A SUCCESSFUL EVALUATION OF A DATA ACCESS CONTROL SCHEME USING IIOT ASSISTED BY THE CLOUD

P. Mohan, Dept of Computer Science and Engineering, Sree Venkateswara College Of Engineering, Nellore (Dt), Andhra Pradesh, India.

R. Prapulla Kumar, Dept of Computer Science and Engineering, Sree Venkateswara College Of Engineering, Nellore (Dt), Andhra Pradesh, India.

Modem. Jeevan Kumar, Dept of Computer Science and Engineering, Sree Venkateswara College Of Engineering, Nellore (Dt), Andhra Pradesh, India.

K.Harshavardhan Reddy, Dept of Electronics and Communication Engineering, Sree Venkateswara College Of Engineering, Nellore (Dt), Andhra Pradesh, India.

ABSTRACT

Designing industrial systems that make use of digital technology is now possible thanks to the Industrial Internet of Things (IIoT). Previously, this was not practical. The Industrial Internet of Things, sometimes known as RFID, is a crucial part of the IIoT. It enables industrial participants to identify things and link IoT time-series data to the recognised objects. Additionally, by using the cloud service, they can exchange data from IoT devices, simplifying information sharing and assisting them in making crucial production decisions. You could more effectively protect sensitive business affairs if there were a way to restrict who could access Internet of Things data stored in the cloud.. For time-series IoT data, traditional cryptographic access control schemes have many issues with efficiency and key leakage. This is because this kind of data was not intended to be used with conventional cryptographic access control systems. You will be expected to develop a secure industrial data access control system for the cloud-based Internet of Industrial Things (IIoT) as part of this project. Participants in the scheme are given the opportunity to restrict access to their Internet of Things data in very specific ways using ciphertext policy-attribute-based encryption, or CP-ABE.The strategy makes use of a hybrid cloud infrastructure so that users may confidently trust the cloud service with time-consuming and resource-intensive CPABE chores without worrying about the security of their data. Importantly, the plan addresses the problem of key leakage by introducing a new type of data privacy for IoT devices, known as "item-level data protection." With the use of a number of various encryption and optimisation techniques, you can achieve these goals. To ensure that the design is trustworthy and risk-free, performance evaluations take into account both the system's real operation and in-depth computer modelling.

Keywords: Attribute –based encryption; Cipher text Encryption; IIoT.

1. INTRODUCTION

The use of the Internet of Things (IoT) in an industrial context, such as a corporation or manufacturing plant, is referred to as the Industrial Internet of Things (IIoT) [1]. By using the internet infrastructure to connect intelligent technologies (smart sensors), data collecting and storage, and cloud-based analytics, an organisation is able to boost productivity in a particular industry [2]. The Internet of Things (IoT) is a network of intelligent, networked devices that can monitor, inform, and improve various aspects of a person's everyday life [3]. These devices are connected to one another over the internet. It connects businesses, people, machines, data, and other devices in an industrial setting using the same technologies and conceptual frameworks to increase the efficiency of the entire manufacturing value chain [4-5]. To increase the manufacturing process's competitiveness, this is done. For instance, the robotic arm on a manufacturing line, the thermostat in a frozen food delivery truck, and the pump that supplies fresh water to a home are all interconnected and exchange data with one another. As a result, reliable data-based decisions may be made in real time, and the process they are a part of can be controlled more successfully [6]. The Industrial

Internet of Things (IIoT) technology can be used to address challenging issues in supply chain management, manufacturing, and logistics, which helps both the producer and the consumer [7-8]. Utilising IIoT in an existing business is a mutually beneficial component of IIoT implementation. This can save operating expenses and raise the standard of a variety of commercial processes. The way people connect with one another, complete jobs, and work together on projects has changed as a result of the internet [9]. People are currently thinking about how they could achieve the same goal using machines. Over the past few years, system developers have spent a lot of time and effort connecting sensors, edge nodes, and analytics to create intelligent systems [10]. Operations are now much more productive as a result. All of these interconnected systems are together referred to as the Industrial Internet of Things (IIoT). In the history of industrial automation, this current iteration of the Industrial Revolution is already proving to be the most transformative [11]. Everything will be impacted, including manufacturing, healthcare, the energy industry, and transportation. Both the pace of change and the advancements in the enabling technologies are quickening. In the next few years, engineers in every industry willfigure out how to use the new capabilities that come from connecting machines and processes with more powerful computing and analytics capabilities. These new possibilities are the result of connecting processes and devices to the Internet [12–14].

2. Related Works

Radio frequency identification tags, often known as RFID tags, are being included into an increasing number of personal items, most notably smartphones, as part of 5G, also known as the fifth generation of mobile networks. The authentication techniques used in 5G wireless networks should be anti-scanning and preserve users' privacy because RFID chips in smartphones regularly leak personal information about their owners [15]. On the other hand, most of the RFID protocols currently in use are monitorable, and back-end servers are vulnerable to distributed denial of service (DDoS) assaults. We suggest that smartphones in 5G networks employ a mutual authentication system based on a hash [16] to eliminate these risks. This protocol stops snooping in public places by dishonest persons from getting access to people's private places. The suggested protocol is a strong deterrent against the dangers mentioned above since it employs hash values to verify RFID readers. Additionally, our system's tag-side authentication efficiency is 2H, which is higher than the vast majority of hash-based solutions that have previously been reported. Only two vectors, the first of which contains k bits and the second of which contains j bits, can be stored by the tag [17–18].

This study looks into the localised polling issue that occurs in massive RFID systems.. When dM and dN are both unknown but all of the tags N, including all of the wanted tags M, have previously been gathered, the challenge involves how to most efficiently acquire information from wanted tags dM of the total interrogated tags dN. There are many important aspects of this issue that are applicable to the actual world, but it seems difficult to find a solution. We recommend utilising LocP, a brand-new polling protocol [19]. The phase for filtering tags and the phase for arranging and reporting make up this process. The goal is to reduce time that is wasted. LocP applies the Bloom Filter twice during the Tags-Filtering step in order to considerably reduce the amount of candidate tags. The tags choose when to submit data during the "Ordering and Reporting" phase based on the allocation vectors that the reader continuously sends to the tags. Perform a large number of simulations to gauge LocP's effectiveness. The results show that LocP is quite efficient in terms of information gathering time. As a result, it is a desirable option for the use and expansion of large-scale RFID systems[20].

Attribute-based encryption (ABE), a promising cryptographic primitive utilised in precise access control systems for encrypted data, was developed by the authors. Waters and Sahai created ABE. The key policy version annotates ciphertexts with attribute sets and connects secret keys to access structures that define which ciphertexts a user is allowed to decipher [21–30]. The majority of KP-ABE buildings share the following characteristics: The number of attributes used during decryption affects how much it costs. This article discusses an alternative method for creating 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 cipher texts that are a constant size.
- The problem with our design is that the size of the secret keys is equivalent to the number of attribute smultiplied by four.

Users can encrypt and decode messages based on the qualities of those messages using attribute-based encryption, or ABE for short. This kind of encryption relies on a secret, or private, key, as opposed to encryption based on public keys. The use of this function is subject to a cost. In the majority of implementations, the quantity of attributes in the ciphertext affects both its size and the length of time needed to decrypt it. The amount of features that are included in the ciphertext increases in direct proportion to its size. Additionally, the majority of ABE's real-world applications demand one pairing operation for each attribute used in the decryption process. The main goal of this research is to design ABE schemes with effective decryption algorithms. It suffices to verify that those attributes can be used by the system as a whole rather than requiring a private key or ciphertext to contain a certain minimum number of attributes. The first key-policy ABE system, which can decipher ciphertexts using a predetermined number of pairings regardless of the length of the ciphertext, is demonstrated in this case. GPSW ciphertexts can be deciphered with just two pairings if the private key is increased by a factor of ||.

This necessitates a corresponding increase in the number of unique features in the private key. This required expanding the private key's size to account for it. Then, we present a generalised construction that enables each system user to choose their own efficiency tradeoffs along a spectrum, with GPSW on one end and our incredibly fast scheme on the other, with our fast scheme being at the other end. This standardised the building process. It is not essential to alter the encryption technique or the settings that are visible to the general public in order to complete this tuning.There are a few considerations that should be made while choosing a certain plan to guarantee the greatest user experience. We shall discuss how these concepts can be used in the ciphertext-policy ABE scenario in the article's concluding section, but at a higher cost than was discussed in the preceding sections.

Rekeying is the process of switching an encryption key from one set to another. It updates the security so that dynamic access control can be used in cryptographic storage and that keys cannot be taken without authorization. However, it is challenging to rekey effectively in encrypted deduplication storage systems.

These systems streamline deduplication by employing deterministic encryption keys, which generate the values of their keys from the contents of ciphertexts. We were in charge of the design and development of REED, a deduplication and encryption storage system that takes rekeying into account. REED can accomplish secure rekeying and deduplication while retaining a small memory footprint (AONT) since it uses an all-or-nothing transform. This ability is made feasible by REED's determinism. Each of the REED encryption algorithms we created compromises security for speed in order to function. Incorporated into REED is also the dynamic access control system. To increase the functionality of the REED prototype, we employed a number of construction techniques. According to our trace-driven test bed evaluation results, our REED prototype has maintained its high performance and ability to effectively utilize storage space.

2. Existing system

The cipher text policy-attribute (CP-ABE) method of encryption is one of the most potent ones. For precise access control, it is the best option. A participant can create access policies based on logical expressions over the properties of their data before delivering it to the cloud service. These guidelines can be used to limit who has access to the data. A secret key that corresponds to a certain collection of traits that best describes each participant is handed to them by a key authority. If CP-ABE is utilized, the only people who can decode the data are those whose traits match the logical expression. 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 muchhighercapacitythanwhatCP-ABEcanprovide.Thisisbecauseitisanexceptionallycostlycryptographicprimitive.
- 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, createsa 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.

3. Proposed system

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

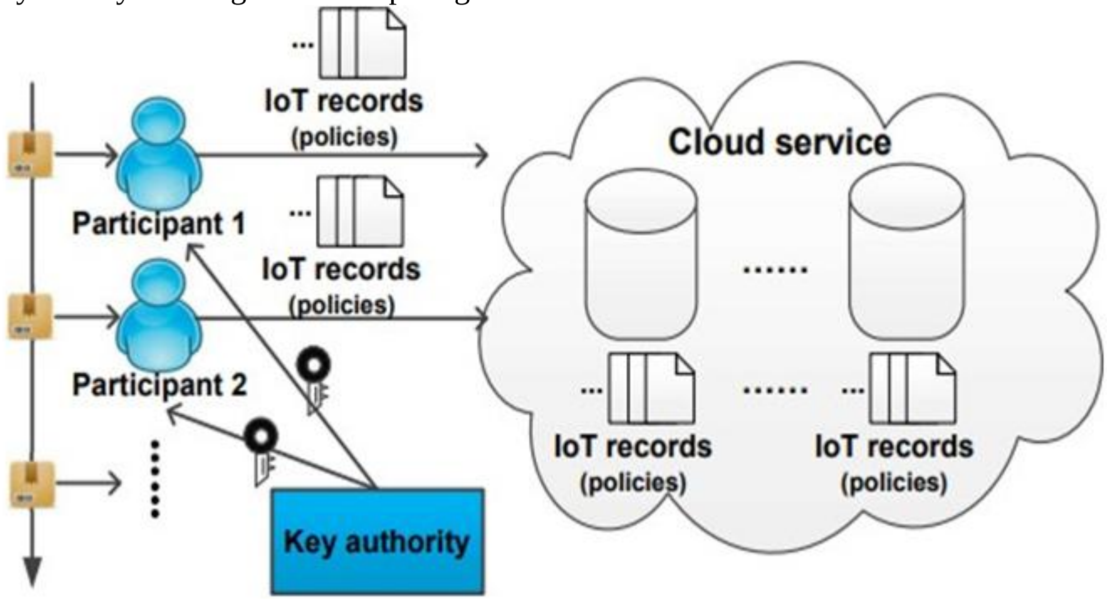

Fig.1.SystemArchitecture

Our current plans call for a hybrid infrastructure that combines a private cloud and a public cloud to implement cloud services. Users' personally identifiable information will be stored in a public cloud. Contracting out CP-ABE processes that require a big number of resources to a cloud provider that provides a significant quantity of storage space is an option. The private cloud is in charge of performing the CP-ABE procedures that must be done on the encrypted IoT data that is kept in the public cloud. To safeguard the information gathered from IoT devices, we employ a system that saves item keys at the item level.. Our system now offers a new privacy feature known as "item-level data protection." [Case in point] Even in the event that Only those people who were involved in the manufacture of the item will have access to the Internet of Things (IoT) data that is related to that item because the key authority's integrity has been compromised.

Advantages of the Proposed System

The protocol enables CP-ABE encryption and decryption operations in batches, in addition to CP-ABE re-encryption operations, in the private cloud.The strategy will actually quadruple the speed.

System modules

The process of figuring out how an information system should be built, ensuring that it is function a land 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

The plan uses three distinct types of cryptographic keys to protect the Internet of Things data that is stored in the cloud service. The matching item is indicated by the "ik" abbreviation for "item key". Each participant receives one that has RFID (radio frequency identification) tags built in. Data keys for Internet of Things records are encrypted in this way. An additional layer of security is offered by the item keys connected to the records in the IoT. An important SK is connected to a group of ABE qualities in the acronym. Each member is responsible for maintaining the object, and its features reveal something about their personality. Only individuals who have the ABE key in their hands are able to access the IoT records. Each IoT record it contains has a unique data key identified by the letter k. The Internet of Things record is created and stored by one of the participants, and symmetric-key encryption, such as AES, is used to preserve the secrecy and integrity of the record. A data key is secure when both an item key and an ABE key are present.

Data Submission

This feature allows a participant to send an ABE-encrypted Internet of Things record to the SSP for sharing. Following receipt of the request, Data-sub will start the CPABE encryption task creation process before submitting it to the task scheduling framework. An IoT participant p can use this action to submit time-series IoT records anytime the participant is handling an object. In order to submit an IoT record IDX, the user must first enter p, the item key ik from Item-list, construct a data key k, and then add the IDX, the time stamp, and the record ID to Record-list. All of this is a component of the IoT record IDX submission procedure. The IoT record's content is protected by a limiting access policy, or Y. Following that, asymmetric encryption is used to protect both ik and k. The temporal component, represented by k1, is then encrypted after the long-term component, marked by k0. The participant then delivers the encrypted IoT record (IDX, p, t,,c1, c2) and a CP-ABE encryption task to the CSP for decoding. The CSP encrypts the IoT record (IDX, p, t, C1, C2) using the ABE public key PK, and then encrypts it once again before sending it to the SSP.

Data Retrieval

To obtain an Internet of Things record that was sent by another participant, this function must be called. As soon as Data-re has the request, the CP-ABE decryption task is produced and sent right away to the task schedule system. A participant p may use this operation to access time series IoT records from a cloud service while processing an item. The person identified as p will have access to these records. In order to continue processing a batch of n items, such as a participant p, participating parties might ask the cloud service for these time series IoT recordings. These records are created by the other participants. The prior action, which involved sending data, will be reversed as a result of this action as it also required sending data. CSP is instructed to do ABE-decryption in order to get the n IoT records that were produced for the batch of objects at a particular time point t as part of a CP-ABE decryption task. This directive is provided as a requirement for a CP-ABE decryption task.

Reformulation of Policies

This feature allows anyone with access to an Internet of Things record to modify who else has access to that record. Users who have access to the record are the only ones who can use this feature. The CPABE re-encryption job will be created by Policy-up when the request has been received, and it will be sent to the task scheduling framework to be processed. This command allows users to modify the users of the cloud service who have access to their Internet of Things records.

4. Results and Discussions

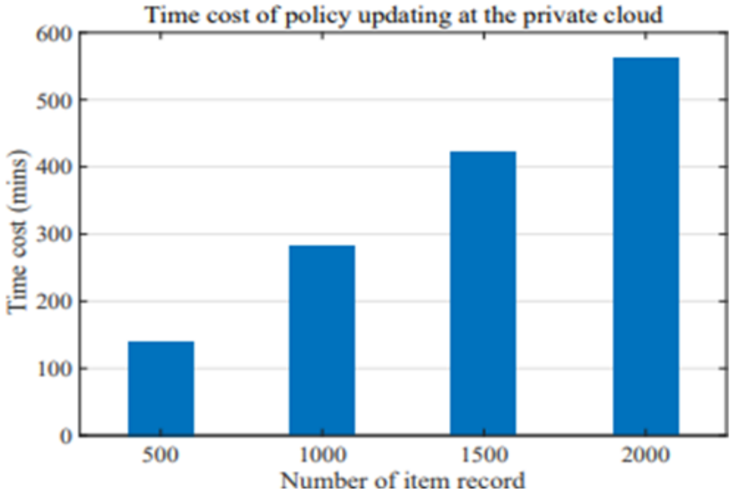

Fig.2.Timecost of policy updating

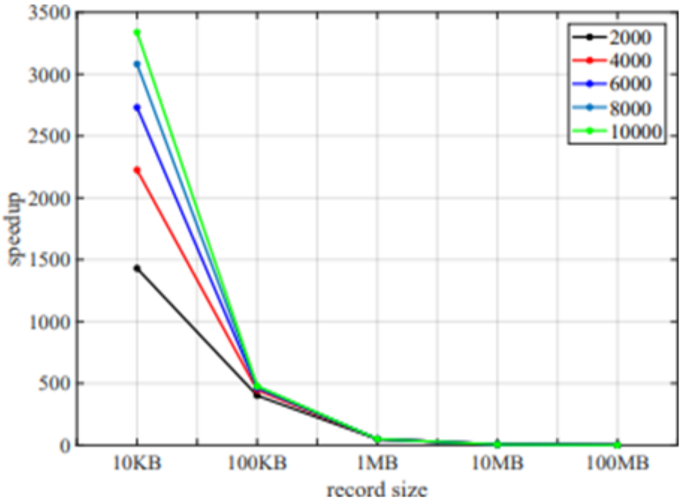

Fig.3.Speed up in data submission

Each IoT record will be between 500 and 2000 bytes long and have a size of 1 megabyte. The CP-ABE re-encryption process takes CSP many hours to complete for a significant quantity of Internet of Things (IoT) records. The method is time-consuming since CSP must first get these IoT records from SSP, re-encrypt them, and then upload them. This demonstrates how critical it is to increase the operational effectiveness of CSP. The results show that while the number of records in a batch is relatively small, our optimisation achieves a large speedup ratio, which rises in direct proportion to the batch size. Our optimisation significantly improves the speed at which data can be submitted, retrieved, and updated when the batch size is 2000 and the record size is 10 KB. We accelerate the policy update procedure using our scalable CP-ABE re-encryption optimisation. Due to the CSP's ability to ask the SSP to re-encrypt the IoT records, we are able to do this regardless of the size of the records. This indicates that our optimisation enables CSP to execute encryption and decryption operations for CPABE in batches.

CONCLUSION

For the Internet of Things (IoT), a secure industrial data access management system that uses the cloud to enforce fine-grained access controls and protect data at the item level is necessary. The strategy, which makes use of hybrid cloud technologies, assigns labor-intensive and expensive access enforcement activities to a dedicated computer service provider. These tasks may be physically and financially taxing. The data at the item level contained in the item records will be secure thanks to the suggested set of encryption algorithms in our approach, which will also address the key disclosure problem. Additionally, it offers a number of suggestions for how to boost computing service provider performance while still maintaining item-level data protection.

REFERENCES

1. Boyes, Hugh, Bil Hallaq, Joe Cunningham, and Tim Watson. "The industrial internet of things(IIoT): An analysisframework."Computersinindustry101(2018):1-12.
2. Kumar,K.Suresh,T.AnanthKumar,A.S.Radhamani,andS.Sundaresan."BlockchainTechnology: An Insight into Architecture, Use Cases, and Its Application with Industrial IoT and BigData." In Blockchain Technology,pp. 23-42. CRCPress, 2020.
3. Singh, Sachchidanand, and Nirmala Singh. "Internet of Things (IoT): Security challenges, businessopportunities & reference architecture for E-commerce." In 2015 International conference on greencomputingand internetofthings (ICGCIoT), pp.1577-1581.Ieee, 2015.
4. Kumar, T. Ananth, A. John, and C. Ramesh Kumar. "2. IoT technology and applications." Internetof Things 43 (2020).
5. Sheth, Amit, Utkarshani Jaimini, and Hong Yung Yip. "How will the internet of things enableaugmentedpersonalized health?."IEEEintelligentsystems33,no.1 (2018): 89-97.
6. Manju Bala, P., S. Usharani, T. Ananth Kumar, R. Rajmohan, and M. Pavithra. "Blockchain-BasedIoT Architecture for Software-Defined Networking." In Blockchain, Artificial Intelligence, and theInternet ofThings, pp. 91-115. Springer, Cham, 2022.
7. Das, Amardeep, Sumanta Chandra Mishra Sharma, and Bikram Kesari Ratha. "The new era ofsmart 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 forSustainable Growth and Energy Management in Smart Cities." In Handbook of Green EngineeringTechnologiesfor Sustainable SmartCities, pp. 155-172. CRCPress,2021.
9. Waizenegger, Lena, Brad McKenna, Wenjie Cai, and Taino Bendz. "An affordance perspective ofteamcollaborationandenforcedworkingfromhomeduringCOVID-19."EuropeanJournalofInformationSystems 29, no. 4 (2020):429-442.
10. Devi, A., M. Julie Therese, P. Dharani Devi, and T. Ananth Kumar. "IoT-Based Smart PipelineLeakageDetectingSystemforPetroleumIndustries."In Industry4.0Interoperability,Analytics,Security, and Case Studies,pp. 149-168. CRCPress,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 SmartCities,pp. 81-103. Elsevier, 2021.
12. Karniadakis, George Em, Ioannis G. Kevrekidis, Lu Lu, Paris Perdikaris, Sifan Wang, and LiuYang."Physics-informedmachinelearning."NatureReviewsPhysics3,no.6(2021): 422-440.
13. Bala, P. Manju, S. Usharani, T. Ananth Kumar, R. Rajmohan, and M. Pavithra. "Blockchain-BasedIoTArchitectureforSoftware-DefinedNetworking."Blockchain,ArtificialIntelligence,andtheInternet ofThings:Possibilitiesand Opportunities:91.
14. Ghosh, Ashish, Debasrita Chakraborty, and Anwesha Law. "Artificial intelligence in Internet ofthings." CAAI Transactionson IntelligenceTechnology 3, no. 4(2018):208-218.
15. Bagay, Dmitry. "Information security of RFID tags." Procedia Computer Science 169 (2020): 183-186.

16. Arumugam,Devi,KavyaGovindaraju,andAnanthKumarTamilarasan."AIIoT-BasedSmartFramework for Screening Specific Learning Disabilities." In Machine Learning for Critical Internet ofMedicalThings, pp. 103-124. Springer, Cham, 2022.
17. Kumar,T.Deva,TSArunSamuel,andT.AnanthKumar."Transforming2GreenCitieswithIoT." HandbookofGreenEngineeringTechnologiesforSustainableSmartCities(2021): 17.
18. Selvi, S. Arunmozhi, T. Ananth Kumar, and R. S. Rajesh. "CCNN: A Deep Learning Approach foran Acute Neurocutaneous Syndromevia Cloud-Based MRI Images." In Handbook of Deep LearninginBiomedicalEngineeringandHealthInformatics, pp.83-102. Apple AcademicPress, 2021.
19. Yang,Fangfei,MingTang,andOzgurSinanoglu."StrippedfunctionalitylogiclockingwithHammingdistance-basedrestoreunit(SFLL-hd)–unlocked." IEEETransactionsonInformationForensicsand Security14,no. 10 (2019):2778-2786.
20. Suryaganesh,M.,T.S.ArunSamuel,T.AnanthKumar,andM.NavaneethaVelammal."Advanced FET-Based Biosensors—A Detailed Review." Contemporary Issues in Communication,CloudandBig Data Analytics(2022):273-284.
21. Kwong, Andrew, Daniel Genkin, Daniel Gruss, and Yuval Yarom. "Rambleed: Reading bits inmemory without accessing them." In 2020 IEEE Symposium on Security and Privacy (SP), pp. 695-711. IEEE,2020.
22. Pugazhendiran,P.,K.SureshKumar,T.AnanthKumar,andS.Sundaresan."AnAdvancedRevealingandClassificationSystemforPlantIllnessesUsingUnsupervisedBayesian-basedSVM Classifier and Modified HOG-ROI Algorithm." In Contemporary Issues in Communication, Cloud andBigData Analytics,pp. 259-269. Springer, Singapore,2022.
23. Nayyar Ahmed Khan, ―Cloud Applications Development and Deployment: The Future of CostEffective Programming and a Step Ahead‖, Middle East Journal of Applied Science & Technology,Volume1, Issue 1, Pages 30-36, October-December2018.
24. NayyarAhmed Khan, ―Design and Verification of Cache Coherence Protocol‖, Middle EastJournal ofApplied Science&Technology,Volume2, Issue1,Pages01-10, January-March 2019.
25. Nayyar Ahmed Khan, ―Security Management Protocols in Cloud Computation‖, Middle EastJournal ofApplied Science&Technology,Volume2, Issue1,Pages16-23, January-March 2019.
26. Prince Kelvin Owusu, ―Smart Garbage Monitoring System using Internet of Things‖, Middle EastJournal of AppliedScience&Technology, Vol.3,Iss.2, Pages74-82, April-June2020.
27. Mohd Meraj Ahemad, Iqbal Ahmad, Dr. Javed Ashraf, Dr. Safdar Tanweer & Dr. Anisur RehmanNasir,―ApplicationsofArtificialIntelligence in HumanLife‖, MiddleEast JournalofAppliedScience&Technology, Vol.3, Iss.3, Pages 28-38,July-September2020.
28. Stefano Farné, Francesco Benzi & Ezio Bassi, ―IIOT based efficiency optimization in logisticsapplications‖ 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 ofintelligent alumni management system for universities‖, Asian Journal of Basic Science & Research,Volume3, Issue2, Pages51-60, DOI: http://doi.org/10.38177/AJBSR.2021.3206.
30. Mercat, Alexandre, Marko Viitanen, and Jarno Vanne. "UVG dataset: 50/120fps 4K sequences forvideocodecanalysisanddevelopment."In Proceedingsofthe11thACMMultimediaSystemsConference,pp. 297-302. 2020.
31. Acharya, Jayadev, Ziteng Sun, and Huanyu Zhang. "Hadamard response: Estimating distributionsprivately,efficiently,andwithlittlecommunication."In The22ndInternationalConferenceonArtificialIntelligenceand Statistics, pp.1120-1129. PMLR, 2019.