FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 54-59 | e-ISSN: 2347-470X

Deep Learning based Effective Watermarking Technique for IoT Systems Signal Authentication

Dr. Manish Korde[1], Dr. Vinit Gupta[2], Dr. Aditya Mandloi[3], Dr. Sachin Puntambekar[4], Devendra Singh Bais[5]

[1]Assistant Professor, Department of Electronics and Communication Engineering, Medi-Caps University, Indore, Madhya Pradesh, India. Email: manish.korde@medicaps.ac.in
[2]Assistant Professor, Department of Electronics and Communication Engineering, Medi-Caps University, Indore, Madhya Pradesh, India. Email: vinit@medicaps.ac.in
[3]Assistant Professor, Department of Electronics and Communication Engineering, Medi-Caps University, Indore, Madhya Pradesh, India. Email: aditya.mandloi@medicaps.ac.in
[4]Assistant Professor, Department of Electronics and Communication Engineering, Medi-Caps University, Indore, Madhya Pradesh, India. Email: sachin.puntambekar@medicaps.ac.in
[5]Assistant Professor, Department of Electronics and Communication Engineering, Medi-Caps University, Indore, Madhya Pradesh, India. Email: devendrasingh.bais@medicaps.ac.in

***Correspondence:** manish.korde@medicaps.ac.in

ABSTRACT- In order to identify cyber-attacks, this research suggests a special watermarking technique for dynamic IoT System signal validation. IoT Systems (IoTSs) can extract a group of randomly generated characteristics from their produced signal and then periodically watermark these attributes into the transmission owing to the proposed efficient watermarking technique. Using dynamic watermarking for IoT signal authentication, a potent deep learning technique is used to detect cyber-attacks. Based on an LSTM structure, the proposed learning system enables IoT devices to extract a set of random features from the signal they release, hence enabling dynamic watermarking of the signal. This method allows the IoT cloud centre to gather signals from IoT devices and effectively confirm the signals' legitimacy. Deep Reinforcement Learning is applied to authenticate the incomplete information. Therefore, the proposed approach provides robust defense against complex attacks, such as eavesdropping, enhancing IoT security.

Keywords: Long Short-Term Memory, IoT System, Dynamic Watermarking, Deep Reinforcement Learning, Signal Authentication.

ARTICLE INFORMATION

Author(s): Dr. Manish Korde, Dr. Vinit Gupta, Dr. Aditya Mandloi, Dr. Sachin Puntambekar, Devendra Singh Bais;
Received:14/09/2023; **Accepted:** 06/01/2024; **Published:** 05/02/2024;
Paper Id: IJEER231005;
Citation: 10.37391/IJEER.120109
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-12/ijeer-120109.html

Publisher's Note: FOREX Publication stays neutral with regard to jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

A key component in accelerating the widespread use of the Internet of Things' services and apps is to secure it. Particularly, the IoT devices' functionality heavily depends on the accuracy of their message delivery. Significant security issues are posed by cyber-attacks such data injection, eavesdropping, and man-in-the-middle vulnerabilities [1]. However, near real-time, reliable, and low complication delivery of messages from IoTSs is necessary for the deployment of IoT services to be successful [2]. Perceptual, network, support, and application are the four layers that make up the majority of IoT architectures. The perceptive layer, which is the most elementary layer, gathers data from the physical world in a variety of ways utilizing instruments like accelerometers and RFID tags [3].

Nowadays, the usage of Quick Response (QR) codes is one of the most popular methods for IoT onboarding. The utilization of pin codes or serial numbers is one of the more well-liked out-of-band IoT on boarding strategies [4]. With the use of a mobile device, a user can translate a QR code from an IoT device into a URL. However, since the QR code is printed on the device, unauthorized individuals who have physical accessibility can able to connect it onto their own private network and meddle with it. As a result, such onboarding solutions often do not defend against unauthorized devices.
Securing IoT signals at this layer is notoriously difficult because of the easy accessibility of the equipment and parts at the perception layer and their limited resources nature [5]. The watermarking process technology is embedded into various frames rather than adding an overhead like in traditional encryption. As a result, it is effective for encryption of information in applications that employ very few resources, such as IoT [6]. The fundamental issue with a simple Recurrent Neural Network (RNN) is short-term memory. RNN might overlook vital information in long-sequence data because to the difficulties in transmitting information from prior time steps to succeeding stages.

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 54-59 | e-ISSN: 2347-470X

RNNs are a type of Artificial Neural Network (ANN) that may be used to analyze time series. An ANN is a type of function approximation that maps an input vector to a target vector. They are composed of layers of artificial neurons that accept a vector as input, aggregate it, and then transmit it via an activation function. The desired vector is the result of the activation parameter of the final layer that was used. While such ANNs convert an input vector to a product vector, RNNs also feedback the output, making them appropriate for analyzing time dependency in the input.

The discovery of Long Short-Term Memory (LSTM) gates assisted in the resolution of the short-term memory problem. The flow of information can be controlled using gates. The gates can store a long string of critical data while eliminating irrelevant data.

Employing a deep learning LSTM structure, the proposed watermarking technique allows IoT systems (IoTS) to extract a collection of stochastic characteristics from their produced signal and constantly watermark these characteristics into the transmitted data. This solution permits the IoT gateway, typically aggregates signals among IoTSs, to properly validate the signal's accuracy and dependability.

The goal of this research is to improve the security of IoT systems by using a novel watermarking method. IoT devices periodically watermark their signals to validate the random features they derive from them. Signal authenticity is ensured by dynamic signal watermarking made possible by deep learning, more especially by LSTM structures. The method offers strong protection against complex attacks like eavesdropping by using Deep Reinforcement Learning to validate missing input. This technique greatly improves cybersecurity for IoT devices by verifying signals in real-time, protecting against various cyberthreats and guaranteeing the integrity of sent data.

Section 1 contains introductory part of effective watermarking in IoTS signal authentication followed by related works are discussed in *section 2*. *Section 3* discusses about proposed methodology followed by *section 4* describes its results and discussion. *Section 5* concludes with advantages, limitations and future work.

Some of the security solutions that have been carried out for IoT signal authentication are addressed below. For the purpose of safeguarding IoT applications, physical layer security approaches are being researched [7]. These techniques include of artificial noise signal transmission, optimal sensor filtering, etc. By utilizing cryptography at the IoT's physical layer, the security hole in IoTS's was developed [8]. The method of communication used by a large number of resource-constrained devices that produce huge amounts of data affects the security and privacy of the objects involved.

Consequently, a security technique known as the lightweight authenticating procedure for IoT had been proposed. Instead of adopting a sophisticated encryption technique like the hash function, an encryption method based on XOR manipulation was used in this case to protect privacy and prevent counterfeiting [9]. Additionally, established learning algorithms for authenticating and fingerprinting IoTSs and their surroundings are detailed in [10]. The use of watermarking technique eliminates the need for an overheard as in traditional encryption by integrating it directly into various frames. The IoT gateway's resource limitations for authentication are still not up to the standard, though.

The detection model of fraudulent activity sensor's attacks for general LTI platforms has been established and an additional set of asynchronous and statistical assessments are provided [11]. An adaptive watermarked approach has been suggested to recognize fraudulent activity sensor attacks for LTI systems with a full rank input matrices and state assessments. Instead of reiterating assaults, this model assists in identifying a specific attack model. However, this model has computational cost limitations.

In order to reduce the theft of information by a type of Gaussian intruder in the system, an information mathematical model has been carried out. The attacker must substitute the control input with the realization of a Gaussian distributed random variable in order to experience the most significant performance deterioration for any given amount of stealthiest on the attacker's part [12]. This system has capable of resistance to the proliferation of cyber-physical systems, which are crucial to the physical plant but lack reliable security guarantees. Actuators are used to inject private excitation into the system, which is watermarked to reveal signal manipulation by turning off the closed loop control signal [13]. Data is hidden using information gathering and data encapsulation methods that utilize a security approach known as digital watermarking. Because of the significant computational and bandwidth requirements, the gateway in an enormous scale IoT system is unable to independently verify all of the signals that are sent from the IoTSs.

Adaptive Watermarking strategies [14], in which anonymous stimulation has been inserted into the control inputs to protect the resultant measurement information, have started to deal with the issues of identifying these assaults, but are limited to linear time-invariant (LTI) systems. As a result, a linear time-varying (LTV) extension of prior dynamic watermarking methods was created by constructing a matrix normalization factor to suit the system's periodic variations. However, this strategy does not account for sophisticated attacks like spying, where the attacker gathers information over an extended period of time.

Mixed-strategy Nash equilibria (MSNE) are particularly useful in modeling situations where players have uncertainty or randomness in their decision-making, as well as in scenarios where there is no clear dominant strategy for any player. These equilibria help predict the likely outcomes of games with mixed strategies and provide insights into strategic interactions in various real-world situations [15]. However, the system possesses high bit error rate that minimizes the authenticating features.

Replay assaults are simple to carry out on such systems and have the ability to cause substantial damage. In consequence,

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 54-59 | e-ISSN: 2347-470X

prompt detection of replaying attacks is critical for mitigating the attack's implications. Researchers present a realistic watermarking methodologies like physical watermarking, dynamic watermarking, etc. for stealthy and replay attacks identification [16]. DLWIoT, named as Deep Learning-based Watermarking for authorised IoT initialization [17], is an image watermarking system that uses deep neural networks and is both reliable and entirely automated. By embedding authentication information into carrier images (such as QR codes printed on IoT devices), DLWIoT makes it possible for only authorised users to initiate IoT onboarding.

2. EFFECTIVE WATERMARKING FOR IOT USING DL

The IoT gateway can verify IoTS signals and identify the presence of a cyber-attacker who aims to harm the IoT by changing its output signal thanks to a powerful watermarking framework that is offered. In order to watermark these properties throughout the source point, the proposed effective watermarking technique leverages deep learning-based LSTM blocks to retrieve stochastic features from the IoT signal, such as spectral flatness, skewness, kurtosis, and central moments.

By lowering the degree of difficulty and duration of data insertion recognition, Effective Watermarking based on LSTM (EW-LSTM) efficiently integrates other security measures like encryption. Here, a network of N IoTSs that are in communication with a gateway such a base station is regarded to be a large-scale IoT system. Any IoTS in the system will produce a signal with a rate of sampling frequency, and then this signal is communicated to gateway. Figure 1 describes the structure of LSTM. A forget gate that receives an additional input known as the cell state input (S_{t-1}) with tanh function and learns how much it should remember or recall in the past. An input gate that aggregates the output of previous steps (h_{t-1}) and the present input and sends it through a function that activates in a similar way as a standard RNN does. An output gate (h_t) of LSTM combines the present state of the cell and the output of the input gate to form the LSTM response. Here σ represents gate activation function indicates with sigmoid.

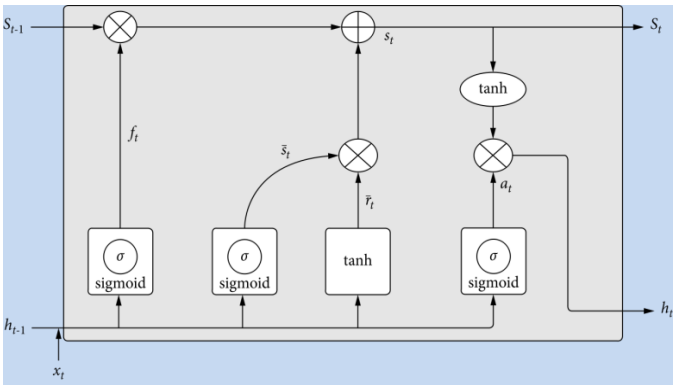

Figure 1. LSTM block Architecture

This approach addresses missing data challenges in a large-scale IoT scenario through its dynamic watermarking technique and DRL application. By utilizing LSTM structures, IoT devices can watermark signals even with missing data, ensuring signal authenticity. DRL is employed to authenticate incomplete information, enabling the system to effectively handle and validate data gaps. This adaptive mechanism allows the approach to function seamlessly despite missing data, ensuring the integrity and security of IoT signals in real-time.

2.1 Attack Detection using Dynamic Watermarking

By using dynamic feature extraction process, the gateway can recognize attacks including dynamic data injection, whereby the attacker can capture and analyze IoT signals, obtain the watermarking key, and inject false data. Additionally, the LSTM-based watermarking that is being proposed works well to supplement existing security measures like encryption. Digital fingerprints of the signal "yi" provided by an IoTS that modifies the bit stream are used in the proposed dynamic watermarking approach. Signal fingerprinting can be extracted using stochastic properties including spectral flatness, central moments, skewness, and kurtosis. Due to the IoTS signal stream's temporal reliance on earlier time steps, the potent deep LSTM system is used, which is more useful for sequencing analysis.

In LSTM, the input gate combines the present input and previous outputs then passes it through the activation function. The output gate integrates the cell's present form and the result of the inputting gate and produces the results of LSTM. Memory gate learns how much information it should remember or disregard from prior inputs from the cell's present state input.

Using an LSTM technique, which enables an IoTS to modify the stream of bits in accordance with the order of generated data, it is possible to constantly extract fingerprinting from IoTS signals. When processing an input (yi (1), yi(n_{ns})), an LSTM algorithm uses gates to determine the capability of how much data can be stored, how much data can be deleted, and how much present data can be used. Therefore, LSTMs are appropriate for IoT applications where the extraction of biometrics from signals depends on earlier time periods. Inside LSTM blocks at IoTS's and gateway, the dynamic bit streams are formed. Data aggregation and recording procedure does not increase the key power ratio succession to signal and the adversaries may not have the capability of retrieving the keys and bit streams. Continuous bit stream production at LSTM blocks overcomes the problem of data injection attacks. The authentication code and obtained watermarked signal from the LSTM are sent to the gateway. Then, the two outputs such as extracted features and extracted bits are compared.

This proposed effective watermarking-based LSTM system consists of an offline training phase. The training phase of the proposed model at IoTS is given in *figure 2*. As a result, an LSTM network is offline trained for each IoTS before being implemented at the appropriate IoTS. Additionally, the gateway may authenticate any IoTS signal using the suggested technique with a time delay '*d*'. Training Phase of Proposed EW-LSTM model at Gateway is shown in *figure 3*. *Figure 4* shows the attack model for the proposed EW-LSTM system.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 54-59 | e-ISSN: 2347-470X

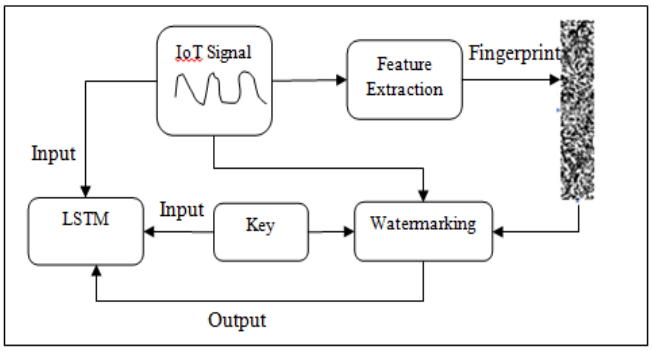

Figure 2. Training phase at IoTS – Proposed Model

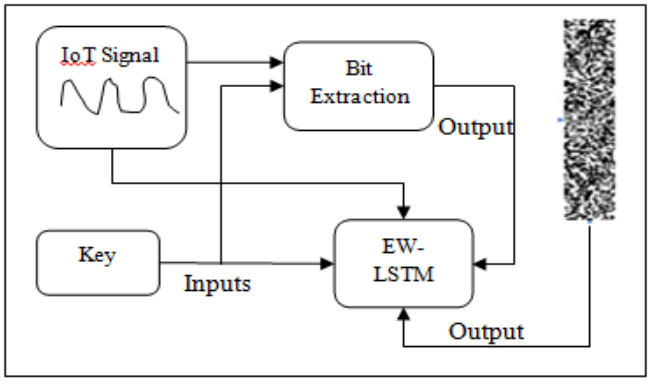

Figure 3. Training phase at Gateway – Proposed Model

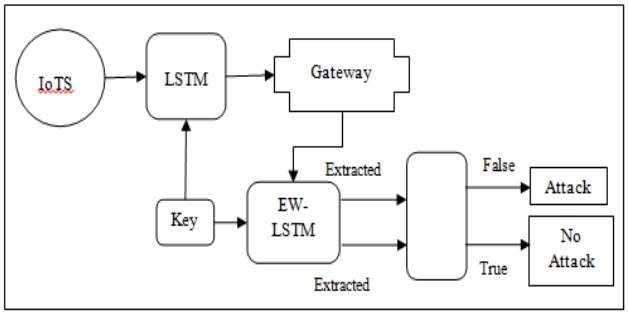

Figure 4. Effective Watermarking for Attack Detection

2.2 Authentication using DRL for Incomplete Information

LSTM blocks are used in a Deep Reinforcement Learning (DRL) method that is suggested to collect the partial information at the gateway. This paper specifies a security framework for a large-scale IoTs scenario with missing data. LSTM blocks are capable of learning complex patterns and relationships within the data. It can identify temporal dependencies and correlations in the partial information received at the gateway. By understanding the context provided by the available data, LSTM blocks enhance the DRL model's ability to make informed decisions, even when some data points are missing.

From IoTSs the signals are received at the gateway by using EW-LSTM blocks and, if DRL activates them through the transmission of a value '1' (trigger signal), validate the signal that was received. When DRL activates the EW-LSTM blocks through the transmission of '1', these blocks analyze the incoming signals using Long Short-Term Memory (LSTM) networks, which are particularly effective for processing sequences of data. If the signals match expected patterns or are within predefined parameters, they are considered valid. If discrepancies or irregularities are detected, the system can take appropriate actions, such as raising alarms or rejecting the signals to prevent unauthorized access or potential security threats. EW-LSTM then transmits to the DRL related IoTS's state. A DL-based EW for IoTS signal authentication learns which IoTSs should be verified in each step on the basis of attacker's priority actions and the computing limitations of the gateway make up the design. Figure 5 depicts the proposed DRL design.

The gateway's reward is roughly estimated using Deep Neural Networks (DNN) at each successive step. A gateway that gets the attacker's action stream from earlier steps, approximating the gateway's reward at each successive step and selects the best course of action uses LSTM in specific.

In order to map one sequence to another and forecast the future using sequences from the past, LSTM blocks are highly helpful. Q-learning algorithm is employed to determine the gateway's action that maximizes its predicted functionality.

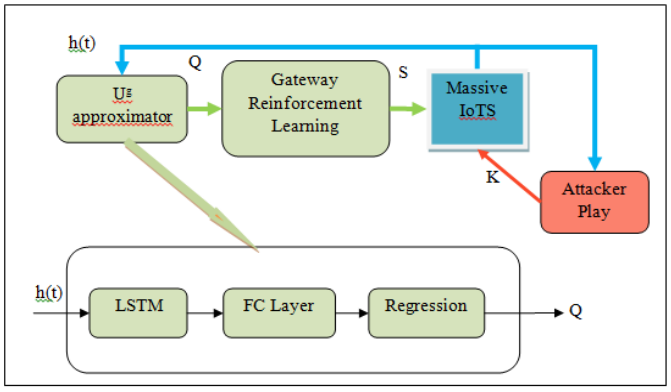

Figure 5. DRL System Architecture

Equation (1) defines the state '*h*' as an N-dimensional adversary action series.

$$, h_i(t) = \left[h_i^1(t), \ldots, h_i^q(t) \right] \quad (1)$$

Every dimension of h, where h^{l}i(t) denotes the attacker's activity on the IoTS i at step t (q l + 1), is a stream from each EW_LSTM at the gateway. Any value between (0, 1, 2); '0' and '1' may be used for this operation, mainly '0' for no attack condition, '1' for under attack condition and '2' denotes non-verification of gateways at that instant. Equation (2) provides the update algorithm for the Q-function, which is utilized to generate the greatest possible action at every single step for the access point.

$$Q_{t+1}(S(t), h(t)) = Q_t(S(t), h(t)) + \alpha \{ Ug(S(t), \delta g(t)) + \gamma_{\max S} Q_{t+1}(S, h(t+1)) - Q_t(S(t), h(t)) \} \quad (2)$$

Where 'γ' is a reduction element and is 'α' a learning rate. Storing numerous values in a database is difficult. In order to learn long-term dependencies within a particular sequence, LSTM blocks that can hold the data for an extended period are

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 54-59 | e-ISSN: 2347-470X

used. DNN is used for approximating the gateway's Q function, and the gateway's best course of action is chosen using this Q function. The DNN learns expected rewards for different behaviors in diverse situations using various input features. Based on this learned Q function approximation, the gateway makes decisions. The DNN's ability to generalize enables adaptation to unobserved states, making it crucial in complex scenarios. Acting as the computational core, DNNs empower the gateway to make optimal judgments. After taking into account the sampling frequency and the resource of the gateway, each player's learning process begins with a random hypothesis. Here learning starts with random hypotheses, influenced by sampling frequency and gateway resources. Sampling frequency dictates data collection frequency, while gateway resources include computational power and storage. Players refine hypotheses based on these factors, enhancing strategies for optimal decision-making. The gateway estimates the condition of the unauthenticated IoTSs at every single step using its belief vector.

At this point a fully connected layer and a regression layer are both given the output of the LSTM block. As with typical neural networks, neurons in a fully linked layer are coupled to every activation in the preceding layer. In DNNs, fully connected layers are used for high-level reasoning. Since the gateway uses an LSTM procedure for predicting an attacker's subsequent actions based on the mutual dependence of the attacker's previous behaviors, even though it lacks complete knowledge of the state of all IoTSs.

Despite this approach might struggle to converge to the algorithm called Mixed-strategy Nash equilibria because it lacks comprehensive data about the state of all IoTSs, since the gateway's algorithm uses an LSTM technique to forecast the attacker's subsequent actions according to the interrelated nature of the attacker's previous behaviors, it is capable of selecting a set of IoTSs at every phase that minimizes the number of impaired IoTSs. As a result, the framework will have an acceptable outcome even with incomplete knowledge.

3. RESULTS AND ANALYSIS

The actual dataset of sampling frequency of fs of 1khz is considered for the simulation. The reliability and latency constraints are achieved in each simulation by using the best values.

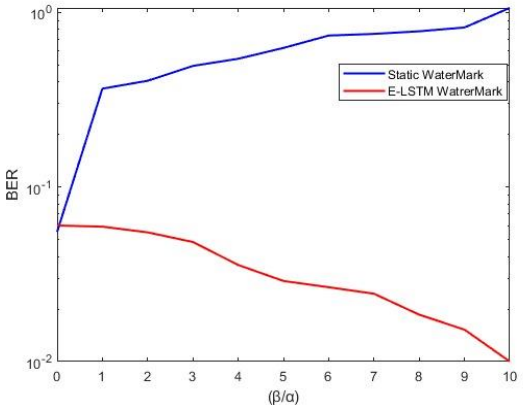

Figure 6. Training Performance

The training's effectiveness is depicted in *figure 6*, where it converges 269 epochs. An epoch in this context is a measurement of how frequently the neural network's weights are updated using all of the training vectors at once. Using the median squared error, the training error is calculated to be 0.0055. Also evaluated on additional accelerometer data, the trained E-LSTM's testing inaccuracy is approximately 0.02 and is suitable for IoT applications.

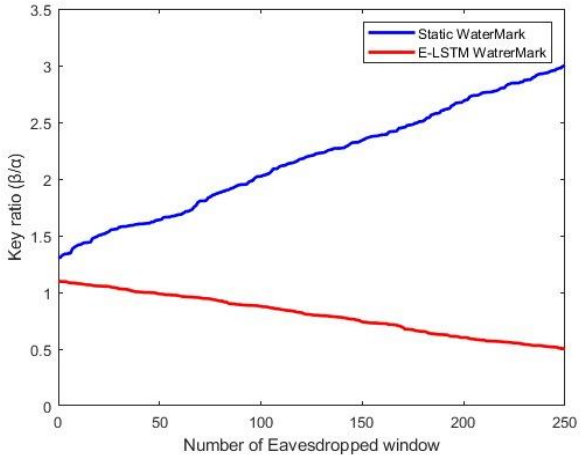

Figure 7. Key vs Signal Power Ratio

Figure 7 demonstrates the way of eavesdropping works against the two watermarking strategies. In conventional static watermarking, the attacker captures the signal, enhances the ratio of the key power to signal power pseudo-noise by adding the recorded data from each window, and then extracts the bit stream. The bit stream in proposed model, representing the watermark, dynamically changes in each window due to LSTM's ability to capture intricate patterns in data sequences. This variability makes it exceptionally challenging for attackers. The summing of the data will not improve, but improves the key power to signal power ratios since in LSTM, the bit stream dynamically varies in each window. The bit stream and key will therefore be impossible for the attacker to derive from the information that was recorded.

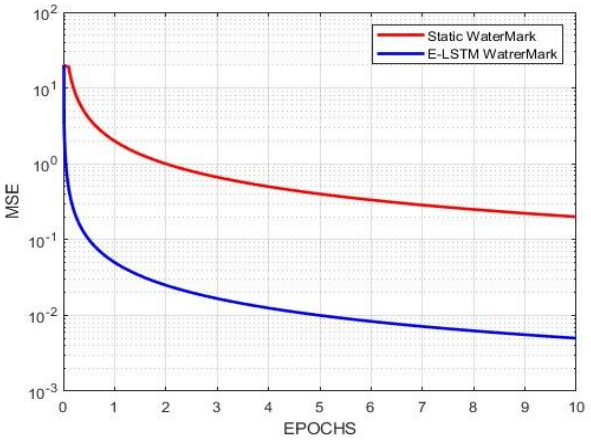

Figure 8. Mean Square Error

Figure 8 demonstrates the Mean Square Error (MSE) through which the LSTM performs better at bit extraction than static watermarking. The relationship between higher / and reduced bit error is widely established. Because of this, when β/σ = 1,

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 54-59 | e-ISSN: 2347-470X

the extraction error rate for LSTM is roughly 1 order factor lower than the conventional static watermarking using deep learning [1], this ratio improves as β/σ increases. As a result, it is possible to create attack detectors with shorter detection delays because the dimension of the window is smaller as well as the initial detection delay is shorter because to the option to select a lower n for the LSTM.

In proposed approach the LSTM's adaptability in generating varied bit streams in different windows enhances the security of watermarking strategies, making it highly resistant to extraction attempts.

Table 1: Comparison results of Static and E-LSTM watermarking

	Existing - Static watermarking [1]	Proposed - E-LSTM watermarking
BER	0.0055	0.02
Key power to Signal Power Ratio	0.6%	2.9%
MSE	0.00251	0.3981

Trained neural network units called LSTM blocks are made to identify long-term dependencies in sequences. LSTMs have special memory cells and gating techniques that avoid the vanishing gradient issue, as compared to conventional RNNs. Because of this, LSTMs can retain knowledge for long epochs, which makes them suitable for applications involving large time delays or complex data patterns.

4. CONCLUSION

For identifying cyber-attacks, an efficient watermarking based on the LSTM algorithm is used for dynamic IoT signal authentication. IoTSs can extract a group of randomly generated characteristics from the produced signal and periodically these features are watermarked into the transmission; this makes proposed watermarking approach efficient. It is built on a LSTM structure for deep learning. The IoT gateway that combines signals from IoTSs may properly test the signal's trustworthiness by employing this technique. In order to handle partial communication scenarios where the gateways are unable to obtain the state of the unauthorized IoTSs, a complex DRL technique is employed for state predictions of unauthenticated IoTSs and allows the gateway to decide which IoTSs to be authorized. The simulation results show that the effectiveness of the proposed EW-LSTM in terms of better compared to conventional method. However, the effectiveness of DRL relies heavily on the availability and quality of training data, which can be a limitation in real-world scenarios. Storing IoT signals in the cloud raises privacy concerns, hence the work can be extended by developing an advanced encryption algorithm.

REFERENCE

[1]. A. Ferdowsi, and W. Saad (2018, May). Deep learning-based dynamic watermarking for secure signal authentication in the Internet of Things. In 2018 IEEE International Conference on Communications, pp. 1-6.
[2]. S. Ali, N. Rajatheva, and W. Saad (2019), Fast uplink grant for machine type communications: Challenges and opportunities. IEEE Communications Magazine, Vol. 57, No. 3, pp. 97-103.
[3]. P. Sethi, and S. R. Sarangi (2017), Internet of things: architectures, protocols, and applications. Journal of Electrical and Computer Engineering, 2017.
[4]. Latvala, S., Sethi, M., & Aura, T. (2020). Evaluation of out-of-band channels for IoT security. SN Computer Science, Vol. 1, pp. 1-17.
[5]. D. U. Ugli Jurayev, (2022), Security in the Internet of Things: A Review. Texas Journal of Engineering and Technology, Vol. 11, pp. 15-17.
[6]. R. Wazirali, R. Ahmad, A. Al-Amayreh, M. Al-Madi, and A. Khalifeh, (2021). Secure watermarking schemes and their approaches in the IoT technology: an overview. Electronics, Vol. 10, No. 14, pp. 1744.
[7]. A. Mukherjee (2015). Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints. Proceedings of the IEEE, Vol. 103, No.10, pp. 1747-1761.
[8]. W. Trappe (2015), The challenges facing physical layer security. IEEE communications magazine, Vol. 53, No. 6, pp. 16-20.
[9]. J. Y. Lee, W. C. Lin, and Y. H. Huang, (2014, May). A lightweight authentication protocol for internet of things. In 2014 International Symposium on Next-Generation Electronics (ISNEI), pp. 1-2.
[10]. P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad (2013). Identity authentication and capability-based access control (iacac) for the internet of things. Journal of Cyber Security and Mobility, Vol. 1, No. 4, pp. 309-348.
[11]. P. Hespanhol, M. Porter, R. Vasudevan, and A. Aswani, A (2017, December). Dynamic watermarking for general LTI systems. In 2017 IEEE 56th Annual Conference on Decision and Control (CDC), pp. 1834-1839.
[12]. M. Hosseini, T. Tanaka, and V. Gupta (2016, June). Designing optimal watermark signal for a stealthy attacker. In 2016 European Control Conference (ECC), pp. 2258-2262. IEEE.
[13]. B. Satchidanandan, and P. R Kumar (2016). Dynamic watermarking: Active defense of networked cyber–physical systems. Proceedings of the IEEE, Vol. 105, No. 2, pp. 219-240.
[14]. M. Porter, P. Hespanhol, A. Aswani, M. Johnson-Roberson, and R. Vasudevan, (2020). Detecting generalized replay attacks via time-varying dynamic watermarking. IEEE Transactions on Automatic Control, Vol. 66, No. 8, pp. 3502-3517.
[15]. C. M. Ahmed, V.R. Palleti and V. K. Mishra, (2022). A practical physical watermarking approach to detect replay attacks in a CPS. Journal of Process Control, Vol. 116, pp. 136-146.
[16]. W. Chen, X. Qiu, T. Cai, H.N. Dai, Z. Zheng and Y. Zhang, (2021). Deep reinforcement learning for Internet of Things: A comprehensive survey. IEEE Communications Surveys & Tutorials, Vol. 23, no. 3, pp. 1659-1692.
[17]. M. A. Jan, F. Khan, S. Mastorakis, M. Adil, A. Akbar and N. Stergiou, (2021). LightIoT: Lightweight and secure communication for energy-efficient IoT in health informatics. IEEE transactions on green communications and networking, vol. 5, no. 3, pp. 1202-1211.