International Journal of Safety and Security Engineering
Vol. 14, No. 2, April, 2024, pp. 447-457
Journal homepage: http://iieta.org/journals/ijsse

RFID Clone Detection in Supply Chain Using Modified Count-Min and BASE Protocol

Mustamin Bin Mustaffa, Manmeet Mahinderjit Singh*, Kalaivani Selvaraj

School of Computer Science, Universiti Sains Malaysia, Gelugor 11800, Malaysia

Corresponding Author Email: manmeet@usm.my

https://doi.org/10.18280/ijsse.140212

Received: 29 December 2023
Revised: 6 February 2024
Accepted: 15 February 2024
Available online: 26 April 2024

Keywords:
counterfeiting, Count-Min, BASE, distance-bounding, manufacturing, antenna ID, Industry 4.0, low-costs

ABSTRACT

Radio Frequency Identification (RFID) clone in supply chain system causes money, and reputation loss. Existing algorithm detects the clone in RFID tag, never detect clone based on the distance between reader and tag. Modified BASE (MB) protocol is modified version of Binary Search (BASE) protocol. Modification in MB is performed based on logical operations and calculations, identify duplicate tags and duplicate reading. Modified Count-Min (MCM) protocol enhances clone detection by empowering reader device and recognizes cloned RFID tags using a local database, ensures tag-based verification in local and online data. Integration of this local database aids in clone detection and streamlines computational complexity through effective encryption and decryption processes, strengthens security and reliability of supply chain. In this paper, RFID clone detection technique using MB and MCM methods solve the problem of countering distance-fraud attacks after ensuring proximity between tag and reader, ensures security in wireless authentication. Proposed MB and MCM authentication protocol avoid cloning through data comparison in embedded based SQL database in reader. From experimental analysis, proposed methods detect clone in supply chain system with 0.2 seconds, detection accuracy is 90% for MCM and MB of 92%. The computation time of MCM is 0.5sec, 7sec for existing algorithm.

1. INTRODUCTION

Industry 4.0 integrates the Internet of Things (IoT), cyber-physical objects (CPS), and Internet of Services (IoS) in industries [1]. The RFID and IoT are integrated such as passive RFID-IOT tags and active RFID-IOT tags, allows objects to wirelessly communicate automatically in cloud environment, transforms manufacturing process applications such as expanding business scale, low-cost, high-security solutions. RFID technology associates all assets through wireless identification [1]. In RFID-IoT model primarily focuses on RFID, data storage and processing. Radio Frequency Identification (RFID) uses spatial coupling of radiofrequency signals [2]. There are two types of RFID tags under UHF and UW, which are Passive tags and Active tags. Active RFID tags require a power source for high-volume storage, while passive tags needs low storage and performs with high complex computations [1]. EPCglobal Class 1 Generation 2 is known as ISO 18000-6C, which is a key RFID technology used in different applications such as target tracking, automatic payment, indoor positioning, access control, and supply chain management [3, 4]. The RFID tag usage increases due to low power embedded system and less cost. However, cloning of tag is the major challenge in RFID usage in SCM. However, low-cost passive tags lacks to support advanced cryptographic schemes, makes the reader and the tags vulnerable to cyber-attacks [2].

In supply chain management (SCM), Internet of Things (IoT), cyber-physical objects (CPS), Internet of Services (IoS) and Radio Frequency Identification (RFID) plays a vital role in smart job-shop in manufacturing units, links the process flow data and physical asset identification [1]. RFID is used for spatial coupling and achieves automatic identification. RFID is less error-prone, when compared to optical barcodes identification system. RFID enhances the administration and planning in supply chain management. However, low-cost passive RFID tags are prone to attacks [2]. RFID is used for higher accuracy in identification.

RFID technology is used in SCM for ensuring the tracking and tracing of products in manufacturing unit for high accuracy. RFID tags used in SCM are in different frequencies such as 13.56 MHz and 860-960 MHz. Moreover, there are certain issues in the usage of RFID tags in SCM, such as insecure communication channels, different network architectures are used for tag communication and manufacturers unable to use standard protocol, which cause diffident issues such as reader collision and anti-collision, and frequent attacks are happening in tags and readers are [5, 6]. Among the above issues, RFID clones are common in SCM.

In SCM, cloning attacks in RFID tags lead to counterfeit products. RFID cloning attack is performed though copying the Electronic Product Code (EPC) details from the original tag to clone tag. The cloning attack potentially replaces genuine tags fixed on products. Clone attack in RFID is performed in different methods sniffing, and eavesdropping [2]. In pharmaceutical supply chain, RFID reduces counterfeit products/drugs [3]. Manufacturers in united states of America suffer huge loss due to counterfeit products [7].

RFID clone detection is performed using different protocol such as SecAuth [8], EPC Gen2 protocol, Ultralightweight RFID Authentication Protocol with Permutation (UAPP) and Improved Three-Pass Mutual Authentication (ITMAP) [3]. SecAuth protocol is hash-based security identity for prevention from counterfeit attacks and provides accurate authentication. EPC Gen2 protocal is a lightweight technique which reduce the burden on tags, readers, and databases and detects counterfeit tags with more efficient, with less resource-constraint RFID tags [2]. UAPP protocal consists of unbalanced OR and AND operations and resist all possible attacks.

However, desynchronization attacks breaks the UAPP protocol. Hence, the Improved Three-Pass Mutual Authentication (ITMAP) [9] is developed for prevention of RFID attacks. Additionally, ITMAP protocol uses secure controls, such as mutual authentication and asymmetric encryption, which are known standard practices in cybersecurity. Extended Tiny Encryption Algorithm (XTEA) Mutual Authentication Protocol [10] uses encryption and mitigates the brute-force decryption through the number of rounds, which is harder to decrypt the data. Still, problem of detcting clone tag is a challenge in the SCM environment.

1.1 Problem statement

BASE protocol protects data, with certain limitations such as (i) Complexity and Overhead (ii) User Experience Impact (iii) False Positives and Negatives (iv) Complacency and Overreliance (v) Interoperability Issues. Moreover, Count-Min protocol affect user experience such as Complexity, Security Perception, Usability and Aesthetics and False Positives and Negatives. The inaccuracies affect user experience and trust in the security measures. The limitations in detection of cloned RFID are the Complexity and Overhead: where clone detection in RFID systems needs high computational overhead and complexity, impacts the practicality and scalability. In Usability and Execution Time, Fast clone tag identification protocols for large-scale RFID systems require high storage space and increases execution time, impacts the overall usability of the systems.

High Detection Accuracy methods never suits for varying RFID tag cloning ratios. Moreover, Reader and Tag Independence which limits their applicability to a wide range of RFID systems. Security Vulnerabilities to various attacks, such as replay attacks, tracking attacks, and impersonation need to be addressed. To mitigate the above problem, need a user-friendly and intuitive cybersecurity protocols.

Traditional distance bounding protocols are used for RFID clone detection. Protocol detects the clone based on of round trip times taken by 1-bit messages between prover and verifier [11]. The distance bounding protocol detects the relay attacks, countering distance-fraud attacks with low computational speed and high usage of memory with high time complexity. Traditional distance bounding protocols needs high execution time [12, 13].

1.2 Contributions

In this paper, distance bounding protocols such as BASE and Count-Min are modified. BASE and Count-Minnare Distance Bounding Protocols are modification and improved the performance of RFID cloned tags detection with adding techniques for high accuracy. The limitations of traditional method need to be effective for clone detection in RFID systems, thereby enhancing the security and usability of RFID applications.

(i) To propose Modified BASE (MB) protocol, logical operations and calculations are altered in the modified version of BASE protocol i.e., compares the number of EPC with the number of RFID tags based on scan iteration, detects duplicate tags.

(ii) To propose Modified Count-Min (MCM) protocol, where the RFID cloned tags are detected at the reader device, since reader device has a local database. The local database in reader prevents the detection clone tags based on the comparison of EPC numbers of tags from cloud dataset and reduces computational complexity based on encryption and decryption.

(iii) To achieve high accuracy with minor inconsistencies based on Confusion Matrix calculation using the Modified BASE and Modified Count-Min protocol.

The outline of the paper is as follows. In section 2, related work of RFID anti-counterfeit techniques has been discussed where BASE and Count-Min method was chosen as the foundation of this paper, section 3, focuses on methodology and discussed along with approaches, in section 4 implementation of RFID Clone Detection using MB and MCM are elaborated, in section 5 Experiment and results are discussed, in section 6 Conclusion is highlighted.

2. RELATED WORK

RFID tag consists of an Integrated Circuits (IC) and antenna, sending information to readers via wireless probes. RFID works in low cost and efficient devices. Due to low cost RFID applied in stock management, aircraft maintenance, baggage handling, security, and healthcare [14-17]. RFID is applied in supply chain management for efficient management and operation. Still tags are prone to cloning attacks in SCM due to more no of tags are used in different operations [3].

2.1 Comparison of existing protocol in tag clone detection

These cloning attacks are prevented through the traditional attacks as shown in Table 1.

Table 1. Comparison between distance bounding protocols

Traditional Protocols	Drawbacks
GREAT [3]	✓ Very high execution time to detect all RFID cloned tags.
DeClone [3]	✓ Can detect but couldn't distinguish a clone or genuine tag.
BASE [3]	✓ Higher execution time to detect clone tags with a higher number of tags.
Count-Min sketch [3]	✓ The computation is quite complex to detect and clone tags and genuine tags positioned on at least two different readers.
Shortest path algorithm [2]	✓ Fail when working in high-density tags area and prone to provide false positive.

Weis has developed the authentication using cryptography, followed by Ohkubo's one-way authentication and Dimitriou's with mutual authentication. Burmester developed the O-TRAP mechanism, which uses pseudorandom number generator, hash function, and keys for RFID tag clone detection. O-TRAP uses matrices for exponential security, recommended size of matrix is lacked [18].

Tree-based anti-collision protocol uses a unique pseudonym for authentication, unable to distinguish RFID cloned and genuine tags [5].

2.2 Prevention of RFID tag clone using PUF

In RFID cloning attack, copy the information from a genuine tag to a cloned one, and replace the original tag with cloned one in the usage. This cloning is performed through sniffing, and eavesdropping [8]. RFID tag with Proxmark III firmware is a widely used [2]. Over $200 billion has been lost by U.S. manufacturers in the past two decades due to counterfeit products, and affects the growth of SCM due to usage of RFID technology [7]. RFID implementation in pharmaceuticals SCM leads to counterfeit drug in market, RFID clone causes brand damage, losses, and endanger people's lives [3]. RFID clone tags in governments control exhibitions and buildings, leads to forgery and theft of sensitive information [2].

The Physically Unclonable functions (PUF) are widely used in authentication protocols for high security [2, 19]. A lightweight mutual verification protocol using PUF and Linear Feedback Shift Register (LFSR) is developed with complex functions for low-cost RFID tags and large-scale systems [20]. The protocol is prone to desynchronization attack [21, 22]. However, the improved protocol resistance to the desynchronization attack is vulnerable and needs further improved protocol [23, 24]. PUF based tags are with high complexity and cost for implementation or prevention methods.

2.2.1 Track-and-trace method for RFID clone preventions

The Track-and-Trace method ensures reliability and trust through secure, trustworthy e-pedigrees, records the product flow from manufacturers to retailers, synchronizes the tags and databases in real-time with encryption [7]. EPC Gen2 will include a Uniform Resource Identifier (URN) in all tags, enables the origin or owner identification. This allows for online access to RFID record databases and robust deployment of readers without hardcoded implementation [25]. Implementation of the track-and-trace method uses statistical methods and determine normal or abnormal tag based on records [3].

The PrefixSpan algorithm accurately identifies the RFID cloned tags, requires extensive training data for accurate identification [26]. Path checker protocols method identifies the unique tag paths that don't match the specified path, for updates and verification [2]. Despite their high accuracy, these methods often consume excessive memory and read and write speed of tags consumes more time [7].

The Distance Bounding protocol utilizes the broadcast and collisions to identify RFID cloned tags and reduces the need for complex cryptography techniques and tag ID transmission. [27]. This method is suitable for large-scale RFID systems with database synchronization, and their limitations are the requirement of separate systems, geographic areas, and time frames [7]. The Floyd-Warshall algorithm is used in RFID clone detection, and needs high time complexity, performs better in high volume of tags [2].

2.3 BASE protocols and Count-Min protocol to prevent tag clone

The BASE approach counts the total number of tags at the end of RFID tag through scanning and compares with the total number of EPC. It is the simplest method with low computation and consistent accuracy. The clone detection is performed in distance bounding protocol as is Eq. (1) and Eq. (2):

$$if\ T_{EPC} == T_{tags}; No\ clone\ tags \tag{1}$$

$$if\ T_{EPC} \neq T_{tags}; Clone\ tags\ detected \tag{2}$$

Count-Min protocol is an unconventional approach using a Count-Min sketch data structure, predicts RFID cloned tags with lower reading counts. However, this requires multiple readers to read both genuine and clone tags, for high accuracy. The advantages and disadvantages of existing clone detection methods is discussed in Table 2. Eq. (3) shows how the Count-Min protocol performs [3].

$$CM[j, h_j(EPC)] = CM[j, h_j(EPC)] + readcount \tag{3}$$

Table 3 shows the inferences from the previous literature studies. This paper will focus on RFID clone detection methods using proposed MB protocol and MCM protocol for low-cost tags, which are vulnerable clone attacks. RFID clone detection plays an important role in defense of clone attacks [14].

Genuine tags have a higher reading count rate due to their regular check at every stage in the SCM is avoided through the proposed protocol such as MB and MCM [3].

Table 2. Advantages and disadvantages of existing clone detection methods

S.No.	Protocol	Advantages	Disadvantages	Remarks
1	Base	Detection is more accurate and consistent [5, 28]	Less efficient to detect clone attack for a large scale [5, 28]	Execution time is linear with respect to the system scale.
2	Count-Min	To address the accuracy problem, the concept of the Count-Min approach and consistency of tag location are utilized [29]	Not effective when one wants to compute the norms of data stream inputs [29]	Requires multiple readers to read both genuine and clone tags, for high accuracy.

Table 3. Inferences from literature survey

S.No.	Ref.	Year	Protocol	Disadvantages
1	[30]	2018	Slotted ALOHA	Collisions, delay in duplicate reading
2	[31]	2006	Tree-based	Counterfeit tag and RF collisions
3	[32]	2014	Query-tree	Delay in duplicate reading and counterfeit tag
4	[28]	2015	De-clone	Delay in duplicate reading and counterfeit tag

3. METHODOLOGY

The MB protocol in RFID clone detection improves efficiency and accuracy. A Modified Count-Min approach and tag location consistency are employed to address this issue. The RFID clone detection speed and accuracy are improved through the quantitative data from the program such as MB and MCM in the tag reader device compared to other Distance Bounding Protocols such as DeClone and BASE. The output of the RFID clone detection system is measured against two manipulated variables input which was the readings sample size from 1,000 to 10,000 with 1,000 increments and range of RFID cloned tags from 1, 2, 5, 10, 20, 50, 100, and 200 for each reading sample size. The MB and MCM performed using 80 readings sample sizes and with variation in numbers of RFID cloned tags. The implementation of the protocol is done with two different programs, one with an online database and the second with a local database. The main purpose is to evaluate the effectiveness of the RFID clone detection system against different readings of sample sizes and cloned tags. The second implementation program utilizes a reader database for assessment through 80 different RFID cloned tag reading samples, variation in size and number.

3.1 Data collection setup

Since the programs are light weight, the CPU utilization for running the proposed RFID clone detection on python is always lesser than 1%. RN16 plays an important role in identifying a tag without referring to EPC. Python's Dictionary function is used to improve the data retrieval speed. Embedded SQL database is used as local database and Google Firebase is used as IoT cloud database.

3.2 Modified BASE and Modified Count-Min protocol implementation

The proposed RFID clone detection system using MB and MCM shown in Figure 1, which is based on BASE and Count-Min. MB and MCM address the problems of BASE and Count-Min protocol.

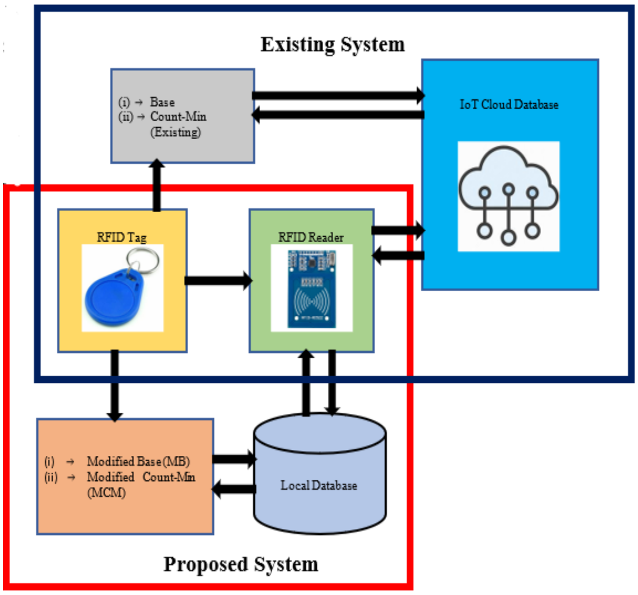

Figure 1. Proposed MB and MCM protocol for RFID clone detection

3.2.1 Modification of BASE

The proposed MB protocol resolves the delay in RFID scanning by comparing the number of EPC and tags on each detected RFID tag. Modifications in the BASE protocol is as shown in Eq. (4) and Eq. (5).

$$\sum_i EPC + EPC_{offset} = \sum_i Tags \tag{4}$$

$$if \sum_i EPC + EPC_{offset} \neq \sum_i Tags\ then\ EPC_{offset} += 1 \tag{5}$$

Whenever the equation is not equal, the EPC is recorded as duplicated EPC tags. MB improves data retrieval speed significantly compared with cloud-based database. With the above two significant changes, Modified BASE improves advantages and overcome disadvantages of existing BASE protocol.

3.2.2 Modification Count-Min

Count-Min needs RFID genuine tag with a higher read count compared to RFID cloned tag and contribute to low accuracy results. In the proposed MCM, determine RFID cloned tags among duplicated tags within the local database. The comparison of genuine tag and duplicated tags are based on Eq. (6) and Eq. (7).

$$Tags_i > Tags_{i-1};\ Tags_{i-1}\ is\ a\ cloned\ tag \tag{6}$$

$$Tags_i < Tags_{i-1};\ Tags_i\ is\ a\ cloned\ tag \tag{7}$$

3.3 Data collection method

The dataset includes Diverse UHF Tag Readings (DUTR). It is a novel dataset that contains passive transmissions of RFID tags that operate at Ultra-High Frequency (1HF). The DUTR system incorporates readings from a total of 300 tags, with each of the three manufacturers contributing 100 total tags. There were five queries performed on each tag, and the Electronic Product Code (EPC) that was transmitted by the tag was observed and recorded. The information was gathered with the assistance of a specialised RFID compliance test equipment that included an FPGA-based IF transceiver, an RF up-converter operating at 2.7 GHz, and an RF down-converter operating at the same frequency.

3.4 Time complexity analysis MB and MCM

The MB and MCM program are evaluated for all data samples and collected results, and results of the MB and MCM are discussed in further section. No data preprocessing is done. Only RFID numbers and data are used. RN16, EPC, Read Count, and Antenna ID features are used to identify RFID cloned tags in reading sample data. The initial evaluation deals with the increased number of readings samples, understands the relationship between the number of readings samples and completion time of the programs. Computation time is measured based on CPU execution time and accuracy is based on number of cloned tag detection %. MB and MCM time complexity is analysed with Distance Bounded Protocol, traditional protocols increase the time directly proportional to the number of readings sample or number of tags. The proposed protocols are evaluated against various readings samples to determine their impact on the solution and discussed in the further section and traditional protocol performs better than traditional Distance Bounding Protocols.

4. RFID CLONE DETECTION USING MB AND MCM

This section discusses the design and implementation of an RFID clone detection system using MB and MCM for detecting duplicate EPC tags. The RFID clone detection design consists of two parts such as detecting duplicate EPC tags using MB approach and identifying clone tags among duplicated tags using Modified Count-Min with Antenna ID consistency check. The RFID clone detection system involves three operations: Tag verification, identifying duplicated tags, and locating exploited EPC tags shown in Figure 2.

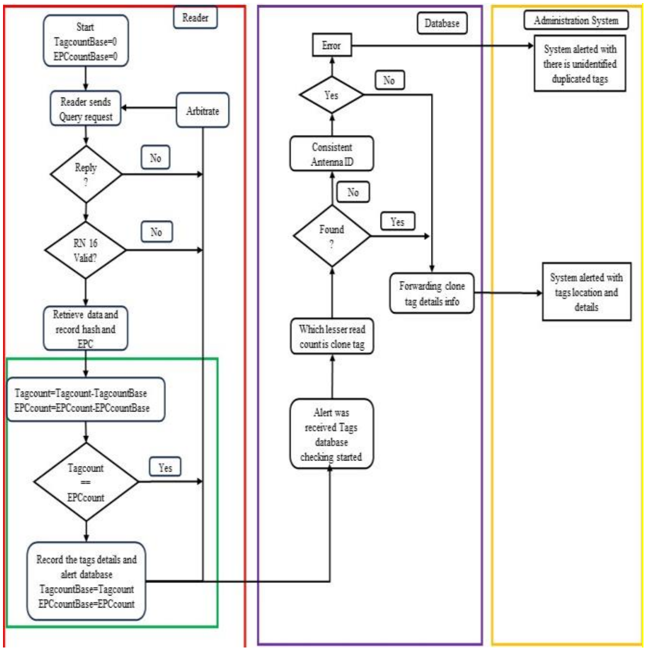
Reader
Start
TagcountBase=0
EPCcountBase=0
Reader sends Query request
Arbitrate
Reply ?
No
RN 16 Valid?
No
Retrieve data and record hash and EPC
Tagcount=Tagcount-TagcountBase
EPCcount=EPCcount-EPCcountBase
Tagcount == EPCcount
Yes
Record the tags details and alert database
TagcountBase=Tagcount
EPCcountBase=EPCcount
Database
Error
Yes
No
Consistent Antenna ID
No
Found ?
Yes
Forwarding clone tag details info
Which lesser read count is clone tag
Alert was received Tags database checking started
Administration System
System alerted with there is unidentified duplicated tags
System alerted with tags location and details

Figure 2. RFID clone detection using MB and MCM

The first operation involves tag verification using RN16 according to EPC Gen2, identifies duplicated tags using Modified BASE techniques as shown in Figure 3. The second operation involves database for further identification of cloned tags. Embedded SQL database is used for local database and Firebase cloud for IoT cloud database. The details of this operation are explained in Figure 4. If cloned tags are identified, backend server or database alerts the administration system by sending an alert message as popup in the computer system and alarm in reader. The user decides to check device or removes tag from inventory. Duplicated tags are identified and exploited EPC tags are located using antenna ID's history.

The basic version of BASE protocol counts RFID and EPC tags after scanning, which is slow and had issues with early reporting and clone attacks. This research proposes a Modified BASE approach to address the problems, through modification of BASE approach. Figure 3 shows the flow of a reader process for the first operation. The Modified BASE approach counts and identifies the total number of RFID tags during each tag read and adds during verification after RN16 and EPC verification. If duplicated tags with the same EPC are detected, the Modified BASE continues scanning and identifies the next duplicated tags. The task is offloaded to a SQL embedded database called SQLite, where there may not be much CPU power available and to avoid more load on the reader and accelerate reader operations, allows the reader to handle more reading sample tags. This approach is faster and less complex than other Distance Bounding Protocols like GREAT or DeClone.

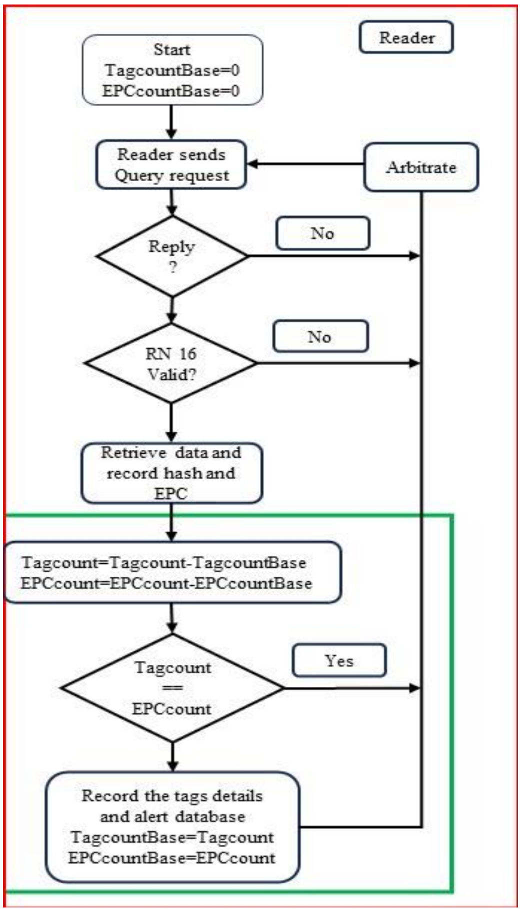
Reader
Start
TagcountBase=0
EPCcountBase=0
Reader sends Query request
Arbitrate
Reply ?
No
RN 16 Valid?
No
Retrieve data and record hash and EPC
Tagcount=Tagcount-TagcountBase
EPCcount=EPCcount-EPCcountBase
Tagcount == EPCcount
Yes
Record the tags details and alert database
TagcountBase=Tagcount
EPCcountBase=EPCcount

Figure 3. Modified BASE on Q-parameter

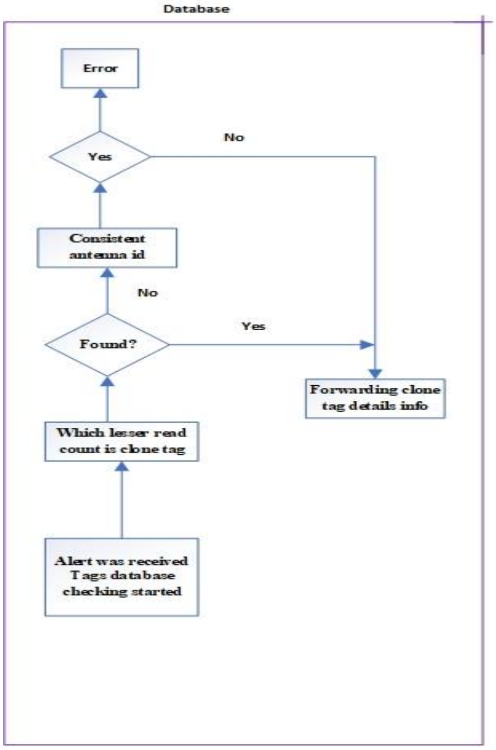
Database
Error
Yes
No
Consistent antenna id
No
Yes
Found?
Forwarding clone tag details info
Which lesser read count is clone tag
Alert was received Tags database checking started

Figure 4. Database/backend server operation

RFID tags have various features such as random generator RN16, CRC, hash value, reader, and antenna ID. To achieve Industry 4.0 standards, database handles simple data comparisons and checking as shown in Figure 4. When an alert on a specific EPC is given by Modified BASE from a reader, some Read Count checking, track, and trace would be done on those tags. A sequence of checking is performed on all tags with the same EPC ID, starting with 'read count'. Genuine tags should have a higher read count than RFID cloned tags, but duplicated tags with lower read count numbers are considered RFID cloned. The consistency of antenna ID is checked, with RFID cloned tags having different antenna Id [33]. If unidentified duplicated tags are detected, the system will notify the user with all the information, with all the information, and the system can act on the detected duplicated tags.

4.1 Result and discussions

This section discusses the implementation of an RFID clone detection system using Modified BASE and Count-Min techniques, utilizing a local and online database.

4.1.1 Sample data creation

The first step of this implementation is the RFID tag samples data creation, which is critical. There are two things considered when creating the readings sample data listed below:

1. The size of the reading's samples data and variation number of RFID cloned tags.
2. The features of RFID as part of each reading are the sample data.

The study uses RN16, EPC, Read Count, and Antenna ID features to identify RFID cloned tags in readings sample data. GID-96 (General Identification with 96 bit) is selected as generic EPC standard, other formats can be used. Official EPC Global standard documents are used for implementation details. The RFID tag's General Manager numbers, managed by the manufacturer or producer, contain URN and owner information. RN16, a randomized value generated by the tag, is crucial for identifying tags without referring to EPC. This feature allows the Q-parameter to count the actual number of tags in an area, even with duplicate EPC values on cloned tags. Sample data varies from 1,000 to 10,000 tags. Each sample tag would contain RN16, EPC, Read Count, and Antenna ID as the RFID features used in this RFID clone detection system as shown in Table 4 and saved in CSV files format. MB and MCM are used for the development of fast and accurate RFID clone detection systems using Modified BASE for speed and Modified Count-Min for accuracy. The concept is implemented in two stages, using a local database within the reader and online via Google Firebase, providing security and encryption for communication. Existing methods performance is low during duplicate reading, counterfeit tag and RF collisions. The future RFID uses URN as part of EPC, provides information and address of the tag database, replaces the existing BASE and Count-Min protocols [34]. They have an online database for IoT applications and Supply Chain Management, with Google Real-time Firebase chosen for extensive API support [35] and the Dictionary data structure used for speedy data retrieval in local databases [36, 37].

4.1.2 Implementation of RFID clone detection system with local database

The next process is performed with local database, utilizing Read Count with a Modified Count-Min approach. Table 5 shows the analysis of RFID clone detection. The detection accuracy of proposed method is about 90% for MCM and MB of 92%. The computation time of MCM is 0.5s whereas the computation time of the existing algorithm with an average time about 7s. The system checks for RFID cloned tags by identifying those with lower Read Count and adding them to the list. If an inconsistent Antenna ID is found, it is added to the list. If duplicate tags exist, a warning is sent to the user, allowing them to identify potential exploited or vulnerable tags.

Table 4. Snapshot of the readings sample data generated

RN16	EPC	Read Count	Antenna ID
35441	35.147303058.1879492.43468522459	55929	6
44113	35.226115088.6960922.44999911700	16737	3
26343	35.153981792.15679896.65394055394	48558	6
6472	35.266574079.8771586.50536700933	18183	4
45852	35.150038679.11248393.58906043812	11459	5
6930	35.101525900.13581982.8266250251	33048	5
57867	35.99498791.6283919.52632475612	4336	2

Table 5. Analysis on tags for clone detection

S.No.	Methods	1000 Genuine Tag/Parameter + Cloned Tags	Number of Cloned Tags Detected	Execution Time	Cloned Detection Time	Cloned Detection %
1	MCM(Proposed)	10	9	0.5s	0.4	90
2	MB(Proposed)	20	18	0.6s	0.5	90
3	MCM(Proposed)	45	42	0.8s	0.7	93.33
4	MB(Proposed)	50	48	0.9s	0.8	96
5	DeClone [5]	10	8	7s	3	80
6	GREAT [5]	30	25	5s	4	83.33
7	BASE [5]	15	12	3s	2	80
8	Count-Min [5]	32	28	6s	5	87.5

5. EXPERIMENT & RESULTS

This paper presents two main analysis matrices: execution time and accuracy of the proposed RFID clone detection system using MB and MCM protocol, considers different reading sample sizes and RFID cloned tag numbers.

5.1 Completion time and speed

The direct comparison of the proposed RFID clone detection system with local database against predecessor work and other Distance Bounding Protocols such as MCM, DeClone and BASE in terms of execution time against the number of readings as in Figure 5.

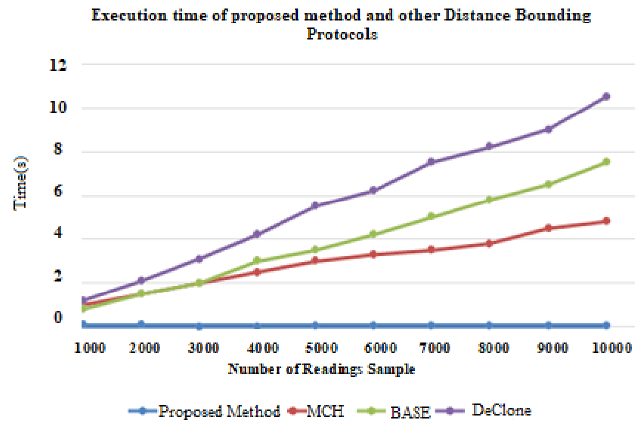

Figure 5. Execution time of proposed method, MCM, DeClone, and BASE against different number of RFID tag

The first observation is execution time of the proposed method such as MCM and MB is lower than any traditional methods. The proposed method execution time almost zero seconds compared to MCM or BASE, reaches eight seconds. The second observation is the execution time of the proposed work is never impacted by the number of readings sample, unlike other Distance Bounding Protocol. The traditional methods execution times are continuously increased with the increased number of readings samples.

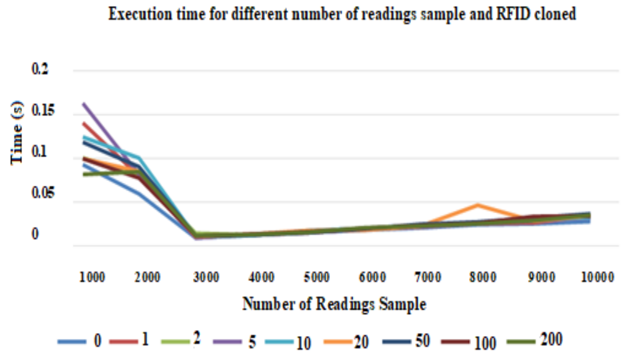

Figure 6. MB method-based execution time vs number of readings sample and number of RFID cloned for the offline database in seconds

Based on Figure 6, the execution time decline to the lowest point at 3,000 readings sample and then, started to incline in a very small number until reached for 10,000 readings sample.

The RFID clone detection program runs the fastest at 3,000 readings samples, small spike in completion time occurs at 8,000 samples with 20 cloned tags. The program completes within 0.2 seconds across various sample sizes. The Modified BASE algorithm finds duplicate tags faster and overcomes limitations of Count-Min. The Python Dictionary function reduces execution time. Although execution time is lower than predecessor works, actual results are better than expected. To implement RFID clone detection in IoT applications such as Supply Chain Management, the solution requires a unified online database in which the RFID database is centralized, and all RFID tags are connected in real-time.

Figure 7 shows a huge incremental in terms of execution time, when moved to the online database compared to the local database. The proposed method such as MCM and MB with an online database has a lengthy execution time of 10 minutes for 8,000 samples, stopping data collection at 9,000 readings.

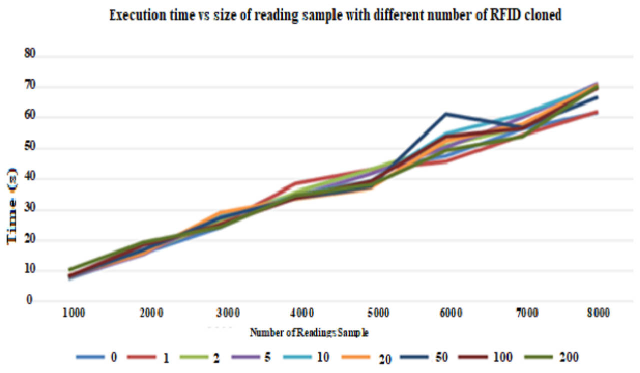

Figure 7. MCM and MB execution time vs size of readings sample with different number of RFID cloned tags in minutes for the RFID clone detection with online database

The number of RFID clone tags does not affect execution time. The method outperforms local distance bounding protocols.

5.2 Accuracy

The RFID clone detection system accuracy value is determined using the confusion matrix, compared the expected and actual results, determines True Positive, True Negative, False Positive, and False Negative values as in Eq. (8).

$$Acc = \frac{TP + TN}{TP + TN + FP + FN} \tag{8}$$

The proposed RFID clone detection system compares detected tags with genuine ones, calculates confusion matrix parameters, and evaluates against previous works, allowing direct comparison in accuracy.

A true negative chart against the number of RFID cloned tags shown in Figure 8. The graph shows 100% genuine tags in readings sample, which are not listed as RFID cloned tags, indicates with 100% accuracy for proposed method.

Figure 9 shows the percentage of true positive RFID cloned tags in the readings sample, above 90% is achieved. The lower percentage is due to the single tag failing detection and being listed as an unidentified duplicate.

Figure 10 shows false-positive values against RFID cloned tags, with a slightly inconsistent percentage within 0.5 percent.

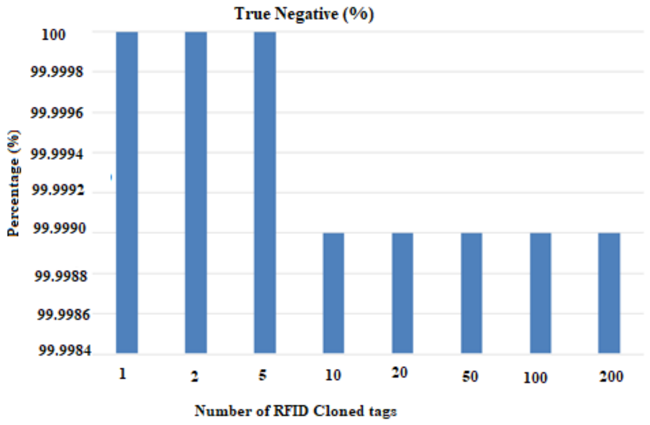

Figure 8. MB-based true negative chart in percentage

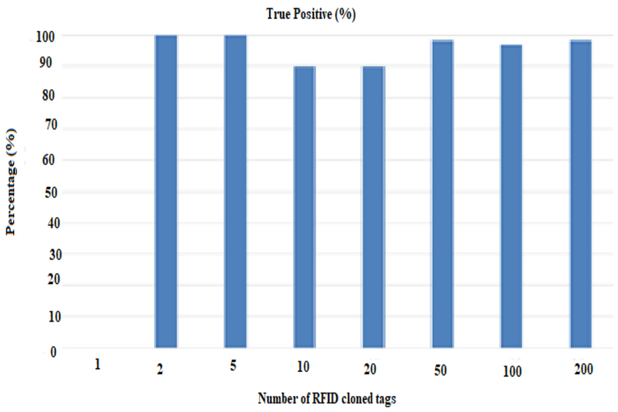

Figure 9. True positive chart in percentage against RFID cloned tags

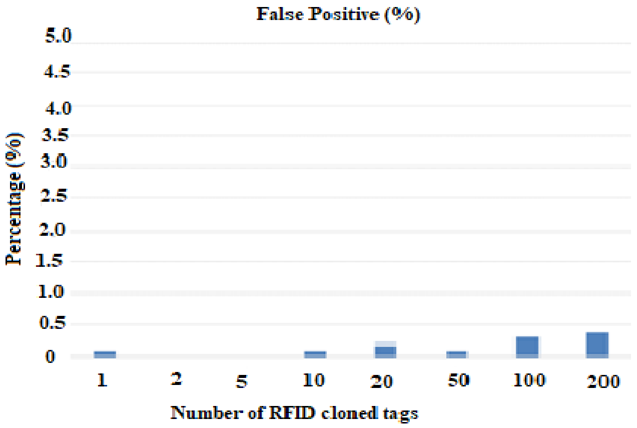

Figure 10. MB-based false positive chart in percentage

Figure 11 displays the percentage of false-negative RFID cloned tags, represents the percentage of genuine tags identified by the proposed methods such as MB and MCM, and the True Positive graph.

The proposed RFID clone detection system accuracy is calculated using Confusion Matrix and compared to previous works like MCM, BASE, and DeClone as shown in Figure 12, results show similar accuracy for both local and offline databases.

The method accuracy is slightly lower than MCM for a smaller number of RFID tags, still maintains closer to 100% with an increased number of tags. High accuracy is attributed to Modified Count-Min implementation and Antenna ID consistency check.

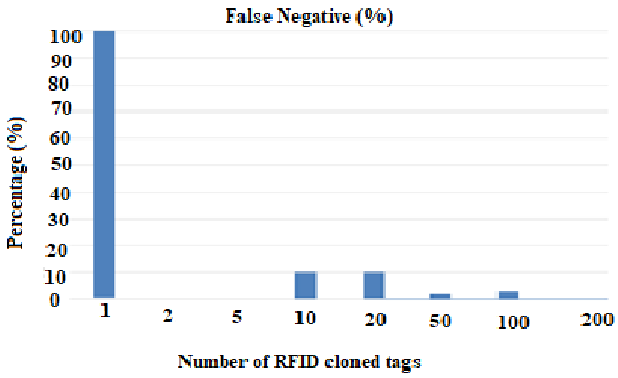

Figure 11. MB and MCM based false negative chart in percentage

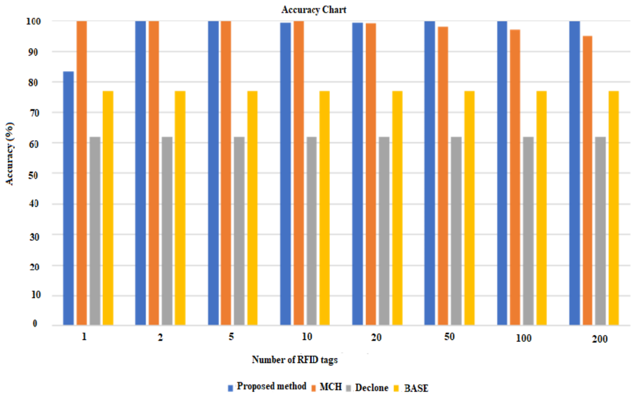

Figure 12. Comparison of RFID clone detection accuracy between proposed method, MCM, DeClone, and BASE vs the number of clone IDs [3]

The proposed RFID clone detection system has the highest accuracy among Distance Bounding Protocols, with small inconsistencies in the graph for lower number of cloned tags. The low accuracy for single-number cloned tags is due to the failure in detection of single cloned tags as an RFID cloned tag. However, reading sample size increases, the accuracy percentage increases. The Modified BASE, MCM with consistency check of Antenna ID provides faster and more consistent accuracy with higher cloned tags. The system identifies RFID cloned tags in reading samples due to similar content, read count, and duplicated EPC tags. The system improves the identification of the exact RFID cloned tag, when the Read Count of an RFID cloned tag is higher than the genuine tag, result in the detection of genuine tags as cloned. The accuracy of the system improves with actual RFID data.

The proposed RFID clone detection with a local database performs better than other Distance Bounding protocols in terms of speed, maintains a completion time within 0.2 seconds for all sizes of readings sample and number of RFID cloned tags is observed and shown in Figure 13. Results improve through the MB and MCM.

However, the proposed RFID clone detection system such as MB and MCM with an online database performs poorly in terms of speed, with the number of RFID cloned tags never affecting execution time. Further understanding is needed to address this issue.

Figure 14 reveals inconsistencies in execution time increments with sample size, with larger samples showing smaller increase.

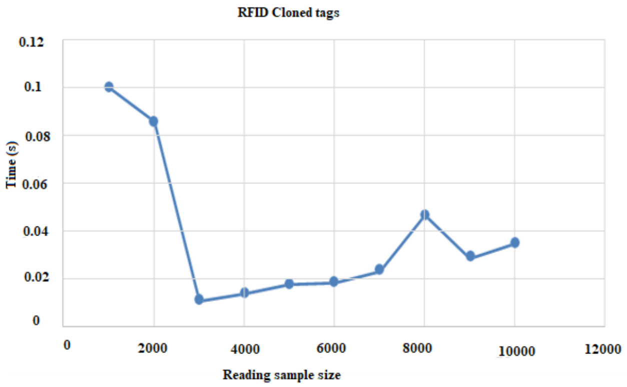

Figure 13. Execution time vs readings sample size with 20 RFID cloned tags of the improved MB and MCM with local database

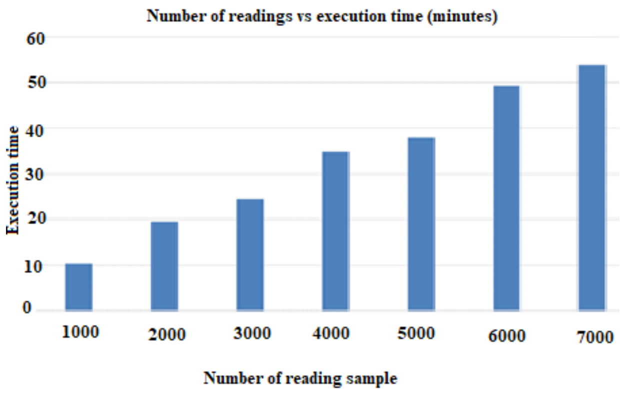

Figure 14. Execution time vs number of readings sample with 50 RFID cloned tags of MB and MCM with online database in minutes

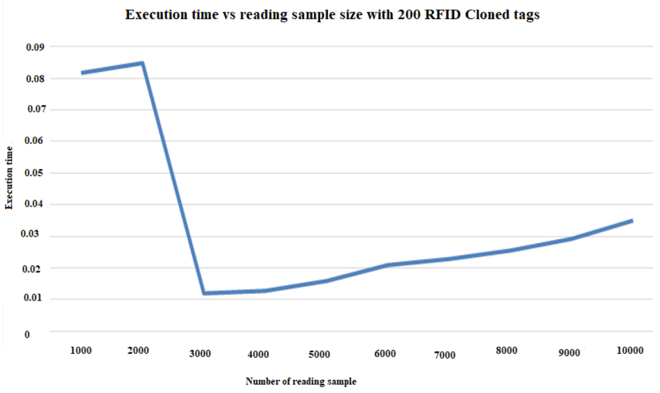

Figure 15. Execution time vs number of readings sample with 200 RFID cloned tags of MB and MCM for offline database

Figure 15 and Figure 16 compare offline and online database implementations of the proposed work with the same number of RFID cloned tags.

The computational values based on accuracy, execution time, precision and recall are shown in Table 6.

5.2.1 Accuracy analysis

The second analysis will be on how the programs perform against the different numbers of RFID cloned tags. Based on the results of previous Distance Bounded Protocols, the accuracy is being expected to reduce with an increase in the number of readings sample [3].

Therefore, the programs are running against the different numbers of RFID cloned tags in different readings sample sizes to evaluate the accuracy of the RFID clone detection system output. The value of accuracy is determined by using the confusion matrix as shown in Figure 17.

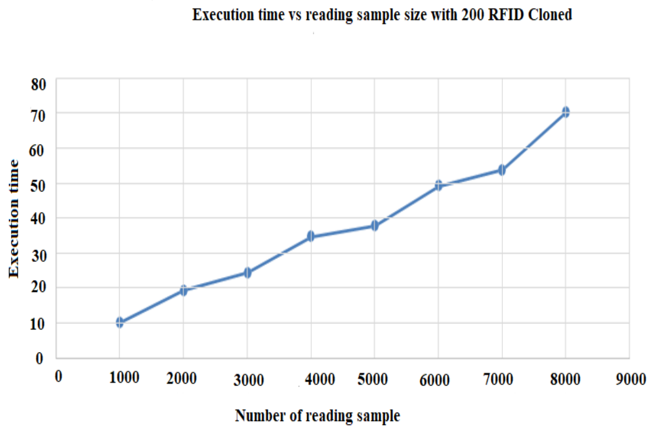

Figure 16. Execution time vs number of readings sample number with 200 RFID cloned tags of the proposed MB and MCM for online database

n=165	Predicted: NO	Predicted: YES	
Actual: NO	TN = 50	FP = 10	60
Actual: YES	FN = 5	TP = 100	105
	55	110	

Figure 17. Confusion matrix weight table

From all the evaluation data, a conclusion can be made on the proposed RFID clone detection system, with both online and local databases, with other Distance Bounding Protocols in terms of speed and accuracy, and is evaluated for its impact on reader processing.

Table 6. Computational values based on accuracy, execution time, precision, recall

S.No.	Methods (Duplicate Reading, Counterfeit Tag and RF Collisions)	Tag/Parameter (Original Tag, Cloned Tag, RF Collision)	Computation Time	Accuracy	Execution Time	Precision	Recall	Data Verification @ Cloud/Local Drive
1	MCM (Proposed)	Cloned tag	7s	96%	0.5s	95%	0.9	Local drive
2	MB (Proposed)	Cloned tag	6s	95.5%	0.4s	93%	0.8	Local drive
3	MCM (Proposed)	RF Collision	8s	95%	0.6s	94.6%	0.9	Local drive
4	MB (Proposed)	RF Collision	7s	95.3%	0.5s	95%	0.9	Local drive
5	Declone+ [28]	cloned tag	10s	90%	8s	89%	1.2	Cloud
6	Federated ML [38]	cloned tag	12s	88%	10s	86%	1.5	Cloud
7	DAG [38]	Cloned tag	14s	86%	12s	84%	1.6	Cloud
8	GREAT [28]	RF collision, cloned tag	10s	90%	8s	89%	1.2	Cloud

6. CONCLUSION

RFID clone detection with proposed methods such as Modified BASE (MB) and Modified Count-Min (MCM) are used for the clone detection in the RFID tag. From experimental analysis the proposed methods detect the clone in 0.2 seconds. The accuracy of clone detection is about 95% for Modified BASE (MB) protocol, which compares the number of EPC with the number of RFID tags duplicate tags detection. In the proposed method reader device has a local database. The local database in reader prevents the detection clone tags based on the comparison of EPC numbers of tags from cloud dataset and reduces computational complexity based on encryption and decryption and proves through the False Negative Chart Percentage. The number of clones increases and the execution time decreases in local database. i.e., embedded SQL database. These embedded databases can offer better performance as they operate within the same process as the application, reducing the overhead of inter-process communication. Proposed MCM method computation time is 50 times less than existing Bounding Protocol. Results show that execution time slightly increases with the number of reading samples, for the small scale. Online implementation is inconsistencies in completion time increments. The study demonstrates an efficient RFID clone detection system using MB and MCM, along with Antenna ID has consistency. The system is accurate and efficient, with minimal hardware indifference impact. However, the offline database implementation has poor execution time. The study's accuracy can be improved by using Deep Learning for more than 40,000 tags and an Embedded base SQL database improves the entire cloning detection process in real dataset for testing. The work is limited by facilities and resources, including time, internet services, and server location.

ACKNOWLEDGMENT

We appreciate School of Computer Sciences of Universiti Sains Malaysia for their technical support during this research work.

REFERENCES

[1] Ding, K., Jiang, P. (2017). RFID-based production data analysis in an IoT-enabled smart job-shop. IEEE/CAA Journal of Automatica Sinica, 5(1): 128-138. https://doi.org/10.1109/JAS.2017.7510418

[2] Huang, W.Q., Zhang, Y.F., Feng, Y. (2020). ACD: An adaptable approach for RFID cloning attack detection. Sensors, 20(8): 2378. https://doi.org/10.3390/s20082378

[3] Kamaludin, H., Mahdin, H., Abawajy, J.H. (2018). Clone tag detection in distributed RFID systems. PloS One, 13(3): e0193951. https://doi.org/10.1371/journal.pone.0193951

[4] Araújo, P.H.M., Jucá, S.C.S., Gonçalves, D.L.C., Silva, V.F.D., Pereira, R.I.S., Silva, S.A.D. (2019). Cloud-based RFID access control using lightweight messaging protocol. International Journal of Advanced Engineering Research and Science, 6(1): 7-17. https://doi.org/10.22161/ijaers.6.1.2

[5] Sheng, Q.Z., Li, X., Zeadally, S. (2008). Enabling next-generation RFID applications: Solutions and challenges. Computer, 41(9): 21-28. https://doi.org/10.1109/MC.2008.386

[6] Mahinderjit-Singh, M., Li, X. (2010). Trust in RFID-enabled supply-chain management. International Journal of Security and Networks, 5(2-3): 96-105. https://doi.org/10.1504/IJSN.2010.032208

[7] Khalil, G., Doss, R., Chowdhury, M. (2019). A comparison survey study on RFID based anti-counterfeiting systems. Journal of Sensor and Actuator Networks, 8(3): 37. https://doi.org/10.3390/jsan8030037

[8] Xie, X., Liu, X.L., Wang, J.X., Guo, S., Qi, H., Li, K.Q. (2023). Efficient integrity authentication scheme for large-scale RFID systems. IEEE Transactions on Mobile Computing, 22(9): 5216-5230. https://doi.org/10.1109/TMC.2022.3172486

[9] Younis, M.I., Abdulkareem, M.H. (2017). ITPMAP: An improved three-pass mutual authentication protocol for secure RFID systems. Wireless Personal Communications, 96: 65-101. https://doi.org/10.1007/s11277-017-4152-0

[10] Anusha, P., Rao, P.R., Rai, N.P. (2023). Secured authentication of RFID devices using lightweight block ciphers on FPGA platforms. IEEE Access, 11: 107472-107479. https://doi.org/10.1109/ACCESS.2023.3320277

[11] Tu, Y., Piramuthu, S. (2017). Lightweight non-distance-bounding means to address RFID relay attacks. Decision Support Systems, 102: 12-21. https://doi.org/10.1016/j.dss.2017.06.008

[12] Sultan, A.R., Rashid, I., Khan, F., Tahir, S., Pasha, M., Sultan, A. (2021). A new secure authentication based distance bounding protocol. PeerJ Computer Science, 7(2): e517. https://doi.org/10.7717/peerj-cs.517

[13] Khalil, F.M., Fazil, A., Hussain, M.J., Masood, A. (2024). Cross-layer RF distance bounding scheme for passive and semi-passive ubiquitous computing systems. Computers & Security, 137: 103633. https://doi.org/10.1016/j.cose.2023.103633

[14] Mahinderjit-Singh, M., Li, X., Li, Z.H. (2011). A cost-based model for risk management in RFID-enabled supply chain applications. Supply Chain Management, 201-236. https://doi.org/10.5772/15067

[15] Wamba, S.F., Anand, A., Carter, L. (2013). A literature review of RFID-enabled healthcare applications and issues. International Journal of Information Management, 33(5): 875-891. https://doi.org/10.1016/j.ijinfomgt.2013.07.005

[16] Chopade, S.S., Gupta, H.P., Dutta, T. (2023). Survey on sensors and smart devices for IoT enabled intelligent healthcare system. Wireless Personal Communications, 131: 1957-1995. https://doi.org/10.1007/s11277-023-10528-8

[17] Sonavane, A., Khamparia, A., Gupta, D. (2023). A Systematic review on the internet of medical things: Techniques, open issues, and future directions. Computer Modeling in Engineering & Sciences, 137(2): 1-26. https://doi.org/10.32604/cmes.2023.028203

[18] Bu, K., Liu, X., Xiao, B. (2014). Approaching the time lower bound on cloned-tag identification for large RFID systems. Ad Hoc Networks, 13(B): 271-281. https://doi.org/10.1016/j.adhoc.2013.08.011

[19] Zhang, J., Chang, C.H., Gu, C.Y., Hanzo, L. (2022). Radio frequency fingerprints vs. physical unclonable functions-are they twins, competitors or allies? IEEE

Network, 36(6): 68-75. https://doi.org/10.1109/MNET.107.2100372

[20] Kulseng, L., Yu, Z., Wei, Y.W., Guan, Y. (2010). Lightweight mutual authentication and ownership transfer for RFID systems. In 2010 Proceedings IEEE INFOCOM, San Diego, CA, USA, pp. 1-5. https://doi.org/10.1109/INFCOM.2010.5462233

[21] Xu, H., Ding, J., Li, P., Zhu, F., Wang, R.C. (2018). A lightweight RFID mutual authentication protocol based on physical unclonable function. Sensors, 18(3): 760. https://doi.org/10.3390/s18030760

[22] Costa, C., Antonucci, F., Pallottino, F., Aguzzi, J., Sarriá, D., Menesatti, P. (2013). A review on agri-food supply chain traceability by means of RFID technology. Food and Bioprocess Technology, 6: 353-366. https://doi.org/10.1007/s11947-012-0958-7

[23] Bendavid, Y., Bagheri, N., Safkhani, M., Rostampour, S. (2018). IoT device security: Challenging "a lightweight RFID mutual authentication protocol based on physical unclonable function". Sensors, 18(12): 4444. https://doi.org/10.3390/s18124444

[24] Kumar, V., Kumar, R., Jangirala, S., Kumari, S., Kumar, S., Chen, C.M. (2022). An enhanced RFID-based authentication protocol using PUF for vehicular cloud computing. Security and Communication Networks, 2022: 8998339. https://doi.org/10.1155/2022/8998339

[25] Garcia-Alfaro, J., Herrera-Joancomartí, J., Melià-Seguí, J. (2015). Security and privacy concerns about the RFID layer of EPC Gen2 networks. Advanced Research in Data Privacy, Springer, Cham, 303-324. https://doi.org/10.1007/978-3-319-09885-2

[26] Liu, Z.L., Liu, D.S., Li, L., Lin, H., Yong, Z.Q. (2015). Implementation of a new RFID authentication protocol for EPC Gen2 standard. IEEE Sensors Journal, 15(2): 1003-1011. https://doi.org/10.1109/JSEN.2014.2359796

[27] Wang, P.C., Yun, Zhou, Y., Zhu, C., Huang, J.C., Zhang, W.M. (2017). Analysis on abnormal behavior of insider threats based on accesslog mining. CAAI Transactions on Intelligent Systems, 12(6): 781-789. https://doi.org/10.11992/tis.201706041

[28] Bu, K., Xu, M.J., Liu, X., Luo, J.Q., Zhang, S.G., Weng, M. (2015). Deterministic detection of cloning attacks for anonymous RFID systems. IEEE Transactions on Industrial Informatics, 11(6): 1255-1266. https://doi.org/10.1109/TII.2015.2482921

[29] Cormode, G., Muthukrishnan, S. (2005). An improved data stream summary: The Count-Min sketch and its applications. Journal of Algorithms, 55(1): 58-75. https://doi.org/10.1016/j.jalgor.2003.12.001

[30] Benny, R., Antony, J.K. (2018). Design and implementation of modified slotted ALOHA protocol for RFID readers. In 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, pp. 540-545. https://doi.org/10.1109/RTEICT42901.2018.9012474

[31] Bonuccelli, M.A., Lonetti, F., Martelli, F. (2006). Tree slotted ALOHA: A new protocol for tag identification in RFID networks. In 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'06), Buffalo-Niagara Falls, NY, USA, p. 6. https://doi.org/10.1109/WOWMOM.2006.112

[32] Yeh, M.K., Lai, Y.L., Jiang, J.R. (2014). An efficient query tree protocol for RFID tag anti-collision. In 2014 20th IEEE International Conference on Parallel and Distributed Systems (ICPADS), Hsinchu, Taiwan, pp. 926-930. https://doi.org/10.1109/PADSW.2014.7097910

[33] Wu, Z.Y. (2019). An radio-frequency identification security authentication mechanism for internet of things applications. International Journal of Distributed Sensor Networks, 15(7). https://doi.org/10.1177/1550147719862

[34] Wang, L., Norman, B.A., Rajgopal, J. (2007). Placement of multiple RFID reader antennas to maximise portal read accuracy. International Journal of Radio Frequency Identification Technology and Applications, 1(3): 260-277. https://doi.org/10.1504/IJRFITA.2007.015850

[35] Kousiouris, G., Tsarsitalidis, S., Psomakelis, E., Koloniaris, S., Bardaki, C., Tserpes, K., Anagnostopoulos, D. (2019). A microservice-based framework for integrating IoT management platforms, semantic and AI services for supply chain management. ICT Express, 5(2): 141-145. https://doi.org/10.1016/j.icte.2019.04.002

[36] TechVidvan, 2020. Python advantages and disadvantages – step in the right direction. Available https://techvidvan.com/tutorials/python-advantages-and-disadvantages/, accessed on Nov. 5, 2020.

[37] Moroney, L. (2017). The firebase realtime database. The Definitive Guide to Firebase: Build Android Apps on Google's Mobile Platform, 51-71. https://doi.org/10.1007/978-1-4842-2943-9_3

[38] Piva, M., Maselli, G., Restuccia, F. (2021). The tags are alright: Robust large-scale RFID clone detection through federated data-augmented radio fingerprinting. In Proceedings of the Twenty-second International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing, pp. 41-50. https://doi.org/10.1145/3466772.3467033