Semantic IoT Transformation: Elevating Wireless Networking Performance through Innovative Communication Paradigms

Ibrahim R. Alzahrani
Computer Science and Engineering Department, College of Computer Science and Engineering, University of Hafr Al Batin, Saudi Arabia
ialzahrani@uhb.edu.sa (corresponding author)

Received: 10 May 2024 | Revised: 29 May 2024 2024 | Accepted: 6 June 2024

 DOI: https://doi.org/10.48084/etasr.7784

ABSTRACT

This paper addresses the privacy concerns inherent in semantic communication within the Internet of Things (IoT) and proposes a Secure Semantic Communication Framework (SSCF) to ascertain confidentiality and communication accuracy without compromising semantic integrity. The proposed framework uses the Advanced Encryption Standard (AES) for encryption to address privacy breaches in semantic communication. Additionally, it introduces a novel approach employing Deep Q-Networks (DQN) for adversarial training to maintain semantic communication accuracy in both unencrypted and encrypted modes. SSCF combines universality and confidentiality, ensuring secure and efficient semantic communication. Experimental evaluations showed that SSCF, with its adversarial encryption learning scheme, effectively ensures communication accuracy and privacy. Regardless of encryption status, SSCF significantly hinders attackers from restoring original semantic data from intercepted messages. The integration of heuristic algorithms enhances performance and security. The proposed framework is based on a shared database for training network modules. The originality of the proposed approach lies in the introduction of a DQN-based adversarial training technique to balance confidentiality and semantic communication accuracy, address key privacy concerns, and enhance the security and reliability of IoT communication systems.

Keywords-semantic communication; privacy-preserving; AES; DQN; SSCF; IoT

I. INTRODUCTION

The Internet of Things (IoT) refers to physical items integrated with sensors, software, and other technologies that communicate with other systems and devices over the Internet [1]. This technology has revolutionized wireless networking by connecting billions of devices and facilitating various applications in multiple domains. The concept of semantic IoT transformation has gained significant attention to meet the diverse needs of IoT applications. This transformation represents a shift from traditional communication methods, which transmit raw sensor data, to a system that leverages the semantic meaning of the data for more intelligent and context-aware communication [2-9]. The semantic IoT transformation enriches communication by incorporating contextual information, enabling devices to convey meaningful messages rather than just raw data. For example, instead of simply transmitting temperature readings, a semantic IoT device might indicate a potential HVAC failure when the room temperature exceeds a certain threshold [10]. This approach improves performance by promoting faster response times and more informed decision-making [11]. Moreover, it empowers devices to perform localized reasoning and decision-making, reducing the reliance on centralized processing [12-13]. Despite its potential, semantic IoT transformation faces certain difficulties such as the complexity of semantic data representation and assuring privacy and security during communication [14-15]. Addressing these challenges requires advanced semantic modeling techniques, efficient communication protocols, and robust security mechanisms [16]. This study introduces a novel approach to semantic IoT transformation, highlighting its implications for wireless networking performance. Key contributions include:

- The proposed Semantic Security Communication Framework (SSCF) deals with the challenge of protecting privacy while maintaining accuracy. Combining the principles of universality and confidentiality, provides an efficient solution for semantic communication.
- Integrating the Advanced Encryption Standard (AES), the SSCF guarantees confidentiality in semantic communication. This approach improves privacy protection, especially in scenarios involving shared background knowledge.
- Employing a Deep Q-Network (DQN) for adversarial training ameliorates semantic communication accuracy while retaining confidentiality. This approach addresses the

difficulty of certifying accuracy in both encrypted and unencrypted modes.

Several recent studies have highlighted the advances and challenges in IoT and semantic communication. In [17], a 5G-based V2X architecture with network slicing was proposed for secure Vehicle-to-Vehicle (V2V) communication. In [18], Privacy-preserving Feature Extraction based on Adversarial Training (P-FEAT) was introduced to enhance privacy in neural networks. In [17], SemProtector, which is a framework to handle security vulnerabilities in semantic communication was presented. In [20], an Information Bottleneck and Adversarial Learning (IBAL) framework was used to optimize the trade-offs between privacy and utility. In [21], a framework was proposed to balance privacy and data utilization in semantic communication. In [22], the Knowledge Discrepancy-oriented Privacy Preserving (KDPP) method was introduced to mitigate privacy risks. In [23, 24], reinforcement learning and semantic-driven approaches were introduced to upgrade privacy and efficiency in IoT systems. In [25, 26], the focus was placed on preserving behavioral semantics and optimizing resource usage through federated edge intelligence. In [27], a smart locker system was proposed, integrating multiple authentication methods, including dual authentication (phone number and OTP), fingerprint, face recognition, and emergency code. Taking advantage of IoT, this approach enhanced security and flexibility, addressing the limitations of single-method systems. A rigorous evaluation demonstrated superior performance, especially in accuracy and flexibility.

The rapid growth of IoT devices has led to an exponential increase in data generation and transmission, posing challenges to existing wireless networks. Traditional communication paradigms struggle to handle the diverse data types and complex interactions in IoT ecosystems, leading to suboptimal performance and scalability issues. The semantic IoT transformation aims to face these challenges by leveraging contextual understanding and intelligence in data processing and communication. However, achieving a seamless integration of semantic capabilities into existing networks involves technical and practical issues, such as interoperability, resource constraints, security, and scalability. There is a pressing need for novel approaches, algorithms, and architectures to fully realize the potential of the semantic IoT transformation and ` wireless networking capabilities. This study explores these matters and proposes innovative solutions to pave the way for efficient, reliable, and secure IoT communication, ultimately enabling seamless interaction and collaboration among IoT devices in smart cities, industrial automation, healthcare, and beyond.

II. PROPOSED METHOD

A. Identification of Privacy Concerns

Semantic communication, which relies on shared background knowledge, faces significant privacy risks due to its inherent sharing mechanism. When users exchange semantic information, they inadvertently expose personal or confidential data. This vulnerability arises because semantic communication often involves the transmission of contextually rich content that can reveal sensitive details about individuals or organizations. Sharing information about preferences, habits, or behaviors can result in privacy breaches if intercepted or accessed by unauthorized parties. Recognizing these privacy concerns is crucial to implement effective protection. Organizations and individuals must implement robust encryption methods, access controls, and privacy-preserving protocols to protect sensitive semantic data. By understanding the risks associated with semantic communication, stakeholders can take proactive measures to ensure a secure exchange of information while preserving privacy. This involves implementing strategies to prevent unauthorized access, limit data exposure, and mitigate the impact of potential privacy breaches.

B. Selection of Encryption Method

The ability of AES to provide strong encryption certifies that sensitive semantic data remain protected, even in the face of potential security threats. AES is widely used, as it offers stronger security compared to its predecessor, the Data Encryption Standard (DES), and its variants such as Triple DES (3DES). The encryption process involves several rounds, each consisting of four main steps:

- SubBytes: Every byte in the segment is substituted with a different byte using a preset Substitution box (S-box).
- ShiftRows: The rows of the segment are shifted continuously to the left.
- MixColumns: Each column of the block is transformed using a matrix multiplication operation.
- AddRoundKey: Every byte of the block is merged with a byte of the iteration key using bitwise XOR.

The number of repetitions depends on the key size: 10 repetitions for a 128-bit key, 12 repetitions for a 192-bit key, and 14 repetitions for a 256-bit key. AES encryption ensures data confidentiality and security, making it suitable for various applications, such as wireless security, database encryption, secure communications, and file encryption. Its robustness against cryptographic attacks and its widespread adoption in both hardware and software implementations make it a cornerstone of modern cryptographic systems.

C. Addressing Semantic Communication Accuracy

Addressing semantic communication accuracy involves recognizing the difficulty in maintaining it in both unencrypted and encrypted modes. This challenge arises due to the encryption process potentially altering the semantic content of the communicated data. In encrypted modes, traditional encryption techniques can obscure the semantic meaning of information, leading to potential misinterpretation or loss of critical details. Similarly, ensuring accuracy in unencrypted modes requires careful handling to prevent unintended disclosures of sensitive semantic information. Thus, addressing this challenge requires the development of innovative solutions that preserve the integrity and meaning of the communicated data while ensuring confidentiality and privacy. Efforts can focus on implementing strategies that strike a balance between encryption for security and semantic preservation for effective communication.

D. Proposed Solution

This study introduces a DQN for adversarial training to overcome the challenge of maintaining semantic communication accuracy while ensuring confidentiality. DQN is a reinforcement learning technique that is used to train a model that can effectively navigate the trade-off between encryption for confidentiality and preserving the semantic content of the communication. Using DQN, the system learns to dynamically optimize the encryption process, adapting to different communication scenarios and requirements. This approach enables the system to achieve semantic communication accuracy, even in encrypted modes, by strategically encrypting the data while preserving its meaning. Thus, using DQN for adversarial training is an innovative solution to address the inherent challenge of maintaining semantic accuracy in secure communication environments.

1) DQN

DQN is a reinforcement learning algorithm that combines deep learning with Q-learning. In DQN, a neural network approximates the Q table, with inputs being state-action pairs and outputs representing the state-value function. To train the neural network, a loss function is introduced to measure the discrepancy between the approximate and actual Q values. The Q-learning update rule is given in (1). The loss function is defined as the Mean Squared Error (MSE) between the predicted and target Q values (2). DQN employs two neural networks: the prediction network and the target network. The prediction network estimates the current Q values, while the target network generates the target Q values. Periodically, the target network parameters are copied from the prediction network to stabilize training. The online neural network is updated using gradient descent based on the loss function, as per (3). DQN follows an off-policy learning approach, where states and rewards are obtained deploying an epsilon-greedy strategy, balancing exploration and exploitation. The agent chooses a random action with probability ε and the best action with probability 1-ε.

$$Q(s,a) \leftarrow Q(s,a) + \alpha[r + \gamma \, max_{\,a'} Q(s',a') - Q(s,a)] \quad (1)$$

$$L(\theta) = E[\sum_{t=1}^{n} \big(y_t - Q(s,a;\theta)\big)^2] \quad (2)$$

$$\nabla_\theta L(\theta) = E\big[\big(y_i - Q(s,a;\theta)\big)\nabla_\theta Q(s,a;\theta)\big] \quad (3)$$

where $Q(s,a)$ is the state-action value operation representing the estimated increasing reward when initiating action a in state s, α represents the learning rate evaluating the weight of new data relative to old data, r is the instant reward obtained, γ defines the discount factor balancing immediate and future rewards, s' is the next state after initiating action a, $max_{\,a'} Q(s',a')$ is the maximum expected cumulative reward in the next state s', and $L(\theta)$ is the loss function measuring the discrepancy between predicted and actual Q values. θ denotes the parameters of the neural network. $\nabla_\theta L(\theta)$ represents the gradient of the loss function concerning the parameters θ of the neural network, y_i is the target Q value for the current sample i, and $\nabla_\theta Q(s,a;\theta)$ defines the gradient of the predicted Q value concerning the parameters θ.

The prediction network is modified employing gradient descent based on the loss function, while the target network periodically copies the parameters from the prediction network to stabilize training. Additionally, the epsilon-greedy strategy is adopted for action selection to balance exploration and exploitation during training.

2) Secure Semantic Communication Framework (SSCF)

SSCF presents a comprehensive solution designed to address the challenges of semantic communication while ensuring privacy and confidentiality. SSCF is conceptualized as a unified framework that combines the principles of universality and confidentiality to protect privacy while supporting the meaningful exchange of information. By integrating advanced encryption techniques with semantic understanding, SSCF enables secure communication channels that protect sensitive data while preserving its intended meaning. This framework is designed to be versatile and adaptable, capable of accommodating various communication scenarios and requirements. The proposed SSCF system operates in a classic security scenario involving three users: Bob, Alice, and Eve. Bob and Alice aim to communicate securely, while Eve attempts to intercept their messages without being able to alter or inject them. The system employs a semantic symmetric cryptosystem, shown in Figure 1. Alice initiates the communication by encoding the confidential semantic message S, producing a ciphertext x_k through semantic and channel encoding. Here, k denotes key encryption. The encrypted message is then delivered via a wireless network, where Bob acquires y^k and Eve acquires $y^{\sim k}$. Both Bob and Eve aim to recover S, resulting in S_{bob} and S_{eve}, respectively. In particular, Bob has a benefit over Eve, as he transfers a private key to Alice. This key, treated as an additional input, ensures secure communication between Bob and Alice. Each semantic message S corresponds to a new key at the time of communication, enhancing the system's security.

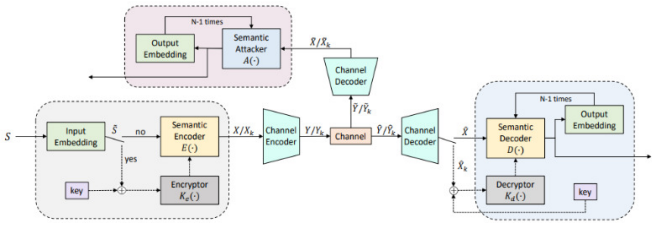

Fig. 1. SSCF structure.

The proposed SSCF offers both universality and confidentiality, allowing users to choose whether to encrypt their messages according to privacy requirements. The system's semantic encoding module is generic, ensuring compatibility across various scenarios, including broadcast channels. Additionally, unified model training improves system efficiency and reduces deployment complexity. For text-type input, such as sentences, the system tokenizes the input and maps every token to a fixed-dimensional vector through a word embedding layer. The transmitter decides whether to encrypt the semantic data. If encryption is required, the input is passed to the encryptor along with the encryption key. Otherwise, the

input is directly processed by the semantic encoder for semantic encoding. The system employs a transformer network as a semantic codec and an autoencoder for channel coding. The encryptor and decryptor networks share a similar structure, reshaping the original semantic message and key before applying dimensional transformations. The encryption approach is trained by the network, with the length of the key not determining its strength. The system considers Additive White Gaussian Noise (AWGN) channels for transmission, where Bob decodes unencrypted messages directly and decrypts encrypted ones before decoding. The semantic decoder structure is identical for both receivers and attackers, facilitating semantic message reconstruction.

In the SSCF, the design of loss functions is pivotal to achieving optimal performance while ensuring confidentiality. The objectives of each participant, Alice, Bob, and Eve, are carefully considered, leading to the formulation of specific loss functions tailored to their roles and objectives.

a) Unencrypted Semantic Communication

The loss function is defined as $L_{ED}(\theta_E, \theta_D)$ aiming to minimize the error between the original semantic message S and the reconstructed message at Bob's end. By jointly training the semantic decoder (D) and encoder (E), optimal parameters θ_E and θ_D are obtained to minimize this loss using:

$$L_{ED}(\theta_E, \theta_D) = D_{CE}\left(S, D\left(\theta_D, E(\theta_E, \theta_S)\right)\right) \quad (4)$$

$$\theta_E, \theta_D = argmin_{\theta_E, \theta_D} L_{ED}(\theta_E, \theta_D) \quad (5)$$

b) Encrypted Semantic Communication

In scenarios requiring confidentiality, the loss function $L_{K_d}(\theta_{K_e}, \theta_E, \theta_{K_d}\theta_D)$ is described in (6). It involves the semantic encoder E, encryptor K_E, decryptor K_d, and semantic decoder D, aiming to minimize the error between the original message S and its reconstruction at Bob's end, while increasing the error between S and its reconstruction by Eve. The optimal parameters for the decryptor O_{K_d} are obtained by minimizing this loss employing:

$$L_{K_d}\left(\theta_{K_e}, \theta_E, \theta_{K_d}\theta_D\right) =$$

$$D_{CE}\left(S, D\left(\theta_D, K_d(\theta_{K_d}, E\left(\theta_E, K_E(\theta_{K_e}, S)\right)\right)\right)\right) \quad (6)$$

$$O_{K_d}\left(\theta_{K_e}\right) = argmin_{\theta_{K_d}} L_{K_d}\left(\theta_{K_e}, \theta_E, \theta_{K_d}, \theta_D\right) \quad (7)$$

c) Semantic Attacker

The attacker intercepts the encrypted data and attempts to restore the semantic data. The loss function $L_A(\theta_{K_e}, \theta_E, \theta_A)$ aims to minimize the error between the original message S and the reconstructed message by the attacker (A) using (8). The optimal parameters for the attacker (θ_A) are attained by minimizing this loss :

$$L_A\left(\theta_{K_e}, \theta_E, \theta_A\right) =$$

$$D_{CE}\left(S, A\left(\theta_A, E\left(\theta_E, K_e(\theta_{K_e}, S)\right)\right)\right) \quad (8)$$

$$O_A(\theta_A) = argmin_{\theta_A}\left(L_A\left(\theta_{K_e}, \theta_E, \theta_A\right)\right) \quad (9)$$

d) Balancing Utility and Confidentiality

The overall loss function $L_A(\theta_{K_e}, \theta_E, \theta_A)$ for the encryptor (K_e) incorporates both the decryption loss L_{K_d} and the attacker's loss L_A. A hyper-parameter λ balances confidentiality and utility, guiding the optimization process given as in (10). Optimal parameters for the encryptor (θ_{K_e}) are acquireed by minimizing this combined loss as in (11). The training process for the encrypted semantic communication network is carefully refined to ensure robustness and adaptability. It involves two main steps, each meticulously designed to optimize performance while addressing specific challenges.

$$L_{K_e}\left(\theta_{K_e}\right) =$$

$$L_{K_d}(\theta_{K_e}, \theta_E, \theta_{K_d}, \theta_D) - \lambda L_A(\theta_{K_e}, \theta_E, O_A(\theta_A)) \quad (10)$$

$$O_{K_e}\left(\theta_{K_e}\right) = argmin_{\theta_{K_e}} L_{K_e}\left(\theta_{K_e}\right) \quad (11)$$

e) Training Channel Encoder and Decoder

Initially, the focus is on training the channel decoder and encoder with a symmetric framework. These components compress the input vector and map it to symbols with real and imaginary parts. Randomly generated vectors, similar to encoded semantic vectors, are used for training. The channel parameters are dynamically modified within a specified range during training to improve robustness. MSE serves as a depletion measure to eliminate misrepresentation.

f) Alternating Training of Attacker and Transmitter-Receiver

Following a strategy reminiscent of Generative Adversarial Networks (GAN), the attacker is alternately trained with the receiver and transmitter. Through iterative steps, the semantic encoder and decoder adapt to meet semantic communication requirements. Meanwhile, the decryptor refines its decryption approach, while the semantic attacker tries to figure out how to directly decode encrypted messages. This iterative process involves updating the encryptor to decrease the receiver's restoration error while increasing the attacker's restoration error, thus fostering encryption methods that are receiver-friendly yet resilient against eavesdropping. Through this refined training approach, the encrypted semantic communication network evolves to achieve optimal performance, striking a delicate balance between communication efficiency and security.

3) Implementation and Evaluation of SSCF

Training all network SSCF modules involved implementing a shared database, allows extensive deployment in practical scenarios while ensuring consistency and scalability. This approach certified that the system's components were trained on a unified dataset, facilitating seamless integration and interoperability. In terms of confidentiality measures, SSCF implemented symmetric encryption to protect the privacy of semantic information during communication. By encrypting the data using a shared key, SSCF ascertained that sensitive information remained protected from unauthorized access or interception, thus preserving the confidentiality of user

communications. To ensure the accuracy of semantic communication under diverse conditions, SSCF deployed an adversarial encryption training scheme. This approach involved training the system to recognize and adapt to potential security threats, therefore enhancing SSCF's resilience against adversarial attacks and ensuring reliable communication across various scenarios. Experimental evaluations were performed to validate the effectiveness of SSCF and its adversarial encryption training scheme. These experiments demonstrated robust performance and security, confirming SSCF's ability to protect privacy while supporting semantic communication in real-world environments. SSCF emerged as an efficient solution for privacy-preserving semantic communication, offering a balance between security and usability. Moving forward, ongoing research and development efforts aim to further enhance SSCF's performance and security, ensuring its continued effectiveness in addressing evolving communication challenges.

III. RESULTS AND DISCUSSION

The effectiveness of the proposed SSCF was assessed using numerical analysis. The experiments utilized the European Parliament's standard proceedings dataset [28], comprising approximately 2.0 million sentences. The evaluation of the SSCF scheme on this extensive dataset aims to provide comprehensive insights into its performance in various communication scenarios, shedding light on its robustness and efficacy in real-world applications. Figures 2 and 3 visually represent the original and encrypted data, respectively. This illustration highlights the transformation process from plaintext to ciphertext, emphasizing the protective measures implemented to protect sensitive information during communication.

sort_id	date_d_m	time	sensor_id	sensor_ty	temp_C	hpa_div_4	batterylev	sensor_cycle
1	5.02.2016	13:01:06	310	B	1612	24861	0	66
3	5.02.2016	13:01:16	306	B	1737	24865	0	69
6	5.02.2016	13:02:40	368	B	1941	24842	0	78
12	5.02.2016	13:03:32	367	B	1811	24834	0	78
20	5.02.2016	13:04:13	365	B	1577	24842	0	75
23	5.02.2016	13:04:45	302	B	1684	24850	0	75
31	5.02.2016	13:06:49	306	B	1554	24866	0	72
38	5.02.2016	13:09:06	367	B	1643	24832	0	81
45	5.02.2016	13:09:51	365	B	1435	24838	0	78
48	5.02.2016	13:10:20	302	B	1550	24847	0	78
56	5.02.2016	13:12:22	306	B	1423	24863	0	75
61	5.02.2016	13:13:38	368	B	1760	24839	0	84

Fig. 2. Original data.

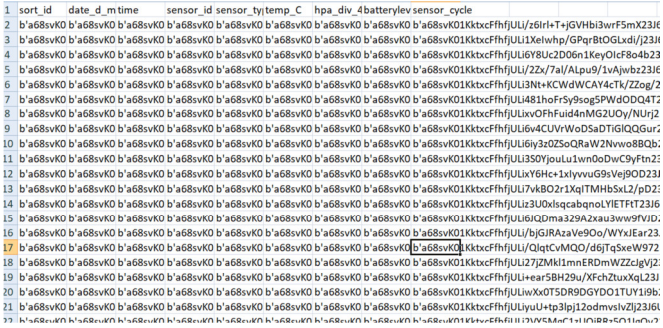

Fig. 3. Encrypted data.

A. Performance Metrics

Security level (S) is given by:

$$S = f(encryption, vulnerability\ count, attack\ resilience)$$

Throughput (T) is given by:

$$T = \frac{Total\ Data\ Transferred (bits\ or\ bytes)}{total\ time\ (s)}$$

Delay (D) is given by:

$$D = Transmission\ Time + Propagation\ Time + Processing\ Time + Queuing\ Time$$

Accuracy (A) is given by:

$$A = \frac{no\ of\ correct\ predictions}{total\ number\ of\ predictions}$$

Execution Time is given by:

$$E = End\ Time - Start\ Time$$

Task Success Rate (TSR) is given by:

$$TSR = \frac{Number\ of\ successfully\ completed\ tasks}{Total\ tasks\ attempted} \quad (17)$$

B. Graphical Representation

Figure 4 provides a graphical representation of key performance metrics across varying epochs. Security level denotes the degree of protection against unauthorized access or breaches, often measured in encryption strength or resilience to attacks. Throughput illustrates the rate at which data are successfully transmitted over the network, indicating system efficiency. Delay indicates the time it takes for the data to travel from the source to the destination, influencing real-time communication. Accuracy reflects the precision of prediction tasks, crucial for reliable decision-making. Execution time denotes the time taken to complete computational tasks and system responsiveness. These representations evaluate the system's evolution over time, allowing the identification of trends and parameter optimizations to achieve desired performance objectives.

Table I compares the task success rates of different encryption methods (TLP-random, SNRLP, SET, Bob's Task) against the proposed one for varying data sizes, ranging from 2 to 10 MB. For a data size of 2 MB, TLP-random achieved a success rate of 0.71, SNRLP 0.89, SET 0.94, Bob's Task 0.76, and the proposed method 0.97. At 4 MB, the success rates were 0.68 for TLP-random, 0.86 for SNRLP, 0.92 for SET, 0.74 for Bob's Task, and 0.96 for the proposed method. For 6 MB, TLP-random achieved 0.64, SNRLP 0.85, SET 0.88, Bob's Task 0.69, and the proposed method 0.95. At 8 MB data size, TLP-random had a 0.62 success rate, SNRLP 0.78, SET 0.86, Bob's Task 0.67, and the proposed method 0.92. Finally, for 10 MB, the success rates were 0.6 for TLP-random, 0.74 for SNRLP, 0.85 for SET, 0.65 for Bob's Task, and 0.88 for the proposed method. Figure 5 also exhibits the task success rate comparison. The proposed method consistently achieved higher success rates across all data sizes (2 MB to 10 MB), demonstrating its superior performance in ensuring successful task completion.

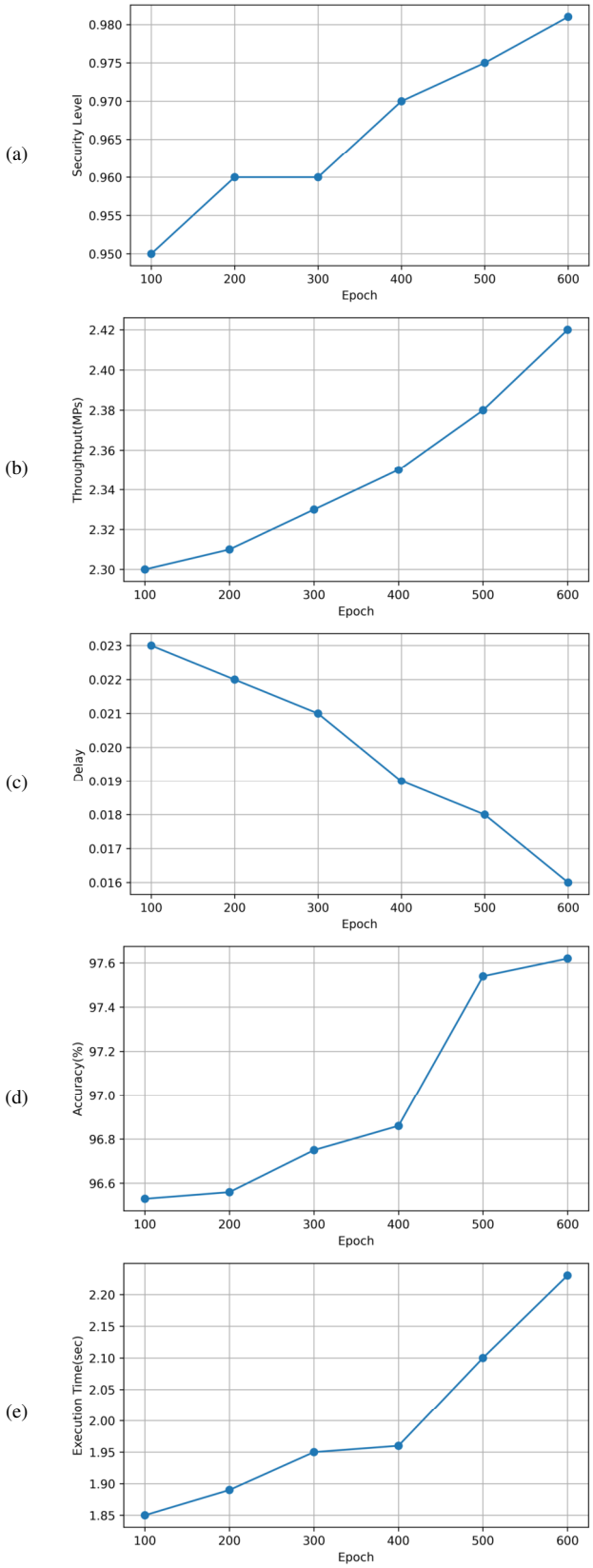

Fig. 4. Metrics in varying epochs: (a) security level, (b) throughput, (c) delay, (d) accuracy, and (e) execution time.

TABLE I. TASK SUCCESS RATE COMPARISON

Data size (MB)	TLP-random	SNRLP	SET	Bob's Task	Proposed
2	0.71	0.89	0.94	0.76	0.97
4	0.68	0.86	0.92	0.74	0.96
6	0.64	0.85	0.88	0.69	0.95
8	0.62	0.78	0.86	0.67	0.92
10	0.6	0.74	0.85	0.65	0.88

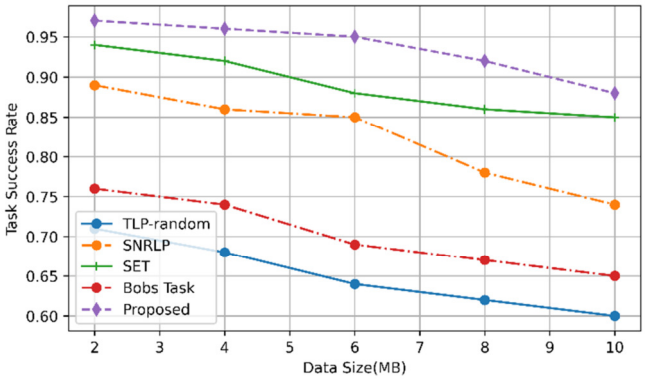

Fig. 5. Task success rate comparison.

IV. CONCLUSION

Accurate semantic communication is difficult to be ensured in both encrypted and unencrypted forms. This study proposed adversarial training with DQN, along with the AES encryption method to improve semantic communication accuracy. The SSCF method introduced is an answer to these difficulties, integrating confidentiality and universality to protect privacy. Additionally, large-scale deployment in real-world situations was made possible by the fact that every network SSCF module was trained utilizing a common database. An adversarial encryption training technique ensures semantic communication accuracy in diverse scenarios and symmetric encryption maintains confidentiality. Experimental results showed the effectiveness of SSCF and its adversarial encryption training method. No matter the encryption status, the SSCF functioned flawlessly, making it difficult for adversaries to piece together the original semantic information from intercepted messages. SSCF is a strong solution to privacy-preserving semantic communication, as it integrates heuristic techniques to improve efficiency and security.

Looking ahead, future work could explore improvements by integrating advanced machine learning algorithms to improve authentication accuracy and robustness. Additionally, research efforts can focus on expanding the system's compatibility with emerging IoT technologies and standards to assure seamless integration and interoperability in diverse environments. Additionally, investigating the implementation of blockchain technology to enhance security and transparency in access control processes is a promising avenue for future exploration.

REFERENCES

[1] M. Anwer, S. M. Khan, M. U. Farooq, and Waseemullah, "Attack Detection in IoT using Machine Learning," *Engineering, Technology &*

Applied Science Research, vol. 11, no. 3, pp. 7273–7278, Jun. 2021, https://doi.org/10.48084/etasr.4202.

[2] Y. Wang, W. Yang, P. Guan, Y. Zhao, and Z. Xiong, "STAR-RIS-Assisted Privacy Protection in Semantic Communication System," *IEEE Transactions on Vehicular Technology*, pp. 1–6, 2024, https://doi.org/10.1109/TVT.2024.3383824.

[3] Y. Wang, Z. Tian, Y. Sun, X. Du, and N. Guizani, "Preserving Location Privacy in UASN through Collaboration and Semantic Encapsulation," *IEEE Network*, vol. 34, no. 4, pp. 284–290, Jul. 2020, https://doi.org/10.1109/MNET.001.1900534.

[4] X. Luo *et al.*, "A Lightweight Privacy-Preserving Communication Protocol for Heterogeneous IoT Environment," *IEEE Access*, vol. 8, pp. 67192–67204, 2020, https://doi.org/10.1109/ACCESS.2020.2978525.

[5] W. Iqbal, H. Abbas, B. Rauf, Y. A. Bangash, M. F. Amjad, and A. Hemani, "PCSS: Privacy Preserving Communication Scheme for SDN Enabled Smart Homes," *IEEE Sensors Journal*, vol. 22, no. 18, pp. 17677–17690, Sep. 2022, https://doi.org/10.1109/JSEN.2021.3087779.

[6] G. S. Poh, P. Gope, and J. Ning, "PrivHome: Privacy-Preserving Authenticated Communication in Smart Home Environment," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1095–1107, Feb. 2021, https://doi.org/10.1109/TDSC.2019.2914911.

[7] J. N. Liu, J. Weng, A. Yang, Y. Chen, and X. Lin, "Enabling Efficient and Privacy-Preserving Aggregation Communication and Function Query for Fog Computing-Based Smart Grid," *IEEE Transactions on Smart Grid*, vol. 11, no. 1, pp. 247–257, Jan. 2020, https://doi.org/10.1109/TSG.2019.2920836.

[8] R. Tan, Y. Tao, W. Si, and Y. Y. Zhang, "Privacy preserving semantic trajectory data publishing for mobile location-based services," *Wireless Networks*, vol. 26, no. 8, pp. 5551–5560, Nov. 2020, https://doi.org/10.1007/s11276-019-02058-8.

[9] C. Iwendi, S. A. Moqurrab, A. Anjum, S. Khan, S. Mohan, and G. Srivastava, "N-Sanitization: A semantic privacy-preserving framework for unstructured medical datasets," *Computer Communications*, vol. 161, pp. 160–171, Sep. 2020, https://doi.org/10.1016/j.comcom.2020.07.032.

[10] S. A. Moqurrab, A. Anjum, N. Tariq, and G. Srivastava, "Instant_Anonymity: A Lightweight Semantic Privacy Guarantee for 5G-Enabled IIoT," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 951–959, Jan. 2023, https://doi.org/10.1109/TII.2022.3179536.

[11] W. Yang *et al.*, "Semantic Communication Meets Edge Intelligence," *IEEE Wireless Communications*, vol. 29, no. 5, pp. 28–35, Oct. 2022, https://doi.org/10.1109/MWC.004.2200050.

[12] H. Kiya, T. Nagamori, S. Imaizumi, and S. Shiota, "Privacy-Preserving Semantic Segmentation Using Vision Transformer," *Journal of Imaging*, vol. 8, no. 9, Sep. 2022, Art. no. 233, https://doi.org/10.3390/jimaging8090233.

[13] R. Bi, J. Xiong, Y. Tian, Q. Li, and K. K. R. Choo, "Achieving Lightweight and Privacy-Preserving Object Detection for Connected Autonomous Vehicles," *IEEE Internet of Things Journal*, vol. 10, no. 3, pp. 2314–2329, Oct. 2023, https://doi.org/10.1109/JIOT.2022.3212464.

[14] Y. Cai, S. Zhang, H. Xia, Y. Fan, and H. Zhang, "A Privacy-Preserving Scheme for Interactive Messaging Over Online Social Networks," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6817–6827, Dec. 2020, https://doi.org/10.1109/JIOT.2020.2986341.

[15] J. Chen, J. Wang, C. Jiang, Y. Ren, and L. Hanzo, "Trustworthy Semantic Communications for the Metaverse Relying on Federated Learning," *IEEE Wireless Communications*, vol. 30, no. 4, pp. 18–25, Aug. 2023, https://doi.org/10.1109/MWC.001.2200587.

[16] W. Ma *et al.*, "FedSH: Towards Privacy-Preserving Text-Based Person Re-Identification," *IEEE Transactions on Multimedia*, vol. 26, pp. 5065–5077, 2024, https://doi.org/10.1109/TMM.2023.3330091.

[17] H. Mun, M. Seo, and D. H. Lee, "Secure Privacy-Preserving V2V Communication in 5G-V2X Supporting Network Slicing," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 14439–14455, Sep. 2022, https://doi.org/10.1109/TITS.2021.3129484.

[18] X. Ding, H. Fang, Z. Zhang, K. K. R. Choo, and H. Jin, "Privacy-Preserving Feature Extraction via Adversarial Training," *IEEE Transactions on Knowledge and Data Engineering*, vol. 34, no. 4, pp. 1967–1979, Apr. 2022, https://doi.org/10.1109/TKDE.2020.2997604.

[19] X. Liu *et al.*, "SemProtector: A Unified Framework for Semantic Protection in Deep Learning-based Semantic Communication Systems," *IEEE Communications Magazine*, vol. 61, no. 11, pp. 56–62, Nov. 2023, https://doi.org/10.1109/MCOM.003.2200777.

[20] Y. Wang, S. Guo, Y. Deng, H. Zhang, and Y. Fang, "Privacy-Preserving Task-Oriented Semantic Communications Against Model Inversion Attacks," *IEEE Transactions on Wireless Communications*, 2024, https://doi.org/10.1109/TWC.2024.3369170.

[21] L. Zhao, D. Wu, and L. Zhou, "Data Utilization Versus Privacy Protection in Semantic Communications," *IEEE Wireless Communications*, vol. 30, no. 3, pp. 44–50, Jun. 2023, https://doi.org/10.1109/MWC.007.2200503.

[22] S. Cheng, X. Zhang, Y. Sun, Q. Cui, and X. Tao, "Knowledge Discrepancy Oriented Privacy Preserving for Semantic Communication," *IEEE Transactions on Vehicular Technology*, pp. 1–10, 2024, https://doi.org/10.1109/TVT.2024.3381222.

[23] M. Min, W. Wang, L. Xiao, Y. Xiao, and Z. Han, "Reinforcement learning-based sensitive semantic location privacy protection for VANETs," *China Communications*, vol. 18, no. 6, pp. 244–260, Jun. 2021, https://doi.org/10.23919/JCC.2021.06.019.

[24] M. Rodriguez-Garcia, M. Batet, D. Sánchez, and A. Viejo, "Privacy protection of user profiles in online search via semantic randomization," *Knowledge and Information Systems*, vol. 63, no. 9, pp. 2455–2477, Sep. 2021, https://doi.org/10.1007/s10115-021-01597-x.

[25] G. Qiu, G. Tang, C. Li, D. Guo, Y. Shen, and Y. Gan, "Behavioral-Semantic Privacy Protection for Continual Social Mobility in Mobile-Internet Services," *IEEE Internet of Things Journal*, vol. 11, no. 1, pp. 462–477, Jan. 2024, https://doi.org/10.1109/JIOT.2023.3287644.

[26] G. Shi, Y. Xiao, Y. Li, and X. Xie, "From Semantic Communication to Semantic-Aware Networking: Model, Architecture, and Open Problems," *IEEE Communications Magazine*, vol. 59, no. 8, pp. 44–50, Aug. 2021, https://doi.org/10.1109/MCOM.001.2001239.

[27] M. Balfaqih, "Enhancing Security and Flexibility in Smart Locker Systems: A Multi-Authentication Approach with IoT Integration," in *2024 21st Learning and Technology Conference (L&T)*, Jeddah, Saudi Arabia, Jan. 2024, pp. 325–329, https://doi.org/10.1109/LT60077.2024.10469610.

[28] "Datasets | European Parliament's Open Data Portal." https://data.europarl.europa.eu/en/datasets?language=en&order=RELEVANCE.

AUTHORS PROFILE

Ibrahim Alzahrani received his Ph.D. in optimizing video streaming over HTTP using AI techniques from the University of the West of Scotland in 2020. He received his M.Sc. in Advanced Computer Networking from Glasgow Caledonian University in 2014. Currently, he is an Assistant Professor at the Computer Science and Engineering Department, Deanship of E-Learning & Digital Transformation. His research interests are in the domains of AI, video streaming, computer networks, computer security, cloud computing, blockchains, and HCI.