulnerabilities by a pioneering approach to securing smart IoT cameras," *Egyptian Informatics J.*, vol. 27, Art. no. 100513, Aug. 2024, doi: 10.1016/j.eij.2024.100513.
[20] S. Abdelkader *et al.*, "Securing modern power systems: Implementing comprehensive strategies to enhance resilience," *Results Eng.*, vol. 23, Art. no. 102647, Jul. 2024, doi: 10.1016/j.rineng.2024.102647.
[21] N. A. Alshuraify *et al.*, "Blockchain-based authentication scheme in oil and gas industry data with thermal CCTV cameras," *Int. J. Intell. Eng. Syst.*, vol. 17, no. 6, pp. 260–272, Dec. 2024, doi: 10.22266/ijies2024.1231.21.
[22] V. A. Cunha *et al.*, "TOTP moving target defense for sensitive network services," *Pervasive Mobile Comput.*, vol. 74, Art. no. 101412, 2021, doi: 10.1016/j.pmcj.2021.101412.
[23] W. A. Jebbar and M. Al-Zubaidie, "Transaction-based blockchain systems security improvement employing micro-segmentation," *SN Comput. Sci.*, vol. 5, no. 7, Art. no. 898, 2024, doi: 10.1007/s42979-024-03239-9.
[24] M. McGiffen, "Hashing and salting of passwords," in *Pro Encryption in SQL Server 2022*. Berkeley, CA, USA: Apress, 2022, pp. 269–275, doi: 10.1007/978-1-4842-8664-7_19.
[25] Z. N. Al-Qudsy *et al.*, "Securing DNA profiles using AES cryptography," *Iraqi J. Comput. Informatics*, vol. 51, no. 2, pp. 70–85, 2025, doi: 10.25195/ijci.v51i2.598.
[26] M. Al-Zubaidie and T. G. Tregi, "A quantum resilient security system for smart power grid data," *Appl. Data Sci. Anal.*, pp. 201–220, 2025, doi: 10.58496/ADSA/2025/017.
[27] R. H. Altaie and H. K. Hoomod, "Hybrid SPECK encryption algorithm for Internet of Things (IoT)," in *Proc. Int. Conf. Reliable Inf. Commun. Technol.*, Cham, Switzerland: Springer, 2023, pp. 317–326, doi: 10.1007/978-3-031-59711-4_27.

[28] R. H. Razzaq, M. Al-Zubaidie, and Atiyah, "Intermediary decentralized computing and private blockchain mechanisms," *Mesopotamian J. CyberSecurity*, vol. 4, no. 3, pp. 152–165, 2024, doi: 10.58496/MJCS/2024/020.
[29] S. Bamashmos, N. Chilamkurti, and A. S. Shahraki, "Two-layered multi-factor authentication using decentralized blockchain," *Sensors*, vol. 24, no. 11, Art. no. 3575, 2024, doi: 10.3390/s24113575.
[30] Y. Wu *et al.*, "An identity management scheme based on multi-factor authentication," *Sensors*, vol. 25, no. 7, Art. no. 2118, 2025, doi: 10.3390/s25072118.
[31] A. Alabdulatif, R. Samarasinghe, and N. N. Thilakarathne, "A novel robust geolocation-based multi-factor authentication method," *Appl. Sci.*, vol. 13, no. 19, Art. no. 10743, 2023, doi: 10.3390/app131910743.
[32] M. Saideh, J.-P. Jamont, and L. Vercouter, "Opportunistic sensor-based authentication factors in and for the IoT," *Sensors*, vol. 24, no. 14, Art. no. 4621, 2024, doi: 10.3390/s24144621.
[33] J. Choi *et al.*, "A PUF-based secure authentication and key agreement scheme for the Internet of Drones," *Sensors*, vol. 25, no. 3, Art. no. 982, 2025, doi: 10.3390/s25030982.
[34] V. O. Nyangaresi and G. K. Yenurkar, "Anonymity preserving lightweight authentication protocol," *High-Confidence Comput.*, vol. 4, no. 2, Art. no. 100178, 2024, doi: 10.1016/j.hcc.2023.100178.
[35] T. Segkoulis and K. Limniotis, "Enhancing multi-factor authentication for mobile devices through cryptographic zero-knowledge protocols," *Electronics*, vol. 14, no. 9, Art. no. 1846, 2025, doi: 10.3390/electronics14091846.