Computer Modeling in
Engineering & Sciences

Tech Science Press

Doi:10.32604/cmes.2025.062082

ARTICLE

Software Defined Range-Proof Authentication Mechanism for Untraceable Digital ID

So-Eun Jeon[1], **Yeon-Ji Lee**[2] **and Il-Gu Lee**[1,2,*]

[1]Department of Future Convergence Technology Engineering, Sungshin Women's University, Seoul, 02844, Republic of Korea
[2]Department of Convergence Security Engineering, Sungshin Women's University, Seoul, 02844, Republic of Korea

*Corresponding Author: Il-Gu Lee. Email: iglee@sungshin.ac.kr

Received: 09 December 2024; Accepted: 07 February 2025; Published: 03 March 2025

ABSTRACT: The Internet of Things (IoT) is extensively applied across various industrial domains, such as smart homes, factories, and intelligent transportation, becoming integral to daily life. Establishing robust policies for managing and governing IoT devices is imperative. Secure authentication for IoT devices in resource-constrained environments remains challenging due to the limitations of conventional complex protocols. Prior methodologies enhanced mutual authentication through key exchange protocols or complex operations, which are impractical for lightweight devices. To address this, our study introduces the privacy-preserving software-defined range proof (SDRP) model, which achieves secure authentication with low complexity. SDRP minimizes the overhead of confidentiality and authentication processes by utilizing range proof to verify whether the attribute information of a user falls within a specific range. Since authentication is performed using a digital ID sequence generated from indirect personal data, it can avoid the disclosure of actual individual attributes. Experimental results demonstrate that SDRP significantly improves security efficiency, increasing it by an average of 93.02% compared to conventional methods. It mitigates the trade-off between security and efficiency by reducing leakage risk by an average of 98.7%.

KEYWORDS: Internet of Things; authentication; digital ID; security

1 Introduction

The Internet of Things (IoT) encompasses wirelessly connected devices that interface with Internet networks [1]. These devices are employed in various domains, including smart grids, homes, cities, and energy management. The proliferation of IoT devices in localized contexts, including campuses, healthcare, and logistics, is projected to increase significantly, rapidly expanding their applications [2–6]. Consequently, organizations must establish robust policies for governing and managing these devices within the comprehensive Internet environment. Software-defined technology, crucial for efficient network management and control [7], is hardware-independent and facilitates the rapid establishment of flexible IT infrastructure by defining and controlling resources through software. The concept of "software-defined" originated with software-defined networking (SDN) and has expanded to include software-defined storage (SDS), software-defined data centers (SDDC), and the broader notion of software-defined everything (SDx) [8]. Notably, smart data exchange is gaining prominence as a core method for IoT management, offering an effective approach to managing and optimizing large-scale data flows between IoT devices. This method significantly enhances the flexibility of network resource management and ensures real-time data communication within

IoT networks [9,10]. Recent studies have reported improvements in the safety and efficiency of data exchange in IoT environments through the application of SDx technology [11,12].

Despite diverse and valuable applications of IoT technologies, several critical challenges persist. Securing IoT networks against advanced cyberattacks remains a significant concern [13]. The increasing proliferation of connected IoT devices raises significant issues regarding personal information leakage and privacy breaches [14]. Additionally, data from wearable devices that directly collect individual sensor data are stored in the cloud. However, the general access policy of the ciphertext-policy attribute-based encryption (CP-ABE) system, designed for information protection and efficient control, may compromise privacy and integrity [15]. Hence, robust authentication mechanisms are essential for ensuring trust among networked devices within IoT technology [16].

Extensive research has investigated secure authentication for IoT-enabled devices [17–19]. Sureshkumar et al. [17] implemented mutual authentication using standardized Burrows–Abadi–Needham (BAN) logic, enhancing mutual authentication and key exchange protocols for chaotic map-based medical information systems. However, this method incurs high computational costs and remains vulnerable to asynchronous attacks. Vinoth et al. [18] proposed a secure authentication protocol for IoT devices, employing hash functions, exclusive OR (XOR) operations, and symmetric encryption, enabling trusted users to access sensing devices remotely. While suitable for resource-limited IoT environments, this protocol incurs significant power consumption and presents considerable cryptographic complexity. Conventional protocols, such as Rivest-Shamir-Adleman (RSA)-based public key infrastructure (PKI) and elliptic curve cryptography (ECC), widely used for secure authentication in traditional networks, are often impractical for IoT devices due to high computational overhead and energy consumption. These protocols require substantial processing power and memory, which resource-constrained IoT devices generally lack. Consequently, the implementation of advanced security features, such as robust authentication protocols, strong encryption algorithms, and real-time intrusion detection systems, becomes impractical in many real-world scenarios. These limitations render such devices vulnerable to security breaches [20]. Furthermore, existing IoT security mechanisms are difficult to apply in real-world environments due to their high computational costs and energy requirements, which are critical considerations for IoT devices with limited battery life and low processing capacity [18,19,21,22]. Given the increasing cyberattacks on IoT devices, the development of lightweight and secure authentication techniques is essential [23].

This study introduces the software-defined range proof (SDRP) technique for secure, low-complexity authentication, addressing the trade-off between security and efficiency. SDRP minimizes the overhead of confidentiality and authentication processes by utilizing range proof [24] to verify whether the attribute information of a user falls within a specific range. The authentication (auth) node determines authentication and transmits de-identified random rules to the user node based on the purpose of authentication. The user generates a digital ID sequence and authenticates it using indirect personal information, avoiding the disclosure of actual individual attributes. Consequently, SDRP generates and authenticates a digital ID that prevents personal information inference, ensuring secure and accurate authentication even if the ID is compromised.

The contributions of this study are as follows:

- SDRP mitigates leakage risk and enhances efficiency by generating an untraceable digital ID using user attribute information in a ruleset of elementary operations.
- We propose a framework to evaluate authentication methods, considering both privacy and efficiency.
- To evaluate the performance of SDRP, we created a practical authentication environment using a user information dataset. The proposed model demonstrated superior performance compared to the conventional zero-knowledge proof model, a standard privacy-preserving authentication method.

The structure of this study is as follows: Section 2 reviews prior research, Section 3 introduces SDRP, Section 4 evaluates conventional models and SDRP, and Section 5 concludes the study.

2 Related Work

This section reviews prior research on conventional authentication methods, categorizing them into privacy-focused and lightweight techniques. Table 1 offers a comparative analysis of these methods.

Table 1: Previous studies of conventional authentication methods

Features	Previous studies	Method	Limitation
Privacy-preserving authentication	Shah et al. [24]	• Proposing a multi-key-based mutual authentication mechanism • The password set for secure storage is updated after each successful communication session	• Frequent updates and sharing of key values introduce limitations, increasing complexity and latency
Lightweight authentication	Santos et al. [21]	• Proposing an IoT-exclusive FIdM protocol that substitutes for complex technologies with streamlined, user-friendly alternatives within conventional FIdM	• Insufficient experimentation compromises the reliability of the results
	Li et al. [20]	• A novel lightweight authentication protocol, designed to satisfy privacy requirements using hash functions and XOR operations, is introduced	• Previous studies lacked performance comparison, thereby impeding the evaluation of computational cost and performance enhancement

(Continued)

Table 1 (continued)

Features	Previous studies	Method	Limitation
	Rana et al. [25]	• Optimized computational processes by implementing lightweight XOR operations alongside symmetric key-based encryption • Optimized network bandwidth usage by developing an authentication mechanism that requires only a single request-response exchange • Engineered to store only essential security parameters, thereby minimizing the data size retained on the smart card.	• Substantial computational power required presents challenges for operation on IoT devices with severely constrained resources
Privacy-preserving lightweight authentication	Gaba et al. [26]	• A novel lightweight authentication protocol, designed to satisfy privacy requirements using hash functions and XOR operations, is introduced	• Determining the precise computational cost is challenging, as performance assessments have primarily relied on mathematical analysis
	Chistousov et al. [27]	• Implement zero-knowledge proof with session keys to streamline authentication processes • In a specific context, it can enhance authentication speed by lowering confidentiality levels	• A trade-off exists: increasing speed necessitates reducing confidentiality levels, while the strength of the authentication protocol relies on the computational cost of solving the Diffie-Hellman problem.

Shah et al. [24] analyzed the security vulnerabilities of password-based authentication methods in IoT systems, focusing on side-channel and dictionary attacks. They proposed a multikey-based mutual authentication mechanism to enhance security between IoT devices and servers. This mechanism securely manages secret keys within an encrypted vault, ensuring that servers and IoT devices share equal-sized keys. A significant advantage of the proposed method is the dynamic updating of securely stored password content with each successful communication session, thereby eliminating reliance on a single key value. However, they did not address the increased latency due to frequent key-value updates and sharing.

Conventional authentication methods are unsuitable for resource-constrained IoT environments, prompting the exploration of lightweight alternatives. Santos et al. [21] identified the shortcomings of traditional identity management (IdM) for lightweight IoT devices and introduced a federated identity management (FIdM) protocol tailored to IoT specifications. Although this protocol simplifies conventional FIdM, it lacks performance comparisons with existing FIdM technologies, leaving its relative efficacy undetermined.

Li et al. [20] addressed security challenges in data transmission within vehicular *ad hoc* networks (VANET) by identifying inefficiencies in conventional authentication methods characterized by excessive computation and security flaws. They introduced a lightweight authentication protocol utilizing hash functions and XOR operations to enhance privacy protection and secure authentication. While their approach preserves vehicle information anonymity and ensures secure authentication, the lack of a comparative analysis with existing research leaves the claimed improvements in computational cost and performance unverified.

Rana et al. [25] proposed a lightweight authentication mechanism tailored for IoT environments. This study introduces a technique leveraging a hash function and symmetric encryption to achieve mutual authentication between users and servers. The implementation of symmetric encryption and a non-collision hash function effectively reduces computational overhead, minimizes communication instances, and decreases the data storage requirements on smart cards. Nevertheless, this mechanism faces challenges with IoT devices with extremely severe resource constraints attributed to relatively high computational demands.

Gaba et al. [26] identified significant security vulnerabilities in wearable IoT devices, which can be exploited to alter medical reports, thereby leading to inaccurate diagnoses and treatments. They proposed various cybersecurity solutions, such as fog, edge, cloud, blockchain, password, biometrics, hash, and elliptic curve cryptography. However, these solutions are prone to cyberattacks and entail high computational and communication costs, rendering them unsuitable for IoT environments. Consequently, the authors introduced a zero-knowledge proof (ZKP)-based authenticated key agreement protocol for Internet of Healthcare Applications (IoHA). This protocol prevents unauthorized access and ensures secure authentication while minimizing computational and communication overhead. Despite ensuring confidentiality, integrity, and availability, its performance evaluation relies solely on mathematical proofs, complicating cost assessment.

Chistousov et al. [27] demonstrated that while encryption systems ensure robust confidentiality for vehicle authentication in VANETs, they require extensive key management infrastructure. Moreover, the compromise of a cryptographic key can significantly weaken the protection of transmitted data within VANETs. To mitigate this issue, a ZKP protocol was proposed, offering strong confidentiality without relying on encryption. This method leverages session-key-based ZKP to streamline the authentication process, allowing for adjustable confidentiality levels to enhance authentication speed. Furthermore, they increased the complexity of ZKPs, proposing a more secure authentication method. Nonetheless, the inherent trade-off remains unresolved: reducing confidentiality to improve authentication speed while considering the computational overhead of Diffie–Hellman operations, which impacts both efficiency and security.

Numerous studies aimed at enhancing conventional authentication technologies have often overlooked key factors such as latency, computational cost, and the balance between security and performance metrics. Furthermore, conventional security research frequently relies on complex mathematical models and algorithms, thereby increasing computational overhead. Conversely, studies prioritizing authentication speed have emphasized efficiency at the expense of security, resulting in a trade-off. Despite considering both evaluation metrics, previous research has often compromised confidentiality for efficiency gains or accepted higher computational costs to maintain privacy. Consequently, the trade-off between efficiency and security remains unresolved.

In this study, we present novel metrics for assessing privacy and efficiency in IoT environments, addressing the limitations of prior research. We also introduce a lightweight authentication method that balances these metrics, ensuring high reliability and efficiency.

3 Software Defined Range Proof (SDRP)

This section presents SDRP, a methodology for generating digital ID sequences using a ruleset to ensure secure and efficient authentication.

3.1 Anonymous Credential

Self-sovereign identity (SSI) introduces a novel identity management systems (IMS) paradigm, offering a privacy-preserving mechanism for identity verification [28]. SSI adheres to ten fundamental principles: existence, control, access, transparency, persistence, portability, interoperability, consent, minimization, and protection [29]. Existence denotes the independent status of users, and control refers to their ability to manage their identity. Access enables data retrieval, transparency ensures algorithmic and infrastructural clarity, and persistence guarantees long-term ID maintenance. Portability supports the transfer of identity-related information, while interoperability ensures broad usability. Consent signifies user agreement for identity use, minimization reduces data disclosure, and protection safeguards users' rights.

Conventional authentication methods frequently employ sensitive personal identifiers encapsulated in encrypted tokens, which are vulnerable to information leakage if intercepted during transmission. Consequently, research on anonymous credential authentication—which verifies user eligibility without disclosing personal identities—has become increasingly prominent. Recent SSI techniques utilize anonymous credentials to protect personal information. These credentials enable users to authenticate themselves without unnecessary identity disclosure [28]. Generating anonymous credentials involves inputting the public key, message, proposition information, credential, and attribute proof signing key of the system. The attributes linked to the credential are identified based on the proposition details, and appropriate proof values are generated for each attribute. Upon receiving the anonymous credential, the server separates the attribute information according to the proposition details and conducts primary verification. Finally, the server authenticates the anonymous credentials by verifying the information of each attribute separately.

3.2 Operation Method of SDRP

Fig. 1 illustrates the operation of SDRP through a flowchart. SDRP interacts with the authorization node (auth node) for identity verification, evaluates authentication permissions, and requests authentication from the user node. Initially, SDRP establishes rules to generate a digital ID that conceals personal information. Within this framework, a rule comprising all de-identification or specific identifiable operations related to the required attribute is stochastically generated and transmitted to the user node based on the authentication purpose. Certain de-identification rules permit the specification of attributes verifiable as sequences, such as age, gender, and affiliation. Upon receiving the rule, the user node computes a digital ID from its personal information and forwards it to the auth node. Subsequently, the auth node verifies whether the user falls within the authorized group range using the received digital ID. If the user node has an invalid ID outside the specified group range, the authentication process is flagged as abnormal, leading to authentication failure. Extending the auth request interval when the user node re-initiates authentication can prevent an infinite authentication loop caused by an abnormal node. Conversely, duplicate users are verified and authorized for authentication if the user node is identified as a legacy ID within the group range under verification. The duplicate user undergoes re-authentication considering the potential derivation of the same digital ID, despite the application of different rulesets. Unlike encrypting and transmitting personal identification information over the network, SDRP generates indirect personal information by performing operations on the attributes' characteristics in the received rule set to derive a digital ID. Consequently, even if an attacker intercepts a digital ID through a side-channel attack, identifying an individual remains impossible, thus mitigating privacy infringement risks. Furthermore, SDRP achieves lightweight performance by employing simple arithmetic operations for digital ID generation.

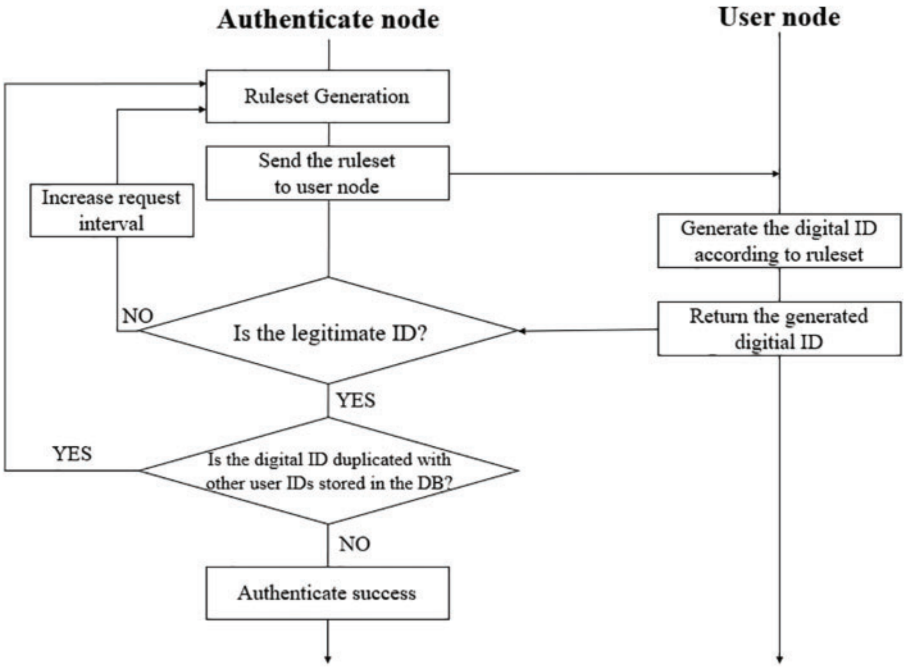
Authenticate node
User node
Ruleset Generation
Send the ruleset to user node
Increase request interval
Generate the digital ID according to ruleset
NO
Is the legitimate ID?
Return the generated digitial ID
YES
YES
Is the digital ID duplicated with other user IDs stored in the DB?
NO
Authenticate success

Figure 1: Flowchart for SDRP operation method

Fig. 2 presents the system architecture of the auth and user nodes.

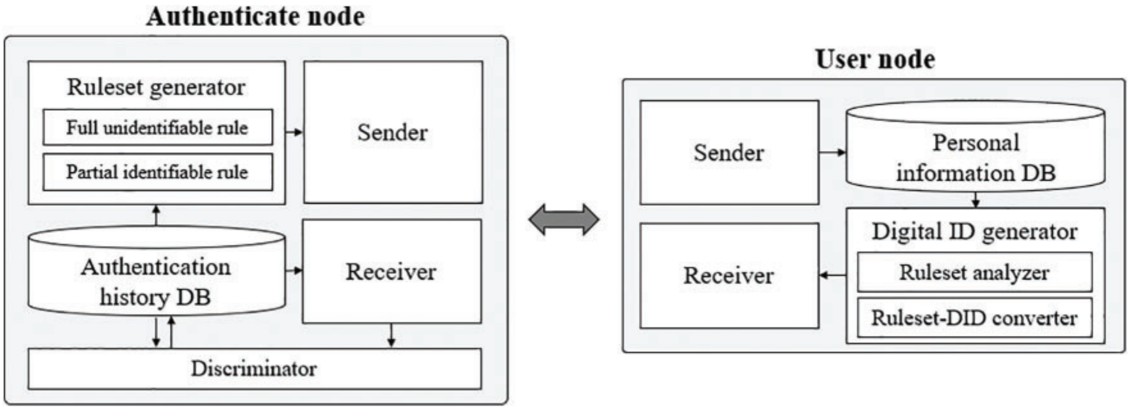

Figure 2: System architecture of auth node and user node

In this architecture, the auth node employs the ruleset generator to create rules that can be fully or partially identifiable, depending on specific authentication requirements. A fully identifiable rule is applied when attributes requiring authentication contain personally sensitive information that needs protection and belong to rule types where sequences undergo specific transformations. Conversely, partially identifiable rules are used for low-sensitivity attributes, posing no significant disclosure issues. This rule permits attributes such as age and gender to be directly identified through a digital ID sequence without additional operations. Fig. 3 provides an example of the SDRP digital ID generation process.

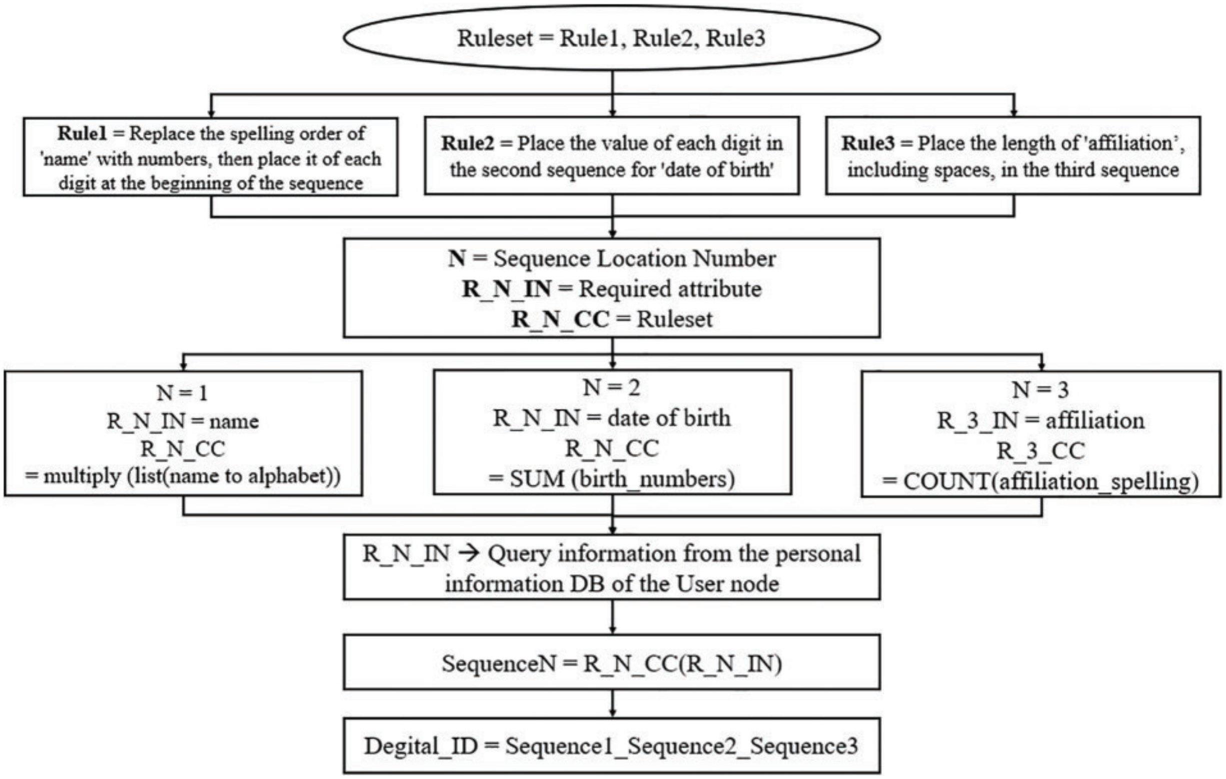
Ruleset = Rule1, Rule2, Rule3
Rule1 = Replace the spelling order of 'name' with numbers, then place it of each digit at the beginning of the sequence
Rule2 = Place the value of each digit in the second sequence for 'date of birth'
Rule3 = Place the length of 'affiliation', including spaces, in the third sequence
N = Sequence Location Number
R_N_IN = Required attribute
R_N_CC = Ruleset
N = 1
R_N_IN = name
R_N_CC
= multiply (list(name to alphabet))
N = 2
R_N_IN = date of birth
R_N_CC
= SUM (birth_numbers)
N = 3
R_3_IN = affiliation
R_3_CC
= COUNT(affiliation_spelling)
R_N_IN → Query information from the personal information DB of the User node
SequenceN = R_N_CC(R_N_IN)
Degital_ID = Sequence1_Sequence2_Sequence3

Figure 3: Example of SDRP's digital ID generation process

As illustrated in Fig. 3, rules are generated based on the required attributes to formulate an operation-based ruleset that ensures the anonymity of personal information. For instance, if the attribute is a string, a ruleset such as "Replace the spelling order of 'name' with numbers, then offset it at the sequence start" can function by substituting the alphabetical order with numbers. After the ruleset is created, it is transmitted to the user node via the sender. The user node applies the personal information stored in the personal information database (DB) to the ruleset within the digital ID generator to produce a digital ID, which is then transmitted to the auth node. The communication protocol between the auth node and the user node is depicted in Fig. 4.

Fig. 4 illustrates that the auth node manages authentication performance by incorporating the ruleset field into the communication packet format. Concurrently, the user node initiates authentication using the digital ID field. Upon receiving the digital ID from the user node, the discriminator assesses its validity and checks for duplicate IDs in the authentication history DB before making a decision.

Algorithm 1 outlines the pseudocode for SDRP encompassing rule generation, ruleset transmission to the user node, digital ID creation and return to the auth node, legitimacy assessment of the user node, and verification of duplicate digital IDs in the DB. In Step 1, fully or partially unidentifiable rules are generated and transmitted to the user node. In Step 2, upon receiving the ruleset, the user node applies a personal attribute to generate a digital ID, which is then returned to the auth node. In Step 3, the auth node calculates the ID condition to verify the authenticity of the user node. The calculated ID is compared with the digital ID received from the user node to determine authentication eligibility. In Step 4, if the ID is authorized for authentication, it undergoes a duplication check by comparing it with the digital ID stored in the authenticated history DB.

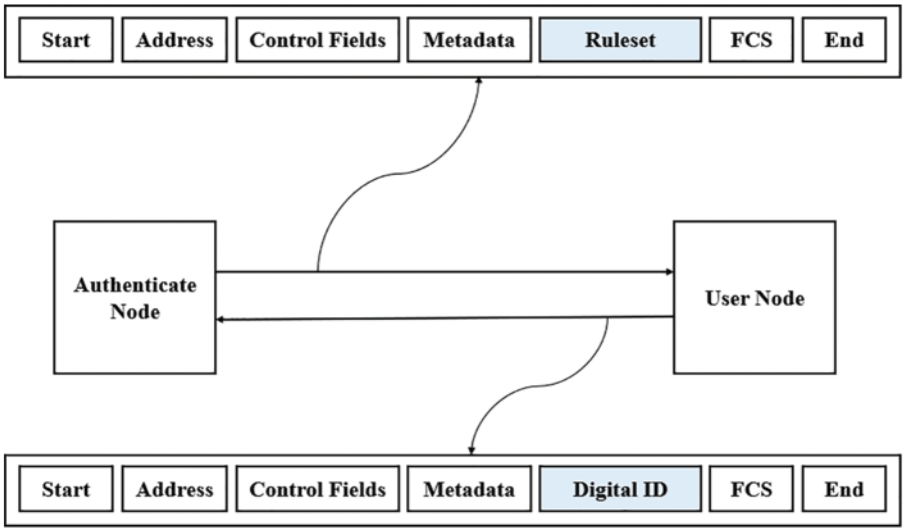

Figure 4: Communication format between auth node and user node

Algorithm 1: Pseudo-code for SDRP evaluation

```
Input:  Personal attribute
Output:  Leakage risk, Efficiency, Computational cost
Step 1: Generate the ruleset and send it to user node
Ruleset = ruleset_generation(full_unidentifiable, partial identifiable)    ▷ Generate the full unidentifiable or partially identifiable ruleset
Transmit (Ruleset)
Step 2:  Calculate the digital ID and return it to auth node
User_node_data = Received(Ruleset)
User_digital_ID = Ruleset(personal_attribute)    ▷ Calculate the digital ID based on the ruleset
Step 3: Discriminate user node, whether legitimate node or not
Legitimate_ID_condition = Ruleset(legitimate_attribute)    ▷ Derive the legitimate ID condition to compare with the user node ID
if Legitimate_ID_condition == User_digital_ID:    ▷ Compare with legitimate ID and user node digital ID
    Auth_result = ‘success’
else if Legitimate_ID_condition  != User_digital_ID:
    Auth_result = ‘fail’
Step 4:  Check the duplicated digital ID in the DB
if Auth_result = ‘success’:
    compare_DB  (auth_history, User_digital_ID)    ▷ Compare whether the User digital ID is duplicated with another user node
```

4 Performance Evaluation

4.1 Evaluation Environment

This section describes the experimental setup used to evaluate the performance of SDRP. The evaluation framework, depicted in Fig. 5, was implemented to compare and assess the performances of conventional and SDRP-based authentication methods.

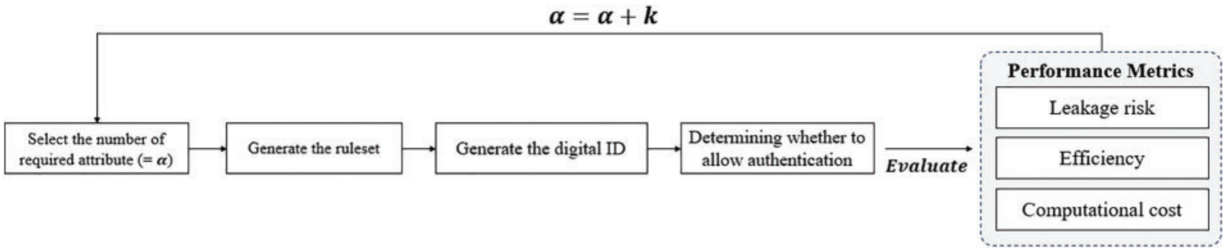

Figure 5: Evaluation framework of digital ID-based authentication techniques

The auth node of SDRP generates a ruleset for the required attributes and transmits it to the user node. The user node then computes the digital ID based on this ruleset, which the auth node subsequently uses to determine authentication permission. In this experiment, the parameter α, representing the number of required attributes, was varied to evaluate leakage risk, efficiency, and computational cost.

User data were obtained from the company–employee dataset [30], which includes information from 5000 users. Table 2 details the features of the data utilized in this experiment.

Table 2: Configuration of user information datasets

Features	Type	Contents
ID	int64	0~4999
Company	str	Glasses, Cheerper, Pear
Department	str	Bigdata, AI, Support, Design, Search Engine, Sales
Age	int64	30~49
Gender	str	Female, male
SocialNumber	int64	6-digit number

Personal information attributes of the user node, including ID, company, department, age, gender, and social number, were extracted from the total features. Only integer (int) and string (str) data types were employed. This dataset served as authentication data to simulate the authentication environment.

In this study, we benchmarked the zero-knowledge proof model (ZKPM) [31] and the identifiable attribute model (IAM) [27] to evaluate the performance of SDRP. ZKPM model employs an AES-based zero-knowledge proof technique for range proof. Here, the user node calculates $y = g^x\ (modp)$ to transmit y as an unidentifiable secret value x to the auth node. Subsequently, the user node generates a random number r and calculates $C = g^r (modp)$ to transmit C to the auth node. Upon receiving this, the auth node iterates the process N times, requesting either r or $(x + r)\ (mod\ (p - 1))$ from the user node to estimate x and perform authentication. Parameters were set with $g = 2$, and $N = 3$. The random value r was chosen between 1 and 20, while p was selected from prime numbers between 100 and 200. User attributes from the company-employee dataset [30] served as the secret value x. Conversely, IAM [27] leverages lightweight zero-knowledge authentication protocols (ZKAP) with a session key for encrypting communication sessions, thereby reducing the number of authentication steps and ensuring confidentiality. IAM is designed for lightweight performance by dynamically adjusting the level of confidentiality. In this study, we compared the IAM environment at the lowest level of confidentiality.

To evaluate the performance of SDRP, we employed computational cost, leakage risk, and security efficiency as metrics. Computational complexity was assessed using Big-O notation.

Leakage risk denotes the potential for ID leakage by an attacker when utilizing SDRP, calculated as described in Eq. (1).

$$Leakage\,risk = \frac{I_t}{RI_t \times O_t\left(N\right)} \tag{1}$$

where RI_t denotes the request interval at time t, $O_t\left(N\right)$ represents the computational cost of the ruleset at time t, and I_t indicates the importance of the required attributes at time t. In this experiment, upon authentication failure, RI_t increased by 10 s. $O_t\left(N\right)$ is the computation cost based on Big-O notation, and I_t is determined by assigning importance to each attribute. Given that Social Number corresponds to sensitive personal information, its importance was set to 5, age and gender were set to 3, and company and department were set to 1 [32].

Security efficiency was calculated using Eq. (2) as a metric for evaluating the security efficiency of the authentication model.

$$Security\ Efficiency = \frac{Privacy\,preserving\,capability}{O_t\left(N\right)} \tag{2}$$

Security efficiency is inversely proportional to the latency and computational cost of authentication, and directly proportional to privacy-preserving capability, quantified as the proportion of preserved privacy, as calculated by Eq. (3).

$$Privacy\ preserving\ capability = \frac{1}{Leakage\ risk} = \frac{RI_t \times O_t\left(N\right)}{I_t} \tag{3}$$

SDRP presents an efficient authentication mechanism designed for lightweight devices to enhance security and minimize data leakage risk—a key security metric. The performance across three evaluation metrics was analyzed by progressively increasing the number of required attributes. To ensure experimental reliability, the average results from 10,000 simulation repetitions were calculated.

4.2 Evaluation Results and Analysis

This section analyzes the performance of SDRP relative to conventional models, ZKPM and IAM, concerning computational cost, leakage risk, and security efficiency. Fig. 6 illustrates the comparative leakage risk between SDRP and conventional models.

As the number of required attributes increased, the probability of incorporating critical attributes also rose. Consequently, the risk of information leakage to potential attackers escalated, with the highest risk observed in the IAM model, followed by SDRP and ZKPM. The IAM model, which transmits and receives personal information at the lowest confidentiality level, exhibited the highest privacy leakage risk. In contrast, SDRP, which uses digital IDs containing only indirect personal information characteristics, and ZKPM, which relies on complex knowledge proof equations, demonstrated a maximum privacy leakage risk that was 10^2 times lower than that of IAM.

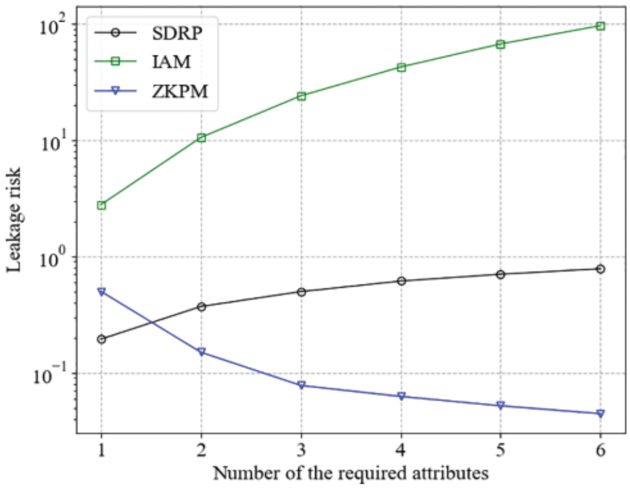

Figure 6: Leakage risk of SDRP by the number of required attributes

Fig. 7 illustrates the comparative results of SDRP and the conventional model regarding computational cost.

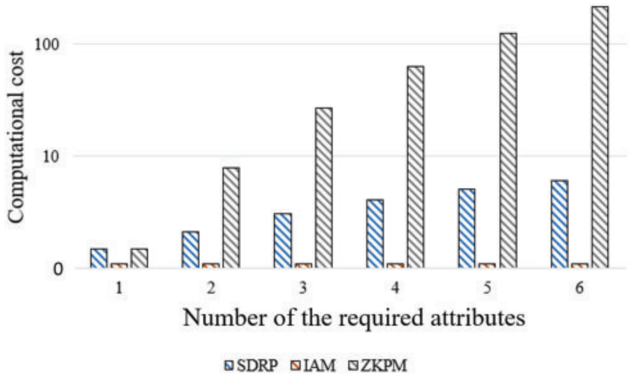

Figure 7: Computational cost of SDRP by the number of required attributes

As the number of required attributes increased, the computational burden for de-identification escalated, consistently increasing overall computational costs. Among the methods, ZKPM, a zero-knowledge proof-based technique, exhibited inefficiencies due to the repeated exchange of complex operational formulas during secret-value de-identification. Conversely, SDRP, which computes a simple ruleset, reduced computational cost by up to 10 times compared to conventional ZKPM. Additionally, the IAM model, which bypasses de-identification processing, demonstrated optimal efficiency by avoiding separate operations. However, the most critical evaluation index for safe authentication, leakage risk, revealed a significant limitation: confidentiality cannot be guaranteed, as it presented the most inefficient results.

Fig. 8 illustrates the comparative security efficiency of SDRP *vs*. the conventional model.

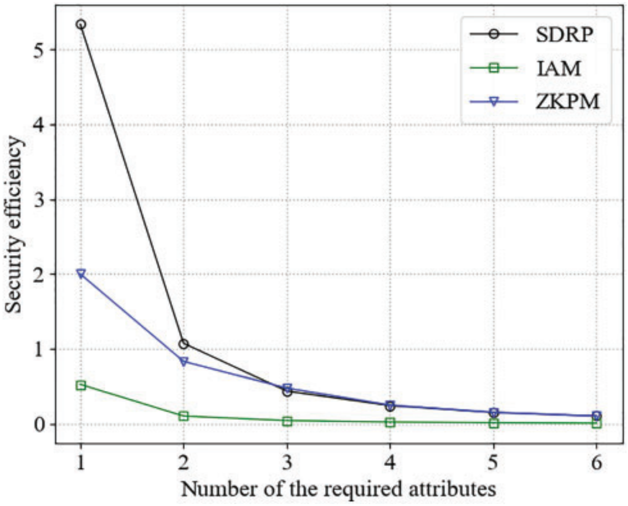

Figure 8: Security efficiency of SDRP by the number of required attributes

Overall, an increase in the number of required attributes correspondingly elevated the computational cost of authentication, diminishing security efficiency. The SDRP model demonstrated up to five times higher security efficiency compared to conventional models. This enhanced efficiency is due to the superior leakage risk performance of SDRP relative to IAM, coupled with its lower computational cost compared to ZKPM. Conversely, while ZKPM achieved optimal leakage risk outcomes, its overall security performance was hindered by significantly higher computational costs.

In summarizing the experimental findings, this study assessed IAM, ZKPM, and the proposed SDRP method across three metrics: leakage risk, computational cost, and security efficiency. For leakage risk, the ranking was ZKPM, SDRP, and IAM, suggesting that more complex techniques offer stronger security. The evaluation of computational cost revealed the ranking as IAM, SDRP, and ZKPM, indicating a trade-off between security and efficiency. Therefore, security efficiency was the final metric, identifying the model that best balanced security and efficiency. In this metric, SDRP, ZKPM, and IAM were ranked accordingly. Since security efficiency is inversely proportional to authentication latency and computational cost while directly proportional to privacy preservation performance, it can be concluded that SDRP achieves the optimal balance between security and efficiency among the three models.

5 Conclusion

Various technologies have been developed to protect IoT networks from increasing cyber threats targeting IoT devices. However, due to the resource constraints of these devices, implementing secure and sophisticated algorithms becomes challenging. Consequently, secure and lightweight authentication methods are essential to balance complexity and security in conventional research. This study proposed the SDRP model, which securely generates a digital ID sequence based on a ruleset without directly transmitting user attribute information over the network. In SDRP, the auth node generates random rulesets that are either fully or partially de-identified. These rulesets are then transmitted to the user node, which generates a digital ID sequence for authentication using indirect personal information rather than actual user attributes. Therefore, even if advanced attacks such as side-channel attacks or timing attacks occur, the attacker cannot identify personal information solely based on the digital ID transmitted over the network. Furthermore, by minimizing the computational load and the number of communication exchanges, the proposed method achieves lightweight authentication, making it efficient regarding energy consumption—a critical factor for

IoT devices. The experimental results indicate that SDRP enhances security efficiency by an average of 93.02% over conventional methods and reduces the risk of information leakage by an average of 98.7%. This balance between security and efficiency demonstrates the efficacy of SDRP. The primary limitation of this study is its focus on a simulated authentication environment. Future research will address this by incorporating advanced attacker nodes in realistic settings and optimizing the request interval of the SDRP to establish an optimal defense environment and validate its performance. Additionally, we will model network environments with varying traffic loads and analyze energy consumption, a critical metric in IoT environments, to demonstrate the scalability and reliability of the SDRP.

Acknowledgement: The authors thank the Korea Institute for Advancement of Technology (KIAT) under the Korean Government's Ministry of Trade, Industry, and Energy (MOTIE) grant and from the Ministry of Science and ICT (MSIT) through the ICAN (ICT Challenge and Advanced Network of HRD) program managed by the Institute of Information & Communication Technology Planning and Evaluation (IITP).

Funding Statement: This study received partial funding from the Korea Institute for Advancement of Technology (KIAT) through a grant provided by the Korean Government Ministry of Trade, Industry, and Energy (MOTIE) (RS-2024-00415520, Training Industrial Security Specialist for High-Tech Industry). Additional support was received from the Ministry of Science and ICT (MSIT) under the ICAN (ICT Challenge and Advanced Network of HRD) program (No. IITP-2022-RS-2022-00156310) overseen by the Institute of Information & Communication Technology Planning and Evaluation (IITP).

Author Contributions: The authors have contributed to the paper as follows: So-Eun Jeon was responsible for conceptualization, methodology, software, validation, visualization, and writing—original draft. Yeon-Ji Lee contributed to resources, validation, writing—review and editing. Il-Gu Lee contributed to conceptualization, validation, writing—review and editing, supervision, project administration, and funding acquisition. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data that support the findings of this study are available from the first and corresponding authors upon reasonable request.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

Abbreviations

IoT	Internet of Things
SDN	Software-defined networking
SDS	Software-defined storage
SDDC	Software-defined data centers
SDx	Software-defined everything
CP-ABE	Ciphertext-policy attribute-based encryption
BAN	Burrows–Abadi–Needham
XOR	Exclusive OR
SDRP	Software-defined range proof
VANET	Vehicular *ad hoc* networks
IdM	Identity management
FIdM	Federated identity management
ZKP	Zero-knowledge proof
IoHA	Internet of Healthcare Applications
SSI	Self-sovereign identity

IMS	Identity management systems
DB	Database
ZKPM	Zero-knowledge proof model
IAM	Identifiable attribute model
ZKAP	Zero-knowledge authentication protocols

References

1. Quy VK, Hau NV, Anh DV, Quy NM, Ban NT, Lanza S, et al. IoT-enabled smart agriculture: architecture, applications, and challenges. Appl Sci. 2022;12(7):3396. doi:10.3390/app12073396.
2. Yun SW, Park NE, Lee IG. Wake-up security: effective security improvement mechanism for low power internet of things. Intell Autom Soft Comput. 2023;37(3):2897–917. doi:10.32604/iasc.2023.039940.
3. Chamoun MM, Fadlallah A, Serhrouchni A. Taxonomy of authentication techniques in internet of things (IoT). In: 15th Student Conference on Research and Development (SCOReD); 2017; Wilayah Persekutuan Putrajaya: IEEE Publications. p. 67–71.
4. Sutjarittham T, Habibi HH, Kanhere SS, Sivaraman V. Experiences with IoT and AI in a smart campus for optimizing classroom usage. IEEE Internet Things J. 2019;6(5):7595–607. doi:10.1109/JIOT.2019.2902410.
5. Zhou Z, Yu H, Shi H. Human activity recognition based on improved bayesian convolution network to analyze health care data using wearable IoT device. IEEE Access. 2020;8:86411–8. doi:10.1109/ACCESS.2020.2992584.
6. Jeon SE, Oh YS, Lee YJ, Lee IG. Suboptimal feature selection techniques for effective malicious traffic detection on lightweight devices. Comput Model Eng Sci. 2024;140(2):1669–87. doi:10.32604/cmes.2024.047239.
7. Amin R, Hussain M, Bilal M. Network policies in software defined Internet of everything. In: Aujla GS, Garg S, Kaur K, Sikdar B, editors. Software defined internet of everything. Cham: Springer; 2022. p. 79–96. doi: 10.1007/978-3-030-89328-6_5.
8. Pajila PJB, Jenifer P, Karpagavalli CK, Angeline AV, Muthu R. Software defined networking based protection against DDOS in IoT. Int J Innov Technol Explor Eng. 2020;9(5):739–45. doi:10.35940/ijitee.E2521.039520.
9. Benson K, Wang G, Venkatasubramanian N, Kim Y. Ride: a resilient IoT data exchange middleware leveraging SDN and edge cloud resources. In: 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI); 2018; Orlando, FL, USA. p. 72–83. doi:10.1109/IoTDI.2018.00017.
10. Albulayhi A, Alsukayti I. A blockchain-centric IoT architecture for effective smart contract-based management of IoT data communications. Electronics. 2023;12(12):2564. doi:10.3390/electronics12122564.
11. Gharaibeh A, Salahuddin M, Hussini S, Khreishah A, Khalil I, Guizani M, et al. Smart cities: a survey on data management, security, and enabling technologies. IEEE Commun Surv Tutor. 2017;19:2456–501. doi:10.1109/COMST.2017.2736886.
12. Liu Y, Zhang C, Yan Y, Zhou X, Tian Z, Zhang J. A semi-centralized trust management model based on blockchain for data exchange in IoT system. IEEE Trans Serv Comput. 2023;16:858–71. doi:10.1109/TSC.2022.3181668.
13. Meneghello F, Calore M, Zucchetto D, Polese M, Zanella A. IoT: internet of threats? a survey of practical security vulnerabilities in real IoT devices. IEEE Internet Things J. 2019;6:8182–201. doi:10.1109/JIOT.2019.2935189.
14. Kumar KP, Prathap BR, Thiruthuvanathan MM, Murthy H, Pillai VJ. Secure approach to sharing digitized medical data in a cloud environment. Data Sci Manage. 2023. doi: 10.1016/j.dsm.2023.12.001.
15. El-Hajj M, Fadlallah A, Chamoun M, Serhrouchni A. A survey of Internet of Things (IoT) authentication schemes. Sensors. 2019;19(5):1141. doi:10.3390/s19051141.
16. Saqib M, Moon AH. A systematic security assessment and review of Internet of things in the context of authentication. Comput Secur. 2023;125:103053. doi:10.1016/j.cose.2022.103053.
17. Sureshkumar V, Amin R, Obaidat MS, Karthikeyan I. An enhanced mutual authentication and key establishment protocol for TMIS using chaotic map. J Inf Secur Appl. 2020;53:102539. doi:10.1016/j.jisa.2020.102539.
18. Vinoth R, Deborah LJ, Vijayakumar P, Kumar N. Secure multi-factor authenticated key agreement scheme for industrial IoT. IEEE Internet of Things. 2020;8(5):3801–11. doi:10.1109/JIOT.2020.3024703.
19. Deebak BD. Lightweight authentication and key management in mobile-sink for smart IoT-assisted systems. Sustain Cities Soc. 2020;63:102416. doi:10.1016/j.scs.2020.102416.

20. Li X, Liu T, Obaidat MS, Wu F, Vijayakumar P, Kumar N. A lightweight privacy-preserving authentication protocol for VANETs. IEEE Syst J. 2020;14(3):3547–57. doi:10.1109/JSYST.2020.2991168.
21. Santos MLBA, Carneiro JC, Franco AMR, Teixeira FA, Henriques MAA, Oliveira LB. FLAT: federated lightweight authentication for the Internet of things. Ad Hoc Netw. 2020;107:102253. doi:10.1016/j.adhoc.2020.102253.
22. Kil YS, Lee YJ, Jeon SE, Oh YS, Lee IG. Optimization of privacy-utility trade-off for efficient feature selection of secure Internet of Things. IEEE Access. 2024;12:142582–91. doi:10.1109/ACCESS.2024.3467049.
23. Couteau G, Klooß M, Lin H, Reichle M. Efficient range proofs with transparent setup from bounded integer commitments. In: Canteaut A, Standaert FX, editors. Advances in cryptology—EUROCRYPT 2021. Vol. 12698. Cham: Springer; 2021. doi: 10.1007/978-3-030-77883-5_9.
24. Shah T, Venkatesan S. Authentication of IoT device and IoT server using secure vaults. In: 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications; 2018; New York, NY, USA. doi: 10.1109/TrustCom/BigDataSE.2018.00117.
25. Rana M, Shafiq A, Altaf I, Alazab M, Mahmood K, Chaudhry SA, et al. A secure and lightweight authentication scheme for next generation IoT infrastructure. Comput Commun. 2021;165:85–96. doi:10.1016/j.comcom.2020.11.002.
26. Gaba GS, Hedabou M, Kumar P, Braeken A, Liyanage M, Alazab M. Zero knowledge proofs based authenticated key agreement protocol for sustainable healthcare. Sustain Cities Soc. 2020;80:103766. doi:10.1016/j.scs.2022.103766.
27. Chistousov NK, Kalmykov IA, Dukhovnyj DV, Kalmykov MI, Olenev AA. Adaptive authentication protocol based on zero-knowledge proof. Algorithms. 2020;15(2):50. doi:10.3390/a15020050.
28. Bosk D, Frey D, Gestin M, Piolle G. Hidden issuer anonymous credential. In: Proceedings on Privacy Enhancing Technologies; 2022; Warsaw, Poland. p. 571–607. doi:10.56553/popets-2022-0123.
29. Grüner A, Mühle A, Meinel C. Analyzing interoperability and portability concepts for self-sovereign identity. In: 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom); 2021; Shenyang, China. p. 587–97. doi:10.1109/TrustCom53373.2021.00089.
30. Iqman SB. Company-employee dataset. [cited 2025 Feb 06]. Available from: https://www.kaggle.com/datasets/iqmansingh/company-employee-dataset.
31. Rasheed AA, Mahapatra RN, Hamza-Lup FG. Adaptive group-based zero knowledge proof-authentication protocol in vehicular *ad hoc* networks. IEEE Trans Intell Transp Syst. 2020;21(2):867–81. doi:10.1109/TITS.2019.2899321.
32. SensitivityScore. Sensitive data protection documentation | Google cloud. 2023. [cited 2025 Feb 06]. Available from: https://cloud.google.com/sensitive-data-protection/docs/reference/rest/v2/SensitivityScore.