CLOUD ASSISTED IOT: AN EFFECTIVE EVALUATION OF DATA ACCESS PROTECTION SCHEME

[1]Dr. P. Sunitha, [2]Bhukya Saritha,[3] Namala Sai Kumar, [4]A Hari Priya
[1]Professor, [2,3]Assistant Professor, [4]Student, [1,2,3,4]Department of Computer Science Engineering , Siddhartha Institute of Engineering and Technology, Hyderabad, India.

ABSTRACT
The Industrial Internet of Things (IIoT) has made it feasible to design industrial systems that leverage digital technologies. Formerly, this was not feasible. Radio-Frequency Identification, or RFID, is a key component of the Industrial Internet of Things (IIoT). It gives industrial participants the capacity to recognize objects and relate IoT time-series data to the objects they recognize. Moreover, they may exchange data from IoT devices through the cloud service, simplifying information sharing and assisting them in making critical production choices. If there were a mechanism to limit who might access Internet of Things data saved in the cloud, you could better safeguard delicate business matters. Traditional cryptographic access control schemes for time-series IoT data have many problems with efficiency and leaking keys when they are used. This is because traditional cryptographic access control schemes were not designed for this type of data. As part ofthis project, you will be required to devise a secure industrial data access control scheme for the Internet of Industrial Things (IIoT) that uses the cloud. Participants in the scheme are granted the ability to utilize ciphertext policy-attribute-based encryption, also known as CP-ABE, to control access to their Internet of Things data in very particular ways. The plan uses a hybrid cloud infrastructure so that participants can confidently delegate time-consuming and resource-intensive CPABE tasks to the cloud service without having to worry about the security of their data. Importantly, the plan provides a new form of data privacy for IoT devices, referred to as "item-level data protection," to solve the issue of key leakage. You can accomplish these objectives with the assistance of several different encryption and optimization strategies. Evaluations of performance incorporate both the actual operation of the system and extensive computer modeling in order to guarantee that the layout is reliable and risk-free.
Keywords: Attribute-based encryption; Ciphertext; Encryption; IIoT.

INTRODUCTION

The Industrial Internet of Things (IIoT) is the term used to describe the use of the Internet of Things (IoT) in an industrial context, such as a business or manufacturing plant [1]. In order to increase an enterprise's productivity in a certain industry, it is able to do this by utilizing the internet infrastructure to link intelligent technology (smart sensors), data collection and storage, and cloud-based analytics [2]. The Internet of Things (IoT) is a system of interconnected, intelligent gadgets that uses the internet to monitor, inform, and enhance several facets of a person's daily life [3]. By the usage of the internet, these gadgets are linked together. It utilizes the same technologies and conceptual frameworks to connect enterprises, individuals, machines, data, and other gadgets in an industrial context to make the entire manufacturing value chain more efficient [4-5]. This is done in order to make the manufacturing process more competitive. For instance, the thermostat in a frozen food delivery truck, the robotic arm on an assembly line, and the pump that brings freshwater to a house are all connected to one another and share data with one another. This enables decisions to be made in real time that are based on accurate data, and it also enables a more effective control of the process that these decisions are a part of [6].

The technology of the Industrial Internet of Things (IIoT) can be used to solve complex problems inthe areas of logistics, manufacturing, and supply chain management, which benefits not only the manufacturer but also the consumer [7-8]. It is a mutually beneficial part of IIoT implementation touse IIoT in a business that already exists. This can reduce operational costs and improve the quality of a wide range of processes in the industry. The Internet has altered how people interact with one another, complete tasks, and collaborate on projects [9]. At this time, people are considering how they might accomplish the same thing with

machines. System developers have been devoting a significant amount of time and energy over the past few years to connecting sensors, edge nodes, and analytics to create intelligent systems [10]. Because of this, operations have become significantly more productive. The Internet of Things in Industry is the name given to all of these interconnected systems (IIoT). This current iteration of the Industrial Revolution is already proving to be the most transformative in the annals of industrial automation [11]. It will have an effect on everything, from manufacturing to healthcare to the energy sector to transportation. Not only is the rate of change accelerating, but so are the leaps in the technologies that underpin it. In the next few years, engineers in every industry will figure out how to use the new capabilities that come from connecting machines and processes with more powerful computing and analytics capabilities. These new capabilities come about due to connecting the machines and processes to the Internet [12-14].

Related Works

As part of 5G, also known as the fifth generation of mobile networks, radio frequency identification tags, also known as RFID tags, are being embedded into an increasing number of personal items, most notably smartphones. Because RFID tags in smartphones frequently disclose personal information about their owners, the authentication protocols used in 5G wireless networks should be anti-scanning and protect users' privacy [15]. On the other hand, the majority of the currently used RFID protocols can be monitored, and distributed denial of service (DDoS) attacks can be carried out against the back-end servers. To eliminate these dangers, we propose that smartphones in 5G networks use a mutual authentication protocol based on a hash [16]. This protocol prevents snooping by dishonest individuals in public areas from gaining access to people's private locations. Because it uses hash values to verify RFID readers, the proposed protocol is a robust defence against the threats described above. In addition, the authentication efficiency of our system on the tag side is 2H, which is superior to the majority of hash-based solutions that have been reported in the past. The tag is only capable -of storingtwo vectors, the first of which contains k bits and the second of which contains j bits [17-18].

This research investigates the localized polling problem that arises in large-scale RFID systems. This problem entails how to most effectively obtain information from wanted tags dM of the total interrogated tags dN when dM and dN are both unknown but all of the tags N, including all of the wanted tags M, have already been collected. This problem is significant in a variety of ways that are relevant to the real world, but it appears that finding a solution to it will be challenging. A brand new polling protocol that we suggest using is called LocP [19]. It is composed of two phases: the phase for filtering tags, and the phase for ordering and reporting. The objective is to cut down on wasted time. During the phase known as Tags-Filtering, LocP applies the Bloom Filter not once but twice in orderto significantly cut down on the number of potential tags. During the phase known as "Ordering and Reporting," the tags make the decision regarding when to send data based on the allocation vectors that the reader repeatedly transmits to the tags. Carry out a great deal of simulations to evaluate the performance of LocP. According to the findings, LocP is very effective in terms of the time it takes to collect information. As a result, it is an attractive possibility for large-scale RFID systems application and scaling up[20].

The authors created attribute-based encryption (ABE), a promising cryptographic primitive used in fine-grained access control systems for encrypted data. Sahai and Waters made ABE. In the key policy version, ciphertexts are annotated with attribute sets, and secret keys are connected to access structures that specify which ciphertexts a user can decrypt [21-30]. Most KP-ABE constructions have the following properties: The cost of decryption is proportional to the number of attributes used during decryption. This article discusses a different way to build KP-ABE[31].The proposed construction is the first KP-ABE algorithm that simultaneously possesses all of the following features:

- It is expressive (that is, it supports any monotonic access structure).
- It is fully secure in the standard model.
- It decrypts quickly.
- It has ciphertexts that are a constant size.

- The problem with our design is that the size of the secret keys is equivalent to the number of attributes multiplied by four.

ABE, which stands for attribute-based encryption, gives users the ability to encrypt and decrypt messages according to the attributes of those messages. In contrast to encryption based on public keys, this method relies on a secret, or private, key. There is a fee associated with making use of this feature. In most implementations, the number of attributes contained in the ciphertext has an effect on both the size of the ciphertext and the amount of time required to decrypt it. The size of the ciphertext grows proportionally with the number of attributes that are included in the ciphertext. In addition, the majority of applications of ABE in the real world call for one pairing operation for each attribute that is utilised during the decryption process. The primary objective of this research is to devise ABE schemes that are equipped with efficient decryption algorithms. It is not necessary for a private key or ciphertext to limit the number of attributes it contains; rather, it is sufficient to ensure that those attributes are not prevented from being utilised by the system as a whole. This scenario provides a demonstration of the first key-policy ABE system, which can decrypt ciphertexts using a set numberof pairings regardless of the length of the ciphertext. If the private key is increased by a factor of ||, then GPSW ciphertexts can be decrypted using only two pairings. This requires the number of distinct attributes contained in the private key to be increased by that same factor. The size of the private key was increased so that it could accommodate this. Then, we present a generalised construction thatgives each individual user of the system the ability to make their own decisions regarding various efficiency tradeoffs along a spectrum, with GPSW on one end and our extremely fast scheme on the other. This standardised building construction. In order to accomplish this tuning, it is not necessary tomake any changes to the encryption algorithm or the parameters that are accessible to the public. When deciding on a particular plan, there are a few things that should be kept in mind in order to ensure the best possible user experience. In the final part of this article, we will go over how theseideas can be applied in the ciphertext-policy ABE setting, albeit at a higher financial cost than was mentioned in the earlier sections.
Switching an encryption key over from one set to another is referred to as rekeying. It brings the security up to date so that keys cannot be taken without permission and dynamic access control can be utilised in cryptographic storage. Effective rekeying in encrypted deduplication storage systems, onthe other hand, is a difficult task. Using deterministic encryption keys, which derive the values of their keys from the contents of ciphertexts, these systems simplify deduplication. REED, a deduplicationand encryption storage system that considers rekeying, is under our design and construction control. Due to REED's use of an all-or-nothing transform, it can perform secure rekeying and deduplication while maintaining a low memory footprint (AONT). Because of REED's determinism, this ability is possible. Each of our REED encryption schemes, which we developed, makes a trade-off between speed and security in order to work. The dynamic access control system has also been integrated into REED. We used a variety of construction methods to improve the REED prototype's functionality. According to our trace-driven testbed evaluation results, our REED prototype has maintained its high performance and ability to effectively utilise storage space.

Existing system

Encryption methods that use the ciphertext policy-attribute (CP-ABE) method are among the most powerful. It's the ideal solution for fine-grained access control. Before sending their data to the cloud service, a participant can set access policies based on logical expressions over the data's attributes. These policies can be used to restrict who can view the data. Each participant is given a secret key by a key authority that corresponds to a particular set of characteristics that best designates the participant. People whose characteristics correspond to the logical expression are the only ones who will be able todecrypt the data if CP-ABE is used. Data that has been encrypted cannot be read by anyone who is not authorized to view it; this includes the cloud storage service.

Disadvantages of Existing System

Even though CP-ABE has been put to extensive use in designing various access control schemes for untrusted clouds, CPABE cannot be used for cloud-aided IIoT because of a few key differences.

- First, the throughput requirements for time-series industrial IoT environment data require a much higher capacity than what CP-ABE can provide. This is because it is an exceptionally costly cryptographic primitive.
- Second, in order to obtain all of the ABE keys from a master key, CP-ABE makes use of a critical authority. The use of a key authority in an IIoT system that makes use of the cloud, on the other hand, creates a significant risk to users' privacy.
- If the key authority is breached, then the data from the entire system's Internet of Things devices will be made public.

Proposed system

For the purpose of this research, we have constructed a reliable and risk-free industrial data access control system by utilising cloud computing.

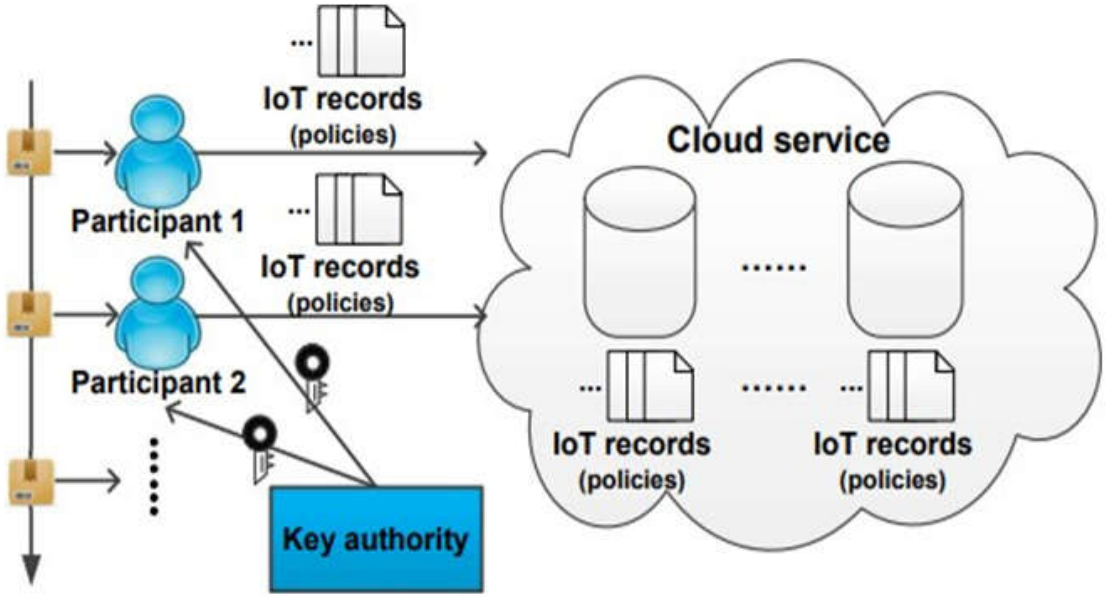

Fig.1. System Architecture

According to our current plans, cloud services will be implemented using a hybrid infrastructure that will consist of both a private cloud and a public cloud. The information that is personally identifiable to users will be saved in a public cloud. CP-ABE tasks that call for a significant amount of resources can be contracted out to a cloud service that offers a substantial amount of storage space. On the encrypted IoT data that is stored in the public cloud, the CP-ABE operations that need to be performed on the encrypted data are the responsibility of the private cloud. We use a system that stores item keys at the item level to protect the data that is collected from IoT devices. Our system now offers a new privacy feature known as "item-level data protection." [Case in point] Even in the event that the integrity of the key authority is violated, only those individuals who were involved in the production of the item will have access to the Internet of Things (IoT) data that is connected to that item.

Advantages of the Proposed System

The protocol makes it possible for the private cloud to carry out CP-ABE encryption and decryption in batches, in addition to CP-ABE re-encryption operations. The plan will effectively double the speed.

System modules

The process of figuring out how an information system should be built, ensuring that it is functional and being used, and ensuring that it meets quality standards, is referred to as systems implementation (i.e., quality assurance).

- Data submission

- Data retrieval
- Policy revisions
- Key management

Key management

The strategy protects the Internet of Things records that are kept in the cloud service by utilising three different kinds of cryptographic keys. The "ik" abbreviation for "item key" refers to the corresponding item. Each participant receives one, which has been embedded with radio frequency identification tags (RFID). Internet of Things records' data keys are encrypted using this method. The item keys that are associated with the records in the IoT provide an additional layer of protection. In the acronym, a group of ABE attributes is linked to an essential SK. All participants have a responsibility to maintain the item and its characteristics provide a glimpse into their personalities. The IoT records can only be accessed by those who have the ABE key in their possession. The letter k identifies the unique datakey for each IoT record it contains. One of the participants generates and stores the Internet of Things record, and symmetric-key encryption is used to ensure the record's integrity and confidentiality (e.g., AES). When an item key and an ABE key are present, a data key is safe.

Data Submission

An ABE-encrypted Internet of Things record can be transmitted to the SSP by a participant using this feature so that it can be shared. After receiving the request, Data-sub will initiate the creation of a CPABE encryption task and will then submit it to the task scheduling framework. This operation can be used by an IoT participant p to send time-series IoT records whenever the participant is processing an item. The user enters p, the item key ik from Item-list, creates a data key k, and then adds the IDX, the time stamp, and the record ID to Record-list as part of the process of submitting an IoT record IDX. This is all part of the submission process for an IoT record IDX. A restrictive access policy Y is in place to safeguard the content m of the IoT record. After that, asymmetric encryption is utilised in order to safeguard both ik and k. The long-term component, denoted by k0, is encrypted first, followedby the temporal component, denoted by k1. The participant then sends a CP-ABE encryption task to the CSP along with the encrypted IoT record (IDX, p, t,,c1, c2) so that it can be decoded. After the IoTrecord (IDX, p, t, C1, C2) has been encrypted with the ABE public key PK by the CSP, it is then encrypted again before being sent to the SSP.

Data Retrieval

This function must be called in order to retrieve an Internet of Things record that was sent by another participant. The CP-ABE decryption task is created as soon as Data-re is in possession of the request, and it is immediately forwarded to the task schedule framework. During the processing of an item, a participant p may make use of this operation in order to obtain time series IoT records from a cloud service. These records will be accessible to the participant designated as p. When participating parties process a batch of n items, such as a participant p, they are able to ask the cloud service for these time series IoT records so that they can continue processing. The other participants are the ones who make these records. The previous action, which included the transmission of data, is going to be undone as a consequence of this action because it involved sending data. CSP is given the instruction to carry out ABE-decryption in order to obtain the n IoT records that were generated at a specific time point t for the batch of items as part of a CP-ABE decryption task. This instruction is given as part of a CP-ABE decryption task.

Reformulation of Policies

Anyone who has access to an Internet of Things record can use this feature to change who else has access to that record. This feature is only available to users who have access to the record. After the request has been received, Policy-up will produce a CPABE re-encryption task and then send it to the task schedule framework for processing. Participants can use this command to change the cloud service users who have

access to the participant's Internet of Things records. Participants can use this command. Using this operation, a participant is able to change the access authority of its n Internet of Things records that were created for an item batch at a given time point. This is possible because the participant has control over the records. Participants are required to provide CSP with a CP-ABE decryption task and instruct it to use ABE in order for this to be successfully completed. Additionally, using CSP, each batch symmetric item needs to be re-encrypted with the participant's new data key and new temporal part. This operation needs to be performed on each individual component of the batch.

Results and Discussions

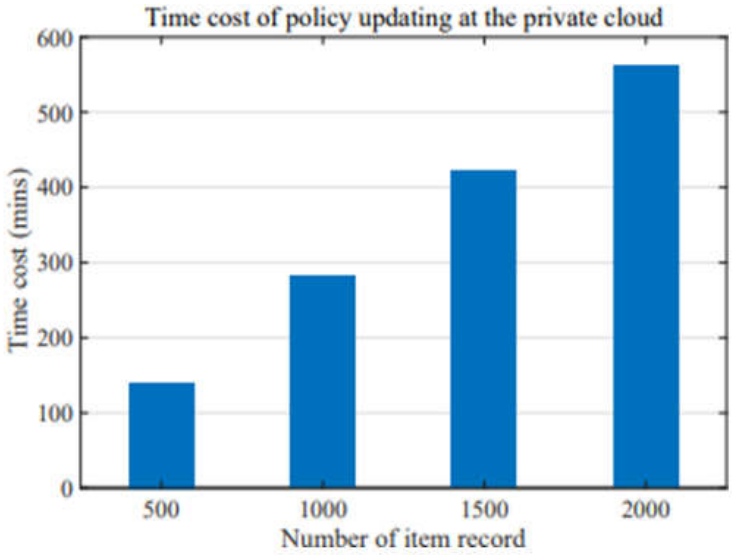

Fig.2. Time cost of csp in policy updating

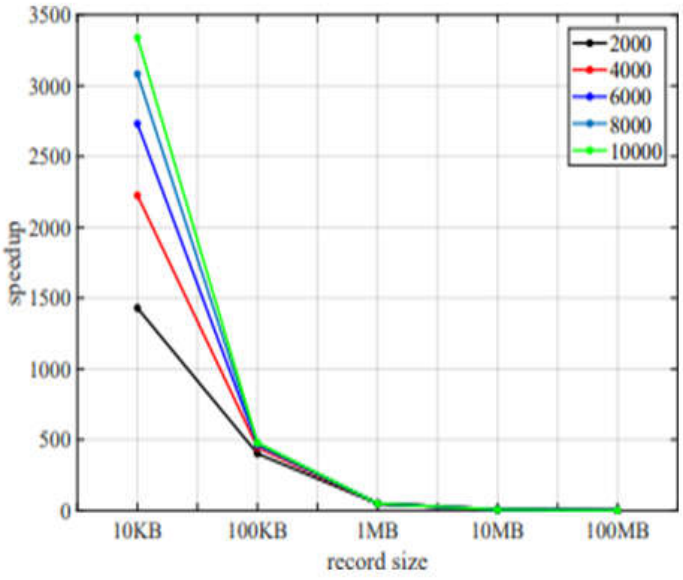

Fig.3. Speedup in data submission

From 500 to 2000 records associated with the IoT, each record will be 1 megabyte in size. For a large number Internet of Things (IoT) records, it takes CSP several hours to complete CP-ABE re- encryption tasks. Because CSP must first obtain these IoT records from SSP, then re-encrypt them,and finally upload them, the process is lengthy. This shows how important it is to improve CSP's operational efficiency.

When the number of records in a batch is relatively low, our optimization achieves a significant speedup ratio, which increases in direct proportion to the number of records in the batch, according to the findings. When the batch size is 2000 and the record size is 10 KB, our optimization makes a difference of at least three orders of magnitude in the speed with which data can be submitted, retrieved, and updated. Our

scalable CP-ABE re-encryption optimization allows us to speed up the policy updating process. This allows us to do so regardless of the size of the IoT records, as the CSP is able to request that the SSP re-encrypt them. This demonstrates that our optimization makes it possible for CSP to perform encryption and decryption tasks in batches for CPABE.

CONCLUSION

A secure industrial data access control scheme that makes use of the cloud to enforce fine-grained access policies and protect data at the item level is required for the Internet of Things (IoT). As part of the plan, which utilizes hybrid cloud technology, a dedicated computing service provider takes care of labor-intensive and financially burdensome access enforcement tasks. These tasks can be burdensome both physically and financially. The data at the item level contained in the item records will be protected by our plan's proposed set of encryption methods, which will also put an end to the problem of key disclosure. In addition to this, it offers a number of suggestions as to how the performance of the computing service provider can be improved while still maintaining the data protection at the item level.

REFERENCES

1. Boyes, Hugh, Bil Hallaq, Joe Cunningham, and Tim Watson. "The industrial internet of things (IIoT): An analysis framework." Computers in industry 101 (2018): 1-12.
2. Kumar, K. Suresh, T. Ananth Kumar, A. S. Radhamani, and S. Sundaresan. "Blockchain Technology: An Insight into Architecture, Use Cases, and Its Application with Industrial IoT and Big Data." In Blockchain Technology, pp. 23-42. CRC Press, 2020.
3. Singh, Sachchidanand, and Nirmala Singh. "Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce." In 2015 International conference on green computing and internet of things (ICGCIoT), pp. 1577-1581. Ieee, 2015.
4. Kumar, T. Ananth, A. John, and C. Ramesh Kumar. "2. IoT technology and applications." Internet of Things 43 (2020).
5. Sheth, Amit, Utkarshani Jaimini, and Hong Yung Yip. "How will the internet of things enable augmented personalized health?." IEEE intelligent systems 33, no. 1 (2018): 89-97.
6. Manju Bala, P., S. Usharani, T. Ananth Kumar, R. Rajmohan, and M. Pavithra. "Blockchain-Based IoT Architecture for Software-Defined Networking." In Blockchain, Artificial Intelligence, and the Internet of Things, pp. 91-115. Springer, Cham, 2022.
7. Das, Amardeep, Sumanta Chandra Mishra Sharma, and Bikram Kesari Ratha. "The new era of smart cities, from the perspective of the internet of things." In Smart cities cybersecurity and privacy, pp. 1-9. Elsevier, 2019.
8. Kumar, K. Suresh, T. Ananth Kumar, S. Sundaresan, and V. Kishore Kumar. "Green IoT for Sustainable Growth and Energy Management in Smart Cities." In Handbook of Green Engineering Technologies for Sustainable Smart Cities, pp. 155-172. CRC Press, 2021.
9. Waizenegger, Lena, Brad McKenna, Wenjie Cai, and Taino Bendz. "An affordance perspective of team collaboration and enforced working from home during COVID-19." European Journal of Information Systems 29, no. 4 (2020): 429-442.
10. Devi, A., M. Julie Therese, P. Dharani Devi, and T. Ananth Kumar. "IoT-Based Smart Pipeline Leakage Detecting System for Petroleum Industries." In Industry 4.0 Interoperability, Analytics, Security, and Case Studies, pp. 149-168. CRC Press, 2021.
11. Kumar, K. Suresh, AS Radha Mani, S. Sundaresan, T. Ananth Kumar, and Y. Harold Robinson. "Blockchain-based energy-efficient smart green city in IoT environments." In Blockchain for Smart Cities, pp. 81-103. Elsevier, 2021.
12. Karniadakis, George Em, Ioannis G. Kevrekidis, Lu Lu, Paris Perdikaris, Sifan Wang, and Liu Yang. "Physics-informed machine learning." Nature Reviews Physics 3, no. 6 (2021): 422-440.
13. Bala, P. Manju, S. Usharani, T. Ananth Kumar, R. Rajmohan, and M. Pavithra. "Blockchain-Based

IoT Architecture for Software-Defined Networking." Blockchain, Artificial Intelligence, and the Internet of Things: Possibilities and Opportunities: 91.
14. Ghosh, Ashish, Debasrita Chakraborty, and Anwesha Law. "Artificial intelligence in Internet of things." CAAI Transactions on Intelligence Technology 3, no. 4 (2018): 208-218.
15. Bagay, Dmitry. "Information security of RFID tags." Procedia Computer Science 169 (2020): 183-186.
16. Arumugam, Devi, Kavya Govindaraju, and Ananth Kumar Tamilarasan. "AIIoT-Based Smart Framework for Screening Specific Learning Disabilities." In Machine Learning for Critical Internet of Medical Things, pp. 103-124. Springer, Cham, 2022.
17. Kumar, T. Deva, TS Arun Samuel, and T. Ananth Kumar. "Transforming 2 Green Cities with IoT." Handbook of Green Engineering Technologies for Sustainable Smart Cities (2021): 17.
18. Selvi, S. Arunmozhi, T. Ananth Kumar, and R. S. Rajesh. "CCNN: A Deep Learning Approach for an Acute Neurocutaneous Syndrome via Cloud-Based MRI Images." In Handbook of Deep Learning in Biomedical Engineering and Health Informatics, pp. 83-102. Apple Academic Press, 2021.
19. Yang, Fangfei, Ming Tang, and Ozgur Sinanoglu. "Stripped functionality logic locking with Hamming distance-based restore unit (SFLL-hd)–unlocked." IEEE Transactions on Information Forensics and Security 14, no. 10 (2019): 2778-2786.
20. Suryaganesh, M., T. S. Arun Samuel, T. Ananth Kumar, and M. Navaneetha Velammal. "Advanced FET-Based Biosensors—A Detailed Review." Contemporary Issues in Communication, Cloud and Big Data Analytics (2022): 273-284.
21. Kwong, Andrew, Daniel Genkin, Daniel Gruss, and Yuval Yarom. "Rambleed: Reading bits in memory without accessing them." In 2020 IEEE Symposium on Security and Privacy (SP), pp. 695-711. IEEE, 2020.
22. Pugazhendiran, P., K. Suresh Kumar, T. Ananth Kumar, and S. Sundaresan. "An Advanced Revealing and Classification System for Plant Illnesses Using Unsupervised Bayesian-based SVM Classifier and Modified HOG-ROI Algorithm." In Contemporary Issues in Communication, Cloud andBig Data Analytics, pp. 259-269. Springer, Singapore, 2022.
23. Nayyar Ahmed Khan, ―Cloud Applications Development and Deployment: The Future of Cost Effective Programming and a Step Ahead‖, Middle East Journal of Applied Science & Technology, Volume 1, Issue 1, Pages 30-36, October - December 2018.
24. Nayyar Ahmed Khan, ―Design and Verification of Cache Coherence Protocol‖, Middle East Journal of Applied Science & Technology, Volume 2, Issue 1, Pages 01-10, January - March 2019.
25. Nayyar Ahmed Khan, ―Security Management Protocols in Cloud Computation‖, Middle East Journal of Applied Science & Technology, Volume 2, Issue 1, Pages 16-23, January - March 2019.
26. Prince Kelvin Owusu, ―Smart Garbage Monitoring System using Internet of Things‖, Middle East Journal of Applied Science & Technology, Vol.3, Iss.2, Pages 74-82, April-June 2020.
27. Mohd Meraj Ahemad, Iqbal Ahmad, Dr. Javed Ashraf, Dr. Safdar Tanweer & Dr. Anisur Rehman Nasir, ―Applications of Artificial Intelligence in Human Life‖, Middle East Journal of Applied Science & Technology, Vol.3, Iss.3, Pages 28-38, July-September 2020.
28. Stefano Farné, Francesco Benzi & Ezio Bassi, ―IIOT based efficiency optimization in logistics applications‖ Asian Journal of Basic Science & Research, Volume 2, Issue 4, Pages 59-73, DOI: http://doi.org/10.38177/AJBSR.2020.2406.
29. Nayyar Ahmed Khan, Ahmed Masih Uddin Siddiqi & Mohammad Ahmad, ―Development of intelligent alumni management system for universities‖, Asian Journal of Basic Science & Research, Volume 3, Issue 2, Pages 51-60, DOI: http://doi.org/10.38177/AJBSR.2021.3206.
30. Mercat, Alexandre, Marko Viitanen, and Jarno Vanne. "UVG dataset: 50/120fps 4K sequences for video codec analysis and development." In Proceedings of the 11th ACM Multimedia Systems Conference, pp. 297-302. 2020.
31. Acharya, Jayadev, Ziteng Sun, and Huanyu Zhang. "Hadamard response: Estimating distributions

privately, efficiently, and with little communication." In The 22nd International Conference on Artificial Intelligence and Statistics, pp. 1120-1129. PMLR, 2019.