Physical-Layer Detection and Security of Printed Chipless RFID Tag for Internet of Things Applications

Grishma Khadka®, Member, IEEE, Biplob Ray®, Member, IEEE, Nemai Chandra Karmakar, Senior Member, IEEE, and Jinho Choi®, Senior Member, IEEE

Abstract—This article has proposed detection and physical-layer security provision for printed sensory tag systems for Internet of Things (IoT) applications. The printed sensory tags can be a very cost-effective way to speed up the proliferation of the intelligent world of IoT. The printed radio-frequency identification (RFID) of a sensory tag is chipless with the fully printable feature, Nonline-of-Sight (NLoS) reading, low cost, and robustness to the environment. The detection and adoption of security features for such tags in a robust environment are still challenging. This article initially presents a robust technology for detecting tags using both the amplitude and phase information of the frequency signature. After successfully identifying tag IDs, the article presents novel physical-layer security using a deep learning model to prevent the cloning of tags. Our experiment shows that the proposed system can detect and identify the unique physical attributes of the tag and isolate the clone tag from the genuine tag. It is believed that such real-time and precise detection and security features bring this technology closer to commercialization for IoT applications.

Index Terms—Backscatter communication, chipless radio-frequency identification (RFID) system, deep learning, long short-term memory (LSTM), physical security.

I. INTRODUCTION

T he importance of the chipless tag system for low-cost item tagging is growing due to its various important features compared to the chipped tag system and Barcodes. Most of the current research on printed chipless tags are focusing mainly on tag and reader technology developments [1]. However, it is still challenging to detect and protect authentication of a chipless tag within the reader interrogation zone in a cluttered environment.

During the detection, the backscattered interfering signal from static and moving objects along with the interference waves from the nearby radio degrades the quality of the tag signal information [2]. The main difficulties lie in the identification of electromagnetic (EM) response of the chipless tag, which is severely affected by conductivity, permittivity, and permeability of the material [3], where the tag is attached. A low-permittivity item has a high speed of signal propagation [4] in comparison to an item with high permittivity. The high-permittivity items result in a noticeable fading of the microwave signal [5], which affects the performance of the backscattered signal of the tag and would be a source of amplitude variation, bandwidth broadening, and shifting of the resonant frequency. Variations in the amplitude level of the tag response cause the misreading of the tag information. Also, the bandwidth broadening and frequency shifting overlap the resonant frequency with the nearby resonances, affecting the detection of the tag ID [6]. Various tag detection techniques have been developed to overcome the detection issue in the chipless radio-frequency identification (RFID) domain. However, most techniques face limitations to decode the tag signature due to the nonstationary clutters. The interference signal of the nonstationary clutters exists around the interested targets, making it challenging to detect chipless RFID tag data bits.

To ensure reliability and security of the communicated data, the RFID system should adapt secure communication techniques. Due to low computational capabilities, the chipless sensory tags are unable to use the traditional low-cost security techniques to protect itself. Therefore, the chipless sensory tags are vulnerable to wide range of attacks like Denial of Service (DoS), malware injection, power analysis, man-in-the-middle attack, or eavesdropping and replay attacks [7], [8]. There are existing works to counter some of the attacks [7]–[9] but others like cloning attack can be avoided using combinations of physical, data link, and application layers protection. For example, a hardware cloning attack cannot be effectively stopped using security techniques limited to application layers only as it does not affect application layers functionalities but the data link layer registers some changes due to change in the physical layer. Therefore, the physical-layer security is an essential requirements beside detection, to avoid security attacks like cloning or spoofing attacks and to advance chipless RFID tag for the Internet of Things (IoT) application. By protecting them from cloning and counterfeit, the tags can ensure their authenticity. For a more sensitive system with high-security requirements, the tag information, during...
transmission and at rest, needs to be protected from malicious use, such as tempering and reply attack. A malicious adversary may try to control and mislead the entire communication system to an unsafe state [10] by tempering transmitted signals or inserting malicious signals, or introducing a counterfeit tag with malicious code [9] in the system. For example, in supply chain or retail, an unauthorized eavesdropper may attempt to obtain the information of different tagged shopping items, which includes the product ID and price without the concern of the item holders [11, 12]. In the literature, studies focused on the security of the chipped, tagged system with very few attempts to address the need for printed chipless tags IoT system’s security. For a practical security solution of chipless RFID tags, it is essential to consider innovative and lightweight security mechanisms [13] by exploring and leveraging the existing features of the system so that it will be feasible and easily adaptable in the industry. In IoT-enabled retail marketplace, cloning or counterfeit of a tag may lead to various security violations, such as losing ownership of the object, privacy invasion, and counterfeiting of expensive products. Therefore, it is essential to identify and isolate cloned or counterfeit smart objects from original objects immediately to prevent further damage.

This article has looked into designing and developing physical-layer detection and security techniques for identifying clone and counterfeit tagged objects in IoT systems. Others attacks on chipless RFID is out of the scope of this article. Initially, the article proposed a detection technique to detect the chipless RFID tag identifications (IDs), which then used a machine learning model to identify an original, clone or counterfeit tags. More importantly, there is no requirement of a hardware modification to implement the proposed techniques in printed tags-based IoT systems. The contributions of this study are as follows.

1) A novel tag detection technique that avoids false detection in a cluttered environment.
2) A clone or counterfeit tag identification using a machine learning model.
3) Verification and validation of the detection technique and machine learning model.

The organization of this article is as follows. Section II presents the background and related work in the development of physical-layer tag detection and security. The details of the IoT system model is presented in Section III. Sections IV and V present the proposed detection technique followed by the physical security model. Discussion and comparative study are presented in Section VI. Finally, Section VII concludes the study.

II. BACKGROUND AND RELATED WORKS

The remarkable progress in microelectronics and semiconductor technologies have moved the conventional chipped RFID technology into mainstream applications. It is a contactless, Nonline-of-Sight (NLoS) wireless communication technology that uses radio-frequency (RF) waves to read electronics tags from a distance and reduce the human intervention interaction and manual scanning of tagged items [14]. Although, conventional chipped RFID tags have moved into mainstream applications. The design and assembling of the application-specific integrated circuits (ASICs) increase the fabrication cost in an integrated circuit (IC)-based tag. Due to the bulky structure of the tag, the printing of the tag on commercial paper or polymer substrate is impossible. Also, the IC-based tag cannot withstand the cold temperature below zero and a high temperature above 40 °C [15].

The recent development of the sensory tag (chipless RFID tag) opens up new possibilities to tackle these issues [16, 17]. A chipless RFID consists of passive resonators on a single-layer structure [18] without a silicon chip. Each resonator of a chipless tag forms a peak or null in the frequency response of the tag based on its property. The absence of a silicon chip significantly reduces the implementation cost in comparison to the chipped tag. Besides being fully printable, it is a favorable solution to overcome the limitation of chipped tags for next-generation RFID technology. Due to the growing interest in an RFID system, various detection techniques and security model have been proposed for the chipless tags. The following section provides a brief discussion of recent works on detection techniques and security models.

A. Related Works on Detection Technique

In the past various chipless RFID tag detection techniques have been developed to overcome the challenges as mentioned above in Section I. However, most of the techniques face limitations to decode the tag signature due to the variations in the amplitude level and shifting of frequency [6]. For example, short-time Fourier transform (STFT) [19] needs a more extended window width to obtain a good frequency resolution. The optimization between frequency and time causes frequency shift, which results in missing bits for high data capacity tags within limited bandwidth [20]. The wavelet-based technique [6] that uses the mother wavelet and confident band for detection does not meet the nonstationary behavior of the signal and is challenging to adapt for high data capacity tag. The threshold-based detection technique [21] detects the tag signature by comparing the magnitude of tag response against a fixed threshold level, which shows minimal flexibility in tag detection in the presence of noise, clutter, and interference. Likewise, the moving average filtering technique [22], which uses a fixed threshold level, faces a similar challenge. The signal space representation (SSR) technique [23] finds the minimum distance between the received frequency signature points with other fixed points. Moreover, the techniques mentioned above are difficult to implement to analyze the tag information in real IoT applications.

B. Related Works on Physical-Layer Security

Due to the growing interest in the RFID system, various security protocols based on software and hardware have been proposed for the conventional chipped RFID to prevent cloning and counterfeiting of the RFID tags. The work in [24] uses an electronic fingerprint of a tag based on the minimum power response at multiple frequencies. Bu et al. [25] proposed a BASE, DeClone, and DeClone+ protocols suitable for faster
deterministic clone detection for small to large anonymous RFID systems. Zanetti et al. [26] study the cloning detection of passive ultrahigh-frequency (UHF) RFID tags. The literature shows numerous research on physical-layer security for chipped RFID tags, using physical-layer fingerprinting [24], [27] and physically unclonable function [28], [29] to prevent cloning, but are limited and not applicable for chipless RFID tags.

Yang et al. [30] presented the unclonable chipless RFID tag (UCR) and analyzed its system to the potential attacks. Its results show the uniqueness and unclonable identifier of the proposed UCR tags. The article in [31] proposed the authentication of chipless tags by using natural randomness to generate a unique electromagnetic signature in the RF field for authentication during the fabrication process. The main limitation lies during the fabrication process, as the design values of the tag shift with the change in slot parameter. It results in the variation of trace width, air gap, substrate thickness, and material dielectric of each resonator, making it difficult to prevent an attack. The different authentication technique in [32]–[35] has a limitation in terms of 3-D structures, printing, and imaging procedure as discussed in [31].

III. SYSTEM MODEL

The article has used an IoT network model, illustrated in Fig. 1 designed for the detection of smart objects tagged using chipless tags. The network model in Fig. 1 has a master reader with low-power wide-area network (LPWAN). The master reader communicates to the backend system in the cloud using wireless, such as Wi-Fi or wired backhaul communication. As illustrated in Fig. 1, the master reader communicates to client readers to collect information of tagged smart objects. The client reader also stores the client module of our physical-layer security model to identify a clone or counterfeit smart objects.

Using network model presented in Fig. 1, the system model in Fig. 2, smart shop, is designed. The shop has tagged smart objects for sale as presented in Fig. 2. In addition to individual tags to identify smart objects, some of these tags are networked [36] or grouped [37] to represent grouped objects to the system. The smart shop in Fig. 2 has an auto checkout that identifies the customer in the system by reading membership card using IoT enabled master reader. The client reader captures the backscatter chipless RFID tag signal attached to the item. It then processes the signal in real time using the appropriate detection algorithm and sends the product information to the master reader. The client readers are responsible for identifying all the objects placed in the shopping cart during checkout.

As illustrated in Fig. 2, an attacker may use secretly clone/counterfeit an expensive items tag to evade paying the item as the system knows that a specific item or group of items are already sold. It can create various dispute scenarios; for example, the attacker pretends to be the customer’s representative and return the item to get a refund. Furthermore, large-scale tag cloning can also be used to jam the entire system by confusing client readers.

For the practical implementation of the chipless RFID system for smart shopping, we need to consider developing the proper detection technique and security model. Thus, this article presents the detection technique to collect backscatter tag signal information and a security model to identify tag authenticity to increase usability and system performance.

IV. DETECTION TECHNIQUE FOR CHIPLESS RFID TAG

In this section, the article proposed detection steps in detecting tag data bits from a high level of noise and interference [38]. The proposed technique is based on the analysis of both amplitude and phase spectral to separate the tag IDs from environment reflection even the tag radar cross-section (RCS) undergo a change in amplitude variation and frequency shifting. The different steps of the proposed technique are explained as follows.

A. Reader Setting and Background Subtraction

Initially, the reader [39] was configured for reading the tag placed in front of it. The tag was illuminated with the reader operating within the frequency range of 3.3–10 GHz by transmitting the radio signal at different frequencies to the passive
The chipless tag using its array of antenna elements [39]. The transmitted signal excites the resonant elements encoded within the chipless tag and starts resonating within their predefined frequency. The exciting signal is reradiated as a backscattered signal to the reader. This signal consists of both the desired tag signature as well as unwanted signal components in the form of interference and noise [40]. The received signal by the reader is defined by

\[ r(t) = \sum_{m=1}^{M} A_{m} \cos \left( 2\pi f_{m}(t - \tau) + \frac{k(t - \tau)^{2}}{2} + \phi_{m} \right) + n(t) \]  

(1)

where \( m \) is the number of the reflected signal from the tag RCS and echoes from static and moving objects. \( A_{m}, \phi, \) and \( \tau \) are the amplitude, phase, and time delay of the reflected signal, and \( k, n(t) \) are the slopes of the frequency-domain signal and the additive white Gaussian random noise. The round trip time \( t_{1} \) is the time excitation signal travels from the transmitting antenna to the stationary chipless tag plus the time backscattered signal travels from the chipless tag to the receiving antenna, \( t_{1} \) is denoted as

\[ t_{1} = 2r/c \]  

(2)

where \( r \) is the distance between the chipless RFID tag and the ultrawideband (UWB) reader, and \( c \) is the speed of the light. The received signal consists of the tag signal and interfering signals, such as cable loss, the coupling between the antennas, free-space path loss, and echoes from static and moving objects. The background measurement, which is the transmission coefficient between the transmitting and receiving antennas without the presence of a tag, also called as empty-room response [41] is performed to remove the effect of the static noise from the environment. Therefore, to eliminate the static interference components, the measured complex RCS of the tag is subtracted from the measured background response without the presence of a tag and divided by the known RCS of the reference object. The calibrated measured tag RCS of the frequency coded tag is given by [42]

\[ \sigma_{\text{tag}} = \frac{\left( S_{21}^{\text{tag}} - S_{21}^{\text{BG}} \right)^{2}}{S_{21}^{\text{Ref}} - S_{21}^{\text{BG}}} \times \sigma_{\text{Ref}} \]  

(3)

where \( S_{21}^{\text{tag}} \) is the measured RCS of the tag, \( S_{21}^{\text{Ref}} \) is the known RCS of the reference object, \( S_{21}^{\text{BG}} \) is the measured background response without the presence of the tag, and \( \sigma_{\text{Ref}} \) is the RCS of the reference object. After background subtraction, the second step is to find the power level and selection of antenna pair. The detail is explained in the next section.

\[ P_{r}[\text{dB}] = P_{t}[\text{dB}] + G_{t}[\text{dB}] + G_{r}[\text{dB}] + 10\log_{10} \frac{\sigma}{4\pi} - 20\log_{10} \frac{4\pi}{\lambda} - 40\log_{10} r \]  

(4)

where \( P_{t} \) is the transmitter output power level, \( G_{t} \) is the gain of the transmitting antenna, \( G_{r} \) is the gain of the receiving antenna, and \( \sigma \) is the tag RCS. For a chipless RFID tag, the theoretical RCS (\( \sigma_{\text{chipless tag}} \)) at the resonant frequency is calculated by

\[ \sigma_{\text{chipless tag}} = \frac{\lambda^{2} \text{Gain}_{\text{tag}}^{2}}{2\pi} \]  

(5)

where \( \text{Gain}_{\text{tag}}^{2} \) is the tag antenna gain, and \( \lambda \) is the operating wavelength. By substituting (5) into (4), we get

\[ P_{r}[\text{dB}] = P_{t}[\text{dB}] + G_{t}[\text{dB}] + G_{r}[\text{dB}] + 10\log_{10} \frac{\lambda^{2}}{4\pi} \]  

\[ + 10\log_{10} \frac{\lambda^{2}}{4\pi} - 20\log_{10} \frac{\lambda}{4\pi} - 40\log_{10} r. \]  

(6)

Equation (6) shows the power received when the tag is within the interrogation zone of the reader antenna. Similarly, the theoretical reflected power analysis is performed in [43] for multiple transmitting and receiving antennas of the UWB reader.

This article used a reader [39] which consists of \( N_{T_{x}} = 4 \) transmitting and \( N_{R_{x}} = 14 \) receiving antenna elements. Each of the transmitter, out of four, operates sequentially within the frequency range from 3.3 to 10 GHz band. If \( i \) and \( j \) represents the transmitter and receiver index, then the measurement vector at \( k \) cycle index for \( N \) number of sample per measurement is given by

\[ f_{k,i,j} = [f_{k,i,j}(0)f_{k,i,j}(1)f_{k,i,j}(2)\cdots f_{k,i,j}(N-1)]. \]  

(7)

Using (7), we can form the data matrix of size \( 56 \times N \) as given by

\[ S_{k} = [f_{k,1,1};f_{k,1,2};f_{k,1,3};\cdots f_{k,4,12};f_{k,4,13};f_{k,4,14}]. \]  

(8)

However, in this research, a few antenna pairs are selected by setting the elevation angle \( \theta \) from \(-60^\circ\) to \(60^\circ\) and azimuths angle \( \varphi \) from \(-60^\circ\) to \(60^\circ\) as the scanned area. It helps to increase the reading speed and avoids the computation complexity of the system while detecting the backscattered tag signal.

C. Detection of Tag IDs

After selecting the antenna pairs, the communication is established between the reader and the tag to extract the backscattered raw signal information. The raw information consists of both signal magnitude and phase. The signal magnitude has a high dependency on environmental reflection, orientation, and geometry of the surface, where the tag is attached, resulting in difficulty finding the peak at particular resonance frequency points. Similarly, the phase of the signal depends on the propagation channel and modulating properties of the tag. Thus, to increase the reliability of the detection technique, instead of using only amplitude or phase information, we performed analysis of amplitude and phase information of the received signal separately to validate the optimum detection efficiency of the tag data. In the frequency domain, the transfer function response \( H(f) \) of the chipless tag amplitude \( A \)
and phase $\phi$ for $M$ number of resonators resonating at different frequencies is defined [44] as

$$A(f) = \prod_{m=1}^{M} |H_n(f)|$$

(9)

and

$$\phi(f) = \sum_{m=1}^{M} \angle H_n(f).$$

(10)

The validation of the detection technique with the experiment is discussed in Section IV-D.

D. Performance Analysis of the Detection Technique

In this section, we analyze the detection of the chipless RFID tag ID in a real environment. For the experiment, as shown in Fig. 3, orientation-insensitive circular patch resonators tags and an UWB reader are selected. The encoding of the tag data is based on the resonant elements [45] resonating at different frequency points. The presence of a peak resembles logic “1,” whereas its absence resembles logic “0” for frequency-domain-based chipless tags. The reader used in the experiment operates over a frequency range of 3.3–10 GHz with a predefined number of antenna pairs for reading the raw signal information of the chipless tag. Multiple reading is recorded to calculate the detection throughput rate of the proposed technique. The throughput is defined as

$$\text{Throughput} = \frac{N_{s-r}}{N_{t-r}}$$

(11)

where $N_{s-r}$ is the number of successful readings of the tag and $N_{t-r}$ is the total number of readings during each measurement.

Fig. 4 shows the 4-bit tag backscatter signal response when placed within the reader interrogation zone. The response in Fig. 4(a) and (b) shows the distinct peaks, which frequently occur at particular frequency points in both amplitude and phase response. Similarly, Fig. 4(c) and (d) shows a more clear response in normalized amplitude and phase response which justify the detection of tag IDs information. The individual analysis of tag response in multiple readings demonstrates the throughput of 99% for a chipless RFID tag.

The experiment is further extended when the tag is attached to items with different permittivity and conductivity. The EM response of the items with different permittivity can be stronger and much bigger than the tag response, which affects the backscatter tag signal [47]. To mitigate this problem and validate our proposed technique’s effectiveness, we select a 4-bit one-quarter ring chipless tag with good co-polar and cross-polar response. Fig. 5 shows the tag response when attached to low and highly scattering items (high-permittivity item) and items with a metallic structure with higher conductivity. For our analysis, we select a corn flakes box, an item with low permittivity with a high signal propagation speed. Similarly, a coke can is selected with a metallic structure with higher conductivity and a stronger backscatter signal with a high amplitude response than the tag response. In addition, a water bottle full of water is chosen as a higher permittivity item. Fig. 5(a) and (b) shows the amplitude and phase response along with normalized amplitude and phase response in Fig. 5(c) and (d). The overall results show that the detection technique can reduce the interfering signals when the chipless tag attached to different smart items. The proposed algorithm easily compensate the loss of information in amplitude response by phase response or vice-versa.
TABLE I

| Ref.  | Detection Technique | Number of bits | Tag attached to | Reading accuracy | Computational complexity | Reader, cost and processing |
|-------|---------------------|---------------|----------------|-----------------|-------------------------|-----------------------------|
| [21]  | Threshold           | 4-bit         | N/A            | 90%             | Low                     | VNA, expensive, PP          |
| [6]   | Wavelet             | 4-bit         | N/A            | 90%             | Medium                  | VNA, expensive, PP          |
| [23]  | SSR                 | 3-bit         | N/A            | 90-95%          | High                    | VNA, expensive, PP          |
| [47]  | ML                  | 4-bit         | N/A            | 90.99%          | High                    | VNA, expensive, PP          |
| This Paper | Proposed Technique | 4-bit | highly scattering items | 99% | Low | Walabot, <500 USD, RTP |

PP: Post Processing (processing after data captured from VNA); RTP: Real Time Processing of chipless RFID tag data

The comparisons of the result using the proposed technique with the existing techniques are shown in Table I. From Table I, we observed that the existing techniques, such as the maximum likelihood (ML) and SSR technique need higher computation capacity with increased computation time in comparison to the proposed technique. The proposed technique is computationally feasible and show a better reading performance with computation time of 35 ms. The previous reported works perform the postprocessing (PP) of data after reading the tag response from the vector network analyzer (VNA). The PP of tag signal by the use of expensive device such as VNA is replaced by using the low cost UWB reader for real-time processing (RTP) in practical application. Furthermore, our technique shows reliable detection of tag signatures even when the tag is attached to highly scattering objects, whereas the analysis of previous techniques with the tagged item is not available in the literature. The proposed technique meets the goal in developing a low-cost intelligent system model demonstrated in Fig. 2.

V. PHYSICAL SECURITY MODEL

This section details the attack model of chipless tags that underpin our proposed physical security model.

A. Attack Model

Fig. 6 illustrates a clone attack using one client reader over a communication link of a chipless RFID system of the smart shop model in Fig. 2.

The attacker has physically cloned tag $T_2$ as tag $T_c^2$ and presented it closer to the client reader $R_1$ for a stronger signal to pose as a genuine owner of the smart object associated with the $T_2$. Current readers will read the cloned tag $T_c^2$ as a real tag if the cloned tag has a stronger signal or closer to the reader itself [7]. A client reader must be able to identify genuine and clone tag before passing the signal to the backend via the master reader as the clone tag may insert a malicious signal to compromise the security of the entire smart shop system [9], [36]. For bulk or expensive objects, the smart shop needs assurance of nonrepudiation, which may play a key role in dispute resolution [8].

The preliminary analysis of the attack model is performed based on two physically different tags with the same number of bits. The hypothesis of this experiment is to observe the tag signature when the attacker tries to clone the tag to produce the duplicate tag physically. Two tags with similar binary logic bits 1111 but physically different tags represented by $T_2$ and $T_c^2$ are selected for the experiment. The third tag has binary logic bits 1101, which is represented as $T_1$ as illustrated in Fig. 6.

We have recorded physical-layer signal characteristics: amplitude and phase, from 4 to 6 GHz frequency range during the execution of novel detection technique developed and discussed in Section IV for the attack model illustrated in Fig. 6. Our analysis of the physical layer is illustrated in 2-D and 3-D planes in Figs. 7 and 8, respectively, where we choose amplitude response of the backscatter signal for further analysis due to its challenging behavior in detecting tag IDs as discussed in [6].

Fig. 7 has plotted amplitude of three different 4-bit tag responses against the 4–6 GHz frequency range. It is clear from Fig. 7, each tag has its unique feature set from 4 to 4.4 GHz frequency range and from 5.6 to 6 GHz frequency range but amplitudes of $T_2$ and $T_c^2$ are traveling closely compare to $T_1$. However, during the transmission of tag’s ID in 4.6–5.5 GHz frequency range, $T_2$ and $T_c^2$ have significantly distinguished patterns from separating them from each other. In Fig. 8, we have plotted the amplitude of the tags in a 3-D
plain against frequency and time to see the state of distinguished patterns over time to identify clone tags. As we can see from the illustration in Fig. 8, the variation in the amplitude level and the shifting of frequency positions over time shows the existence of distinguished patterns of clone tags $T_{c}$. From the security perspective, the results show some initial efforts in identifying the falsified tag based on the contextual changes of the tag reading distance, object it attached, and duration of its existence in the system.

A well-planned cloning attack by a group of organized attacked may make the master reader busy using many false interrogations while fooling the client readers for financial gain. Therefore, in this article, we have proposed a physical-layer security model which is lightweight to be resident in the client reader to identify a clone or counterfeit tag in real time. The model also aims to eliminate the possibility of DoS, signal jamming, and malware injection using cloned/counterfeit tags.

B. Physical Security Model Using Deep Learning

1) Methodology: In this study, we adopt the long short-term memory (LSTM) deep learning technique, a specific type of recurrent neural network (RNN) which was initially designed to capture long-term dependencies [48], [49]. It is widely used in different emerging applications of RF sensing due to its capability to maintain information in memory for longer periods and outperforms RNN for long dependencies [50]. It solves the problem of vanishing and exploding gradient problems by introducing the gates to control the flow of data [49].

There are four control gates in LSTM: 1) forget ($f$); 2) cell candidate ($g$); 3) input ($i$); and 4) output ($o$). Fig. 9 depicts the general architecture of LSTM blocks [51]. The working mechanisms of each control gates are mathematically expressed as in (12)–(15) in each time stamp $t$

$$i_t = \rho_g(W_i I_t + R_i O_{t-1} + b_i)$$
$$f_t = \rho_g(W_f I_t + R_f O_{t-1} + b_f)$$
$$g_t = \rho_g(W_g I_t + R_g O_{t-1} + b_g)$$
$$O_t = \rho_g(W_o I_t + R_o O_{t-1} + b_o)$$

where $\rho_g$ denotes the gate activation function. $W, R,$ and $b$ are the learnable (adaptable) input weight, the recurrent weights, and the bias. It formed the matrices which are concatenations of the input weights, the recurrent weights, and the bias of each component, respectively. Based on the loss functions, these learnable weights are updated at each time step.

The cell $c_t$ and hidden state $h_t$ at timestamp $t$ are expressed by

$$c_t = f_t \odot c_{t-1} + i_t \odot g_t$$
$$h_t = O_t \odot \rho_c(c_t)$$

where $\odot$ denotes the elementwise multiplication of vectors and $\rho_c$ denotes the activation function. However, in MATLAB software, the lstmLayer function uses the hyperbolic tangent function $\tanh$ to compute the state activation function.

2) Modeling Approach: For this analysis, a sequence of amplitude and phase information of individual time steps is fed into the LSTM network, obtained at different frequency points. To feed the LSTM network-based machine learning model, the Gaussian copula-based framework has been used to generate synthetic data, where the model is developed that contains all the possible dependencies in a multivariate Gaussian distribution. The data generated using the Gaussian copula-based framework are statistically similar to the source data with dependence across variables. The model is trained within
the frequency range between 4 and 6 GHz, based on the available chipless RFID tag discussed in Section III. The input data set contains the tag information at every frequency interval of 0.025, corresponding to 81 input features within the 2-GHz frequency range. Equation (18) represents the total data collection time $t_T$ with 81 input feature $I_f$, and two output class $O_{\text{class}}$ for real (1) and clone (0) tags

$$ I_f | O_{\text{class}} = \begin{bmatrix} I_{f_1} \\ I_{f_2} \\ \vdots \\ I_{f_{81}} \end{bmatrix} \begin{bmatrix} O_1 \\ O_0 \end{bmatrix} $$  \tag{18}$$

The LSTM network architecture, which is fed with real and clone tag information with 81 input features and two output classes, is defined using one Bidirectional LSTM layer with 100 hidden units to learn the full sequence at each time step. The LSTM network is designed with MiniBatchSize 27 using the “adam” optimizer algorithm to classify the network either clone or real tag, $O_{\text{class}}$ output. The training and test data sets are sorted by sequence length by specifying the sequence length to be the “longest” and minibatch size to 27. The configuration model [51] of the LSTM framework is shown in Fig. 10.

3) Results: This section provides a comparative analysis based on the accuracy and loss of the LSTM classification model to identify the real and clone tag. For analysis, the real and clone tag data sets were obtained under two different scenarios: 1) backscatter tag signal obtained after adding additive interference’s and 2) the backscatter tag signal without additive interference in a real time environment. Thus, obtained data sets are splits into training and testing groups. 70% of the data set are within the training group to optimize the model, and the rest 30% data set from the whole sequence is used for testing. The performance accuracy of the LSTM model with and without additive interference is shown in Figs. 11 and 12, respectively. It shows a higher accuracy of 92.33% with interference and 95.5% without interference for classifying the real and clone tags. Similarly, the model loss of 0.242 is obtained with interference and 0.1512 without interference, which is shown in Figs. 13 and 14. Results showed high accuracy in classifying clone tags from the actual legitimate RFID tag.

VI. DISCUSSION AND COMPARATIVE STUDY

Table II presents four performance parameters with three-fold cross-validation for the proposed model detailed in Section V-B. The three cross-validation in Table II is done for two data sets by varying training and testing ratios.
For accuracy, the standard deviation value between cross validation results is $\sigma = \pm 0.00140119$ using data set without interference whereas $\sigma = \pm 0.001634$ with interference. Therefore, the cross-validation variation is minimal in our model between two data sets, with interference and without interference, and the accuracy standard deviation is $\sigma = \pm 0.018323$, which is low but higher than the variation within the data set.

The other three performance parameters: 1) room mean square error (RMSE); 2) normalized RMSE (nRMSE); and 3) mean absolute percent error (MAPE), show similar variation trend of cross-validation result in Table II. While RMSE and nRMSE show errors on the model, the MAPE is a widely used index to determine the forecast accuracy with respect of scale independency and interpretability. Based on the MAPE value in Table II, we can say the proposed model has a slight error and high scale independency and interpretability to detect clone tags in our system model. As the accuracy of the proposed model is higher, the RMSE, nRMSE, and MAPE parameters of the traditional (statistical and machine learning) algorithms become irrelevant and unnecessary to compare with our proposed model.

VII. CONCLUSION

This article demonstrated a novel approach to collect backscatter data from a low-cost passive chipless RFID tag. It introduced a novel detection technique to identify the tag IDs and a deep learning model to capture clone or counterfeit tags in commercial applications. Initially, the performance analysis and validation of the proposed detection technique were investigated by measuring the response from the chipless RFID tag placed within a handheld reader. The proposed method showed a throughput of 99%, a positive and convincing outcome which indicates that the proposed technique can be a low-cost solution to address the detection issues. The article also presented a physical-layer security model to develop a systematic and cost-effective approach for different IoT applications, such as retail and supply chain management. Using a deep learning-based security model provides a high accuracy above 93%, isolating the clone tag from the legitimate RFID tag even in the presence of additive interference in real time.

The outcomes of this research open up new possibilities in developing coordinated backscatter communication techniques for cost-effective IoT connectivity using multiple chipless RFID tags and readers. In the future, we intend to develop a novel approach of the detection and security model for a large number of chipless tags and mobile readers to support future IoT applications.

REFERENCES

[1] C. Herrojo, F. Paredes, J. Mata-Contreras, and F. Martín, “Chipless-RFID: A review and recent developments,” Sensors, vol. 19, no. 15, p. 3385, 2019.
[2] M. Forouzandeh and N. Karmakar, “Self-interference cancelation in frequency-domain chipless RFID readers,” IEEE Trans. Microw. Theory Techn., vol. 67, no. 5, pp. 1994–2009, May 2019.
[3] S. Shrestha and N. C. Karmakar, “Analysis of real-world implementation challenges of chipless RFID tag,” IET Microw. Antennas Propag., vol. 13, no. 9, pp. 1318–1324, 2019.
[4] M. T. Sebastian, Dielectric Materials for Wireless Communication. London, U.K.: Elsevier, 2010.
Grishma Khadka (Member, IEEE) received the Ph.D. degree in electrical and computer system engineering from Monash University, Clayton, VIC, Australia, in 2020, and the M.Sc. degree in information and communication from Chosun University, Gwangju, South Korea, in 2014. He is currently working as an Associate Research Fellow in the field of Intelligent Backscatter Communication with Deakin University, Burwood, VIC, Australia. From 2015 to 2016, he was a Research Engineer with Pusan National University, Busan, South Korea. His significant research contributions are in the areas of RFID system, backscatter communication, digital signal processing, error correction, and machine learning.

Biplob Ray (Member, IEEE) received the Ph.D. degree from the Deakin University, Geelong, VIC, Australia, in 2015. He is currently working as a Senior Lecturer with CQ University, Melbourne, VIC, Australia, with a background mix of research, academic, and industry experience. He is highly interested in multidisciplinary research with core interests in secure communication protocols of cyber-physical systems, Artificial Intelligence (AI), and Internet of Things. He has been working with several Australian federal government and industry-funded research projects since 2016. He has more than 47 book chapter, journal, and conference publications, which have been recognized by peers and cited extensively.

Dr. Ray received the Deans’ Award and Vice-Chancellor’s Award for Outstanding Researchers Commendation in 2019. He has received the CQU Vice-Chancellor’s Award for Exemplary Practice in Learning & Teaching and the Student Voice Commendation in 2019 and 2021. He has served as the guest editor, editorial board member, and reviewer in reputable journals. He has also served as a keynote/plenary speaker, organizing chair, PC member, and reviewer for several conferences since 2012.

Nemai Chandra Karmakar (Senior Member, IEEE) received the M.Sc. degree in electrical engineering from the University of Saskatchewan, Saskatoon, SK, Canada, in 1991, and the Ph.D. degree from the University of Queensland, Brisbane, QLD, Australia, in 1999. He is currently an Associate Professor with the Department of Electrical and Computer Systems Engineering, Monash University, Melbourne, VIC, Australia. He has authored or coauthored over 220 refereed journal and conference papers, 24 book chapters, and eight books. He holds nine international patent applications on chipless RFID. He has over 20 years of teaching, design, and development experience in antennas, microwave active and passive circuits, and RFIDs in Canada, Australia, and Singapore.

Jinho Choi (Senior Member, IEEE) was born in Seoul, South Korea. He received the B.E. (magna cum laude) degree in electronics engineering from Sogang University, Seoul, in 1989, and the M.S.E. and Ph.D. degrees in electrical engineering from Korea Advanced Institute of Science and Technology, Daejeon, South Korea, in 1991 and 1994, respectively. He is with the School of Information Technology, Deakin University, Burwood, VIC, Australia, as a Professor. Prior to joining Deakin University in 2018, he was a Professor/Chair in Wireless with Swansea University, Swansea, U.K., and as a Professor with Gwangju Institute of Science and Technology, Gwangju, South Korea. He authored two books published by Cambridge University Press in 2006 and 2010. His research interests include the Internet of Things, wireless communications, and statistical signal processing.

Dr. Choi received a number of best paper awards, including the 1999 Best Paper Award for Signal Processing from EURASIP. He is on the list of World’s Top 2% Scientists by Stanford University in 2020 and 2021. He is currently an Editor of IEEE WIRELESS COMMUNICATIONS LETTERS and a Division Editor of the Journal of Communications and Networks. He has also served as an Associate Editor or an Editor of other journals, including IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE COMMUNICATIONS LETTERS, Journal of Communications and Networks, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and ETRI Journal.