International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600

http://www.ijcsjournal.com Volume 10, Issue 2, No 6, 2022. ISSN: 2348-6600
Reference ID: IJCS-448 PAGE NO: 3025-3034

A NOVEL APPROACH TO PROTECT CLOUD-BASED IIoT SENSITIVE DATA USING DYNAMIC ABE SCHEME

Sameera Chatti[1], Tejaswini Amballa[2],
Chaitanya Pithani[3], Pradeep Velasiri[4]
Department of Computer Science and Engineering,
School of Technology,
GITAM Deemed to be University,
Visakhapatnam, Andhra Pradesh, India.

Abstract

The industrial internet of things is bending towards developing technology. The main concern in the presence of abundant data is the security and the capturing of the time-series data when a particular process is being carried on. Security concerns come into the limelight when the collected IoT time-series data is uploaded to the cloud for further processing. When large data is being handled, it faces major efficiency and key leakage issues. And using the traditional encryption and decryption techniques for the encrypting and decrypting process of the captured IoT data might cause some efficiency problems. In this article, we ensure to provide better efficiency and diminish the key leakage issues that are generally faced. In our scheme, we propose a reliableIIoT cloud-based data access control approach. The scheme we propose is based on how the RFID tags can be replaced by the BLE (Bluetooth-Low Energy) or the UWB (Ultra-wide range Bluetooth).Our scheme enables users to enforce a novel approach to secure their sensitive data using the cipher text policies and access controls that provide the maximum level of security to the data that is to be kept confidential. Our scheme adopts a hybrid cloud infrastructure to allow the users to use the policies and the CP-ABE tasks which are expensive. Our scheme guarantees strong privacy protection which may be a concern in the older versions which might lack optimal efficiency results. This scheme, with the help of item-level data security, ensures the strong protection of sensitive data that is at high risk of having leakage issues. We attain these goals with the help of the respective encryption and optimization techniques. Our performance assessments combine system implementation with large-scale emulations and confirm the security and efficiency of our design.

Introduction

The Industrial Internet Of Things (Iiot) Allows The Industrial System To Collect Abundant Iot Data Including The Time-Series Data Of The Production Process. The Foundational Means Is

Radio-Frequency Identification (Rfid) Technology, But The Rfid Tags Can Be Replaced With The Ble And The Uwb. Uwb Is Widely Used In Home Appliances And For Lower-Range Distances. But The Uwb Can Sustain The Larger Ranges And Provide A Higher Data Transmission Rate Than The Rfid Technology That Is Being Used Now. By Wearable Technology, Virtual Helpers, Automobiles, And Other Sophisticated Equipment, The Internet Of Things (Iot) Has Completely Changed How We Live. Iot Is Widely Employed In Both Commercial And Consumer Environments [1]; It Is Not Just Confined To The Consumer World. This Technology Has Completely Changed How Businesses Use Data And Operate. Industrial Iot (Iiot) Utilizes Advanced Data Analytics And Digital Interconnectivity To Improve Manufacturing, Production, Transportation, And Other Industrial Sectors. Businesses In The Production And Manufacturing Sectors Have Quickly Embraced Iiot To Gain A Competitive Edge[2].Our Scheme Adopts A Hybrid Cloud Infrastructure To Allow The Users To Use The Policies And The Cp-Abe Tasks Which Are Expensive [4-10].

TECHNOLOGIES:

1. RFID TECHNOLOGY:

Readers and tags are the two-fold of the wireless networks called Radio Frequency Identity (RFID). A reader is a micro electronic device having few transmitters that broadcast radio signals and get in signs after RFID tags. Tags may be active or passive, with these radio signals we can send respective device identification and supported info to their neighbor readers. passive RFID tags can be powered by the reader even without a battery which is utilized to control active RFID tags. These tags include a range of data categories, extending after a unique serial number to several pages of info. Readers might be installed on a position or dangling after the ceiling, or if they are portable so they might be passed by finger. Reader techniques might also be integrated with cabinet designs, areas, or construction.

2. ULTRA-WIDEBAND BAND TECHNOLOGY:

When two UWB devices like a touch phone, nimble watch, AI-based key, or tile, are near each neighbor device, the gadgets begin "reaching." Determining the point in time of flying (ToF) among gadgets, or the slice time of trial/reply protocol data units is referred to as ranging. Ultra-wideband is a little-scale connectionless transmission structure that uses radio signals, the same as WIFI and Bluetooth. Though, not like its entrants, it works at exceptionally high-level frequencies, including a broad range of Giga Hertz frequencies, and can be utilized to track exceptionally accurate spatial and maneuvering info.

3. BLUETOOTH LOW ENENRGY:

The Less Energy (LE) approach based on Bluetooth is constructed to function at exceptionally less power consumption stages. The

Less Energy(LE) approach based on Bluetooth presents companies with a substantial measure of tractability to make manufactured goods that fit the certain link establishment of their marketplace by broadcasting data over forty channels with a 2.4GHz unlicensed ISM frequency spectrum. The Less Energy(LE) approach based on Bluetooth encourages a range of transmission topographic anatomy, varying from peer to peer to broadcast and, best newly, mesh, getting it potential to develop a reliable, vast range of device internetworks using Bluetooth expertise. Bluetooth LE is increasingly frequently employed as a device positioning technology to meet the growing need for highly accurate indoor location services, while initially being renowned for its device communications capabilities. One device can now use features in Bluetooth LE to find, locate, and detect the direction of another device.

MODEL AND DESIGN GOALS:

This scheme validates that the data transmission rate is optimal when the BLE and UWB are used then by the usage of the RFID technology. UWB offers longer battery life and is already successfully implemented in the vast usage of home appliances and other related sectors. While preparing this paper believed that the higher data transmission rate might result in the faster collection of the data and the upload to the cloud service for the further processing of the attribute-based encryption (ABE) tasks would be done at an optimal speed[11-15].

EXISTINGMODELS VS PROPOSED MODEL:

The existing models that are proposed by using the RFID technology have some issues regarding security and efficiency. The problem we identified is the data transmission rate and optimal security while being encrypted and uploaded to the cloud service for the execution of the CP-ABE tasks. The older models that use RFID technology to detect the item at the warehouse or while the production or manufacturing process detects the time-series data are way less optimal than compared to the new evolving technologies. We identified some of the emerging technologies that are being vastly used in the other sectors and give better and optimal results than compared the older models that are proposed using the RFID and related technologies.

1. DRAWBACKS IDENTIFIED:

- Time complexity
- Encryption and decryption time
- Revocation
- Update policy
- Alternatives for RFID technology.

2. IDENTIFIED ALTERNATIVES FOR THE RFID TECHNOLOGY:

1. Active RFID
2. Ultra-wideband and RTLS
3. Wi-Fi RTLS
4. INFRARED RTLS

Basically, the Passive RFID TAGS are being used in the foundational RFID technology. The Passive

RFID tags help you identify the item and help to confirm the presence of the specific tagged item in the room, but it does not tell you where it is located. This is the reason the passive RFID tags are not being used in the appliances like smart watches, etc., if lost the item's particular location in the room cannot be quickly determined. When a large-scale industry like industrial IoT with large-scale rooms and warehouses where the location of the tagged item is the primary source to transport or in a manufacturing company to detect the affected product to be eliminated by the workers/employees that are taking care of the manufacturing process. But the Passive RFID tags when compared to the Active RFID tags are accurate but are expensive. RFID tags are generally used for immediate and quick access to an item in a vast space where all the products are stored. The RFID technology with great advantageous specifications also has some disadvantages and drawbacks that question the users to think for a minute and choose what technology they really want to adopt. The spine of the RFID technology is the "backscatter communication" that immediately records and fetches the data required from the database or sends any updates to the database. The better the used RFID tags with optimal ranging and speed, the faster backscatter communication, and the faster the data collection and fetching process.

DESIGN GOALS:

Our design is mainly to increase efficiency by proposing a new technique which is currently the promising technology in a vast range of applications including home appliances, smart gadgets, etc., the developed design might reduce the issues that the existing models that are developed with the RFID-technology. Our design is based on the model which uses the Ultra-wideband RTLS(UWB).Among the researched technologies that are evolving gradually and are being used we bent towards the UWB due to its competence and capability to sustain a longer life and also the range that it can provide giving the accurate positioning than compared to the RFID and the other technologies.

The Barcode system and other Image identification systems are also used in some industries, but they cause some security issues so in most large-scale industries these Barcode systems and Image systems are not utilized. The major reason that these Barcodes and other Image systems are that they require the line-of-sight and might cause some errors.

DRAWBACKS OF RFID TAGS IDENTIFIED ARE:

- cost of Active RFID tags
- security
- privacy
- reliability

The main concern in using the "tag-aided system" is that the tags themselves might arise errors. Multiple tags might reply at one once resulting in reception errors. When the large-scale industry is considered, these little errors might cause a huge ruckus and might result in the alterations of the items. When a particular production or manufacturing process is being processed the items are positioned and identified with the help of the tags that are set to each and every item that is involved in the production process. Even though, the Image systems like barcode systems will not cause multiple receiver errors like RFID when something goes wrong in the process these Image systems are outdated due to the emerging technologies which overruled the old methods even though they are efficient. When large-scale industries are considered Image systems are not much feasible as the items are more and require a special team to scan the tags also not adapting to the growing technologies might cause loss of data and other security issues [16].

CHIPLESS TECHNOLOGY:

RFID is the foundational technology that is used in industrial IoT concepts. RFID tags that do not require a microchip in the transponder are known as chip less RFID tags. Compared to barcodes, which need a person to scan them, RFIDs have a greater range and can be automated. The price of RFIDs is the biggest barrier to widespread adoption. There is an existing news article that supports that the “next generation asset tracking solutions based on the Bluetooth Low Energy (BLE) and the Ultra-Wide Band (UWB) will replace the RFID”.

WHY ULTRA-WIDE BAND (UWB)?

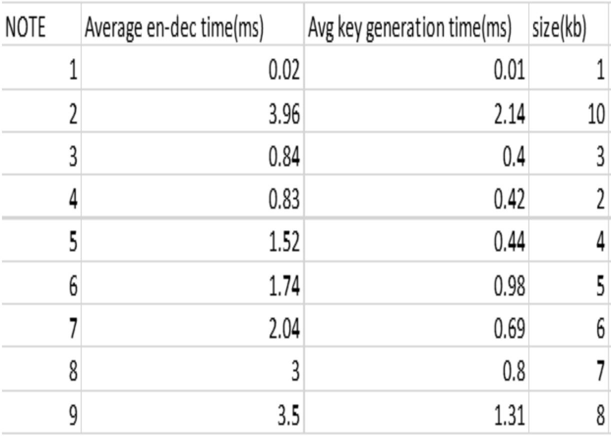
The use of wireless technologies is essential for putting the Internet of Things into industrial use. The precision, security, and real-time localization capabilities offered by Ultra-wideband (UWB) are unsurpassed by those of other wireless technologies, such as Wi-Fi, Bluetooth, and GPS. UWB has been around for a while, but until the late 1990s, it was only used for military purposes. UWB technology is currently driving the IIoT transformation wave.UWB has a wide range of applications, including asset tracking, smart grids, fleet management, and safety in human-robot interactions. Positioning systems based on UWB might have benefits like flexible deployment options and a favorable performance-cost ratio. With the capacity to work in mixed indoor-outdoor contexts, UWB offers essential flexibility and enables excellent localization accuracy with either global or relative positioning. As automation becomes one of the primary transformation goals for CIOs, the IIoT industry is anticipated to grow quickly. This aids manufacturing facilities in controlling production levels to satisfy consumer demand. The administration has also placed a major emphasis on boosting the nation's local industrial capacities.UWB positioning systems, which may be integrated into a variety of intelligent industrial systems, can offer competitive solutions for asset and person tracking. UWB technology has a significant chance of being widely used in IIoT across a variety of sectors and areas. It has the incredible advantages of having one of the lowest power footprints and having high-precision positioning capabilities, which would undoubtedly open the door for expanding usage in the future.

MODELS PROPOSED:

IJCS International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
SKRGC Since 2012
http://www.ijcsjournal.com Volume 10, Issue 2, No 6, 2022. ISSN: 2348-6600
Reference ID: IJCS-448 PAGE NO: 3025-3034

1. MODEL – 01

The model-1 we considered takes an only a text file as the input. The model is run in the command prompt using the respective commands. The model takes the input of the text file and evaluates the file and follows to give the average encryption time, average key generation time. The time taken to generate the key and average encryption-decryption time(ms) depends on the size of the text file considered or the text file that is given as the input to the encrypting algorithm.



NOTE	Average en-dec time(ms)	Avg key generation time(ms)	size(kb)
1	0.02	0.01	1
2	3.96	2.14	10
3	0.84	0.4	3
4	0.83	0.42	2
5	1.52	0.44	4
6	1.74	0.98	5
7	2.04	0.69	6
8	3	0.8	7
9	3.5	1.31	8

Table 8.1.1

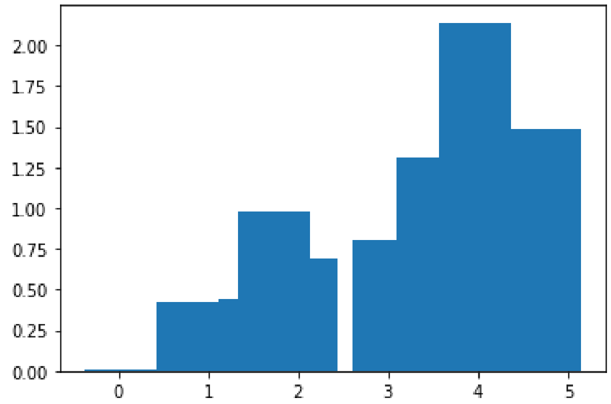


Fig.8.1.1

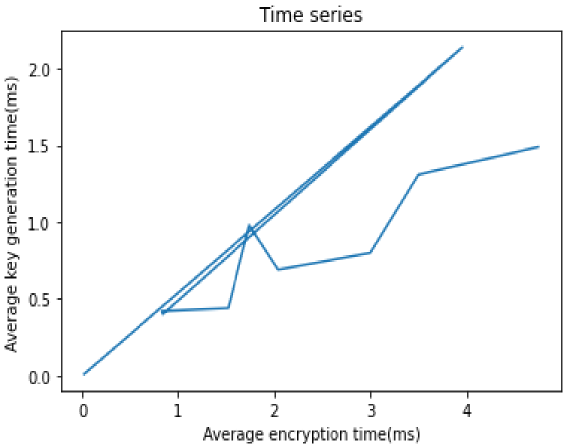


Fig.8.1.2

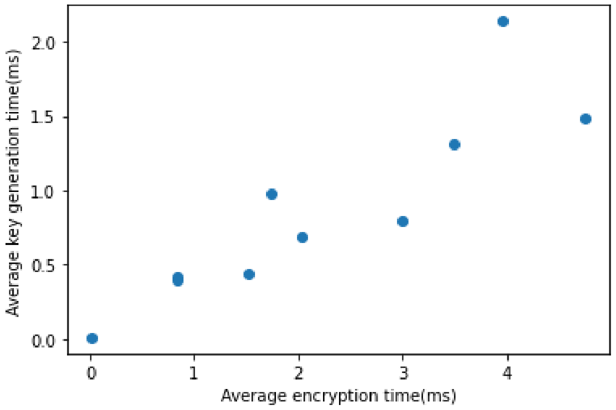
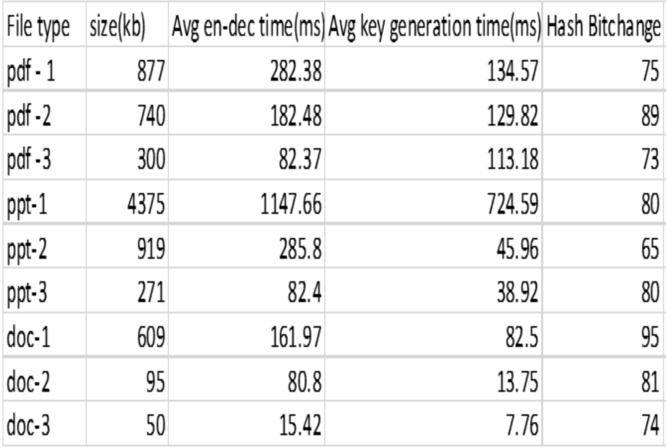


Fig.8.1.3

2. MODEL – 02

The model-2 we considered takes any file as the input. The model is run in the command prompt using the respective commands. The model takes the input of any input file given like files with CSV, pdf, document, ppt, etc., extensions and evaluates the file, and follows to give the average encryption time and average key generation time. The time taken to generate the key and average encryption-decryption time(ms) depends on the size of the text file considered or the text file that is given as the input to the encrypting algorithm.



File type	size(kb)	Avg en-dec time(ms)	Avg key generation time(ms)	Hash Bitchange
pdf - 1	877	282.38	134.57	75
pdf -2	740	182.48	129.82	89
pdf -3	300	82.37	113.18	73
ppt-1	4375	1147.66	724.59	80
ppt-2	919	285.8	45.96	65
ppt-3	271	82.4	38.92	80
doc-1	609	161.97	82.5	95
doc-2	95	80.8	13.75	81
doc-3	50	15.42	7.76	74

table.8.2.1

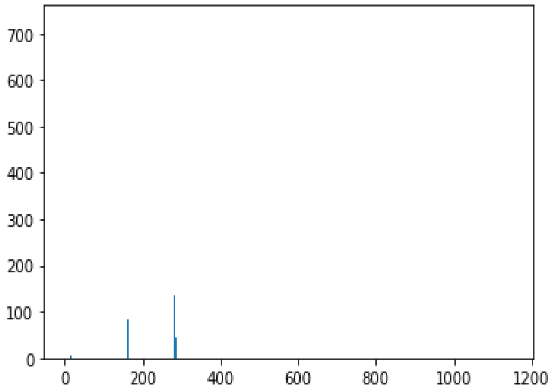


Fig.8.2.1

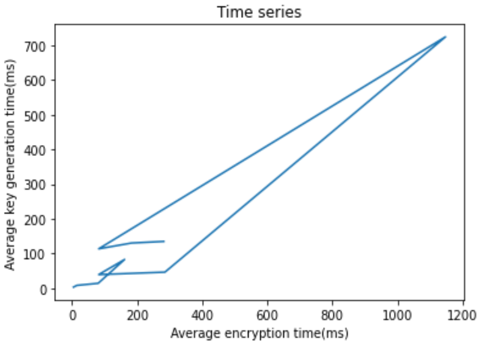


Fig.8.2.2

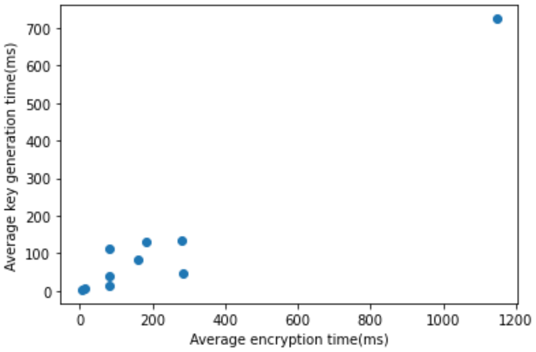


Fig. 8.2.3

CONCLUSION AND FUTURE SCOPE

1. CONCLUSION:

According to our research the future of the IIOT depends on how fast can the gadgets receive and transmit the information and data that has to be further sent to the respective cloud storage that the user possess. Thus, the existing traditional technologies might be less efficient and slow than compared to that of the devices that use the emerging technologies that are capable of transmitting the data securely and faster. As the world leans towards the speed and secure strategies every second to send and receive their data. This proposition might not only be an open door to a new transition but also a secure-efficient way that enables the users to safely trust the system while allowing their data to upload in some of the public cloud storage spaces that are now widely spread diminishing the use of physical storage spaces like hard disks and compatible drives.

2. FUTURE SCOPE:

As the security concerns are seeing a raise day by day the world needs an efficient and secure data transmission that allows them to send their private and confidential data through the cloud storages. The item-level data security can be implemented to the personal clouds as well so that even the cloud service providers cannot access the private data like photos without hesitation. These days we can observe that the private and personal photos that users usually directly upload into the cloud storages are being maliciously used by the third-party cloud service providers. This item-level data protection system if implemented can help the users to save their personal data safely in the cloud storage. As we know the cloud storages are more efficient in a way than compared to the physical storage spaces, we suggest this kind of security that ensures the security to the private and personal data of the users.

REFERENCES

1. Fine-grained access control for big data based on CP-ABE in cloud computing [Yuan, Qi, Changing Ma, and Junyu Lin. "Fine-grained access control for big data based on CP-ABE in cloud computing." International Conference of Young Computer Scientists, Engineers and Educators. Springer, Berlin, Heidelberg, 2015.]
2. An efficient ECC-based CP-ABE scheme for power IoT [Cheng, Rui, et al. "An efficient ECC-based CP-ABE scheme for power IoT." Processes 9.7 (2021): 1176.]
3. User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage [Li, Jiguo, et al. "User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage." IEEE Systems Journal 12.2 (2017): 1767-1777.]
4. Cloud Computing Storage Data Access Control Method Based on Dynamic Re-Encryption [Xiaodan Chen, Desheng Zeng, Shuanglong Pang, Fu Jun, "Cloud Computing Storage Data Access Control Method Based on Dynamic Re-Encryption", Security and Communication Networks, vol. 2021, Article ID 4953074, 10 pages, 2021.]
5. Replacing cryptography with UWB Modulation in secure RFID [Ha, D.S. & Schaumont, P.R. (2007). Replacing Cryptography with Ultra -Wideband (UWB) Modulation in Secure RFID. IEEE

International Conference on RFID. 23 - 29. 10.1109/RFID.2007.346145.]

6. Singamaneni, Kranthi Kumar, et al. "A Novel QKD Approach to Enhance IIOT Privacy and Computational Knacks." Sensors 22.18 (2022): 6741.
7. Singamaneni, Kranthi Kumar, et al. "An Efficient Hybrid QHCP-ABE Model to Improve Cloud Data Integrity and Confidentiality." Electronics 11.21 (2022): 3510.
8. Kranthi Kumar Singamaneni, Abhinav Juneja, Mohammed Abd-Elnaby, Kamal Gulati, Ketan Kotecha, A. P. Senthil Kumar, "An Enhanced Dynamic Nonlinear Polynomial Integrity-Based QHCP-ABE Framework for Big Data Privacy and Security", Security and Communication Networks, vol. 2022, Article ID 4206000, 13 pages, 2022. https://doi.org/10.1155/2022/4206000
9. Kranthi Kumar, S., Ramana, K., Dhiman, G., Singh, S., & Yoon, B. (2021). A Novel Blockchain and Bi-Linear Polynomial-Based QCP-ABE Framework for Privacy and Security over the Complex Cloud Data. Sensors, 21(21), 7300.
10. Singamaneni, Kranthi Kumar, and P. Sanyasi Naidu. "An efficient quantum hash-based CP-ABE framework on cloud storage data." International Journal of Advanced Intelligence Paradigms 22.3-4 (2022): 336-347.
11. Singamaneni, Kranthi Kumar, and Pasala Naidu. "Secure key management in cloud environment using quantum cryptography." Ingénierie des Systèmes d'Information 23.5 (2018).
12. Singamaneni, Kranthi Kumar, and Pasala Sanyasi Naidu. "IBLIND Quantum Computing and HASBE for Secure Cloud Data Storage and Accessing." Rev. d'Intelligence Artif. 33.1 (2019): 33-37.
13. Singamaneni, Kranthi Kumar, Pasala Sanyasi Naidu, and Pasupuleti Venkata Siva Kumar. "Efficient quantum cryptography technique for key distribution." Journal Europeen des Systemes Automatises 51.4-6 (2018): 283.
14. Singamaneni, Kranthi, Abdullah Shawan Alotaibi, and Purnendu Shekhar Pandey. "The Performance Analysis and Security Aspects of Manet." ECS Transactions 107.1 (2022): 10945.
15. Singamaneni, Kranthi Kumar, and Sanyasi Naidu Pasala. "An improved dynamic polynomial integrity based QCP-ABE framework on large cloud data security." International Journal of Knowledge-based and Intelligent Engineering Systems 24.2 (2020): 145-156.
16. Kumar, Singamaneni Kranthi, et al. "Image transformation technique using steganography methods using LWT technique." Traitement du Signalvol 36 (2019): 233-237.
17. RFID technology and its applications in Internet of Things (IoT)[Jia, Xiaolin, et al. "RFID technology and its applications in Internet of Things (IoT)." 2012 2nd

international conference on consumer electronics, communications and networks (CECNet). IEEE, 2012.]

18. A new security and privacy framework for RFID in cloud computing[Kardas, Süleyman, et al. "A new security and privacy framework for RFID in cloud computing." 2013 IEEE 5th international conference on cloud computing technology and science. Vol. 1. IEEE, 2013.]
19. Cloud-based lightweight secure RFID mutual authentication protocol in IoT[Fan, Kai, et al. "Cloud-based lightweight secure RFID mutual authentication protocol in IoT." Information Sciences 527 (2020): 329-340.]
20. Cloud-based remote RFID authentication for security of smart internet of things applications[Ahmed, Mohammed Imtyaz, and G. Kannan. "Cloud-based remote RFID authentication for security of smart internet of things applications." Journal of Information & Knowledge Management 20.supp01 (2021): 2140004.]