Secure Agent Interaction System for Monitoring Industrial IoT Classification using Attribute Selection

Nusrat Hamid Shah[1], Anne Anoop[2], Laila Fhaid bin Libdah[3], Lubna Hamid Shah[4]

[1,2,3] *College of Computer Science and Information Technology, Jazan University, Jazan, Saudi Arabia.*
[4] *College of Business Administration, Jazan University, Jazan, Saudi Arabia, ORCID: 0000-0003-2614-7644*

[1]snusrt01@gmail.com

Abstract - ***Many industries appreciate manufacturing, food, drink and transportation have recently shown increasing interest within the Industrial Internet of Things to achieve a competitive advantage. IoT could be a set of technologies that brings along the Internet of Things, computing devices, components and sanctionative intelligent business transformation through advanced huge knowledge analytics. The demand and increasing complexness of IIoT with large-scale interconnection deployment, internet access management and service offered of IIoT objects such as compute, network, users or servers are getting imperative requirements. In this paper, we propose a SecIIoT sensible annotated information authorization system for monitoring IIoT objects. It connected via two-dimensional with big processing with a versatile and economical authorization model to fulfil the new IIoT security needs. To demonstrate the quality of the planned structure, an image with take a look at results is implemented. The experiment results are showed that the connected authorization model works effectively in an exceedingly large-scale readying per the new IIoT security requirements.***

Keywords *- Industrial Internet of Things, Agent Interaction System, Classification, Securing Objects, Attribute Selection*

DOI Number: 10.48047/nq.2022.20.19.NQ99123 NeuroQuantology2022;20(19): 1353-1360

1. Introduction

Asymmetric key generation, symmetric encryption and decryption of sensitive data, and asymmetric encryption and decryption of the symmetric secret key are all included in the digital envelope. Encryption is used to create the digital envelope in this case, whereas decryption is used to open the digital envelope. Several secure methods have been proposed, however most rely on single cloud infrastructure for big data access. We propose the dual digital envelope for distributed cloud based big data security for practical and real-time data management in the cloud [1].

Less secure cloud services have varying security criteria and threat levels. Cloud-dominant computing services include IaaS, PaaS, and SaaS. (SaaS). These include bandwidth, communication, computing power, storage, and virtualization. It is used for PaaS and SaaS. These are common IaaS threats. Scalable PaaS applications connect operating systems and server hardware. Peer-to-peer security is rare in PaaS. Periodic software changes and interruptions are risks [2]. Also included are software security, data access, authentication and authorization. SaaS risks include session hijacking, data loss, and privacy violations. The SaaS model is ideal for storing sensitive viewer data in the cloud. Encryption algorithms are used to protect the user's privacy. An important part of network security is data integrity and authentication [3].

The KGS generates cryptographic keys. These keys encrypt data. For real-time applications, this KGS module must be protected. Cryptosystem keys can be symmetric or asymmetric. The KGS and cypher receivers share a secret key. Sender uses KGS' shared public key (d, N) to encrypt

plain text, and receiver uses its private key (e, N) to decode cypher text. Asymmetric RSA KGS uses the same N-bit moduli for both public and private keys. Kleinjung broke the 768 N-bit RSA modulus in 2009. 2048 or 2K bits is recommended by NIST. Start with two N/2 secret primes, p and q. N-bit primes and private keys Thus RSA KGS uses φ(N)=(p-1)* (q-1). It is possible to improve the security and key storage of RSA by breeding it [4].

When the private key size is small, the apt attack can hack the original message from the sent public key. Wiener demonstrated the dangers of RSA using d<N0.25. By obtaining tiny solutions of the polynomial problem using Lattice theory, Boneh and Durfee demonstrated the Wiener Attack's vulnerability at d<N0.292. The Wiener attack is dormant when e >N1.5. These assaults are also polynomial time bound. Dual RSA is insecure when d<N0.333, say Sun et al. In 2014, L. Peng [5] extended the attack to Dual RSA with d<N0.368 [6].

The suggested technique is significant because it provides a flexible approach for businesses that want to adopt SaaS but need high data storage security [7], like the online software training industry. Our proposed solution prevents cloud providers from directly accessing consumers' original data. This study makes two major contributions:

- With our innovative cryptographic solution, cloud operators cannot directly access consumers' original data.
- We provide a low-cost data split approach that ensures data retrievability.

2. Related Works

There are many rhombohedral cryptography rules that use of block or stream cipher methods. Advanced encryption standard (AES), thought of secure algorithm and it is wide used and offers various keys such as the pair of 128, 192, and 256 bis. Blowfish and 2 fish also a symmetric block cipher algorithm [8]. The RC2 may be a stream cipher based symmetric key algorithm employed in network communication. The security standards enable RC2 via Wi-Fi and Internet services. The benefits of asymmetric key encryption rely upon the specific implementation. Below the key level pairs the number of the common advantages publicized by symmetric key answer suppliers are Easier provisioning and revocation, Easier to guard throughout use, quicker execution speed, power management, memory and electronic equipment usage (compared to RSA and ECC) and Low-key cost [9].

Certificate-based authentication goes even additional [10]. It uses a public key cryptography system wherever the general public secret key signed by a sure certificate authority (CA). The certificate authority uses its non-public key to sign the supplicant public key. This connects the remote point with the pair private key and additionally is proof of identity. Certificate based authentication is measured to calculate mutual authentication of server-to-server or device-to-server connections [11]. The important somebody for the IIoT isn't the practicality of individual devices, however the flexibility to use those capabilities to speak over the web and different networks. IIoT devices are full-fledged computers that may be simply integrated into your network environment by adding new communications libraries to your existing applications. As a result, the IIoT may be a cost-efficient thanks to build and deploy a wide vary of sensors and controllers [12].

However, these changes produce new risks for enterprise IT. specialised devices that have historically been isolated are currently exposed to threats and supply opportunities for compromise or attack of organizations' systems and networks [13]. Unauthorized access is wont to modify device software, offer false information to devices, or build different changes that would — within the worst case — physically damage staff and customers. As a result, IIoT needs special attention to network and device security compared to previous generations of technology [14].The most significant objective of business production systems is availability, that ought to stop any spare delay in production that ends up in loss of productivity and loss of revenues. This significantly includes protection against denial-of-service attacks against cyber physical production systems [15].

3. Problem Statement

A distributed file architecture called the Interplanetary File System (IPFS) aims to decentralize the Internet and make it faster and more efficient. It combines key innovations such as Bit Torrent and Git to create multiple registry structures for data sharing. Since its introduction in 2016, IPFS has seen amazing improvements and support from people and organizations. The fact that IPFS is designed to function on top of other protocols, including FTP and HTTP, partly explains the rapid adoption of this distributed document system. When dealing with large files that may take a long time to download or require high transfer speeds when downloading, IPFS works well.

To prevent false declarations, researchers developed software. Due to the lack of a forgery protection mechanism, the certificate is subject to forgery. Therefore, the decentralized application had to use the Ethereum blockchain technology. Initially, they created a digital certificate for the paper certificate, at which point the hash value created for that particular certificate was transferred

to the blockchain structure. The framework reduces the cost of paper and eliminates fake certificates. A blockchain-based authentication framework was developed. In this framework, data on the status of authentication or Certification Center (CA), and data on the status of refusal of the authentications in question are distributed to the subject (Certification Center). The activity of the Certification Center is monitored using public logs. This framework was implemented using Nogix and Firefox. This system has established trust, but the delay in certificate approval gives a false impression of security.

The authors of used the Hyper record Fabric blockchain stage. In this system, the Certificate Authority (CA) simply obtains a certificate from the domain owner using Google's Certificate Transparency (CT) method. These are intended to prevent an SSL/TLS CA from issuing a certificate for a domain without the domain owner's knowledge. This system also experienced low adaptability and less exchange.

The Verification Privacy Control Protocol (VPC) aims to support four key services such as privacy, authentication, confidentiality, and verification. Only administrators can issue certificates online in a decentralized solution or in a decentralized network. And user input is limited to controlling the locking and unlocking of certificates through the paper contracts mentioned in the design, thus privacy control is controlled only by the students. Only authorized universities can issue education certificates, excluding any fraudulent issuance by shadowy individuals or unauthorized organizations. It also makes it easy to verify certificates in Fig.1

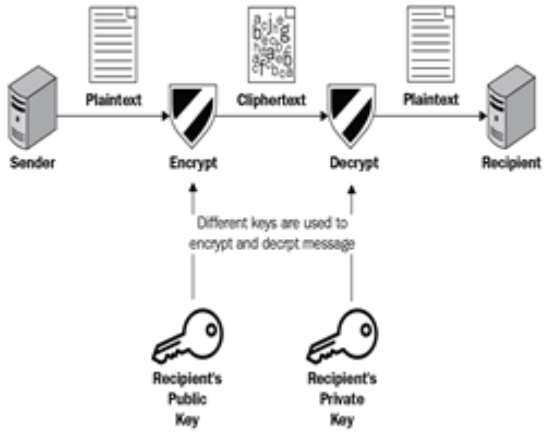

Fig. 1. Key Generation and Exchange Process using general applications

Using IoT in Secure-IoT provides an application envelope in healthcare systems (people, equipment, drugs, etc.) are often ceaselessly caterpillar-tracked and monitored due to the ever-present identification, sensing and communication capabilities of the IoT. With international connectivity, all info concerning healthcare (logistics, diagnostics, therapy, recovery, medication, fiancé, Human resource development and management) can be expeditiously collected, managed and shared.

Employers and universities still sometimes have to call the issuing authority if they want to be sure a transcript hasn't been tampered with. It's complicated and tedious, which is one of the main drivers of fraud. Students must request official transcripts from college enrolment centres and pay for each duplicate transcript. Creating certificates that are easily verified and transferred is one of the advantages of digital systems. There are several advantages to creating a digital infrastructure for certificates, but the stakes are high as such systems evolve and represent our professional reputation. Using a centralized database, poorly formatted queries, and overly general queries can all cause slowdowns. Relational databases are typically designed to run on a single server and require more complex and powerful hardware to scale. Recognizing a fake and unique certificate will require a lot of attention and will lead to the loss of valuable time.

4. Agent Interaction System

An association is a framework for shielding IIoT objects with specified metadata is presented. this permits homeowners of IIoT facilities to define restrictions on IIoT services in a granular and versatile manner. The authorization model works with efficiency and flexibly to fulfil new IIoT security requirements.

An classification is a framework for IIoT object with protection of information in detailed frame rly model. this permits homeowners of IIoT facilities to outline constraints equivalent to time and site restrictions on IIoT services in an exceedingly granular and versatile.

The system model is working with efficiency and flexibility in large-scale deployments to fulfill new IIoT security requirements.

SecIIoT is an authorization system which will efficiently answer security requests supported the roles of the requestors within the context of the commercial Internet of Things.

It consists,

- Metadata format definition / declaration module
- multidimensional classification
- question associate object processing
- optimization in key pairs

- interface in connected objects

Users are allowed to outline IIoT Service information within the a flat file, that could be a terribly helpful to the feature and facilitate the processing in an exceedingly non-SQL atmosphere equivalent to an HDFS distributed file system.

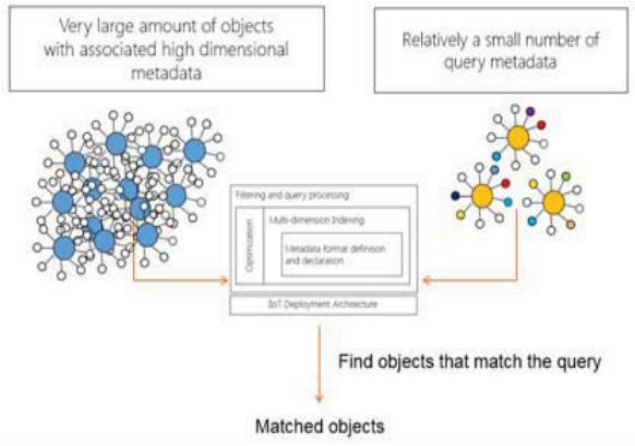

Fig. 2. Agent Model of Secure_IIoT

Secure_IIoT is an authorization system that may effectively reply to security requests supported the roles of requesters within the context of the economic Internet of Things.

It consists of ,

- Information format definition and declaration module
- Multidimensional indexing
- Question filtering and processing
- Optimization
- Interface.

Figure 2 shows that the Secure_IIoT usage diagram. The goal of the Secure_IIoT engine is to go looking for relevant objects in variety of massive pool of IIoT objects that are expeditiously accessible exploitation multidimensional query metadata. The information is classified into IIoT_Service metadata and IIoT_Access metadata. Each metadata has identical range of owner-defined attributes. For example, IIoT_Service information are often scan from an electronic information service table or a flat file. Table should match the subsequent pattern, as shown in Table 1.

Table 1. Metadata—definition and declaration

Index(i)	Column_Name	Field
1	Atribute_1	Data_Type(Attr_1)
2	Atribute_2	Data_Type(Attr_1)
3	Atribute_n	Data_Type(Attr_1)

For a concrete illustration, we have a tendency to use the predefined 10 tuple attributes example of the IIoT_Service metadata schema. As you'll see, there are 10 predefined attributes: "Classification", "Problem", "Source", "Service Type", "Category", "Country", "Project", "Created Date", "Service ID" and "ID Notes" ". and therefore the corresponding index positions are denoted as 1, 2, …, ten respectively. Similarly, the index position of associate degree attribute is adequate to the table column in a relative database.

Table 2. Name field and attribute selection

Index_i	Column_C	Name_Field
1	Classification-X	Varchar_(2)
2	issue_i	Varchar_(80)
3	Source_x	Varchar_(5)
4	Service_Type	Varchar_(5)
5	Category_C	Varchar_(80)
6	Country_Cn	Varchar_(5)
7	Project_Pn	Varchar_(5)
8	Date_Report	Varchar_(8)
9	Service_ID	Varchar_(10)
10	Remark_ID	Varchar_(255)

Universities can now obtain the certificate from the interplanetary file system and verify it. The hash value provided by the user is entered once the verifier has been authenticated. If the submitted hash value is present in the ledger or if the certificate is valid, that hash value will return the document; otherwise, a prompt stating that "no such certificate exists" is displayed to indicate the absence of the files.

Table 3. IIoTService Data Inputs

Index_i	Supported-Values	Example
1	Singular-String	C{165}
2	Multiple-String	Cat{105,302}

Algorithm: Agent Representation and Secure_IIOT Algorithm

Like IIoTService metadata, IIoT Access metadata can also be read from a relational database table or from a flat file.

If it is read from a table, the table must conform to the schema as shown in Table I, and the predefined 10 are the same as in IIoTService.

However, IIoTAccess metadata provides several new ways to define attribute values compared to IIoT service metadata. In addition to the single and multiple strings used in service metadata, IIoTAccess metadata provides:

A range string, the range is defined by its minimum and maximum values. Any number between these two values is called the range.

The ACSII symbol "-" is used to separate its minimum and maximum values. The value to the left of the "-" is the minimum value and the second is the maximum value.

left of the "-" is the minimum value and the second is the maximum value.

A wildcard type (indifferent type), the ASCII asterisk character (*) is used to represent any value when selecting specific files.

Date Range Symbol the ACSII symbol ">" is used to represent the "After" value of the query date. The ACSII character '<' is used to represent a query date value of 'Before'.

For the proposed technology, it translates "< XXX" to a string in the range "19000101-XXX", where the string "19000101" is the earliest date that the proposed technology can support. For date range "> XXX",

it will be translated to a string in the range "XXX-29000101", where 29000101 is the farthest date the proposed technology can support.

Examples of IIoTAccess metadata in a file-based format are shown in Fig. 4. Table IV summarizes the valid value format that can be used to define IIoT Access metadata.

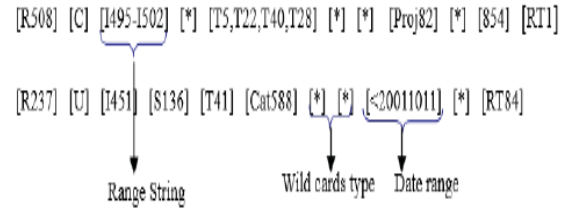

Fig. 3. IIoT Data Payload generated by using Colab

5. Experimental Setup

The Inter-Planetary File System (IPFS) is a convention and shared organization for sharing information in a distributed file system framework. IPFS uses content-addressing to specifically identify each document in a global namespace bridging all calculating devices. During certificate verification, IPFS is used to fetch and store the certificates in the distributed file system. In order to provide a robust system for file storage and sharing, IPFS is built around a decentralized system of client administrators that each hold a portion of the general information. Different peers within the organization can locate and request specific content from any hub by using a distributed hash table (DHT), and any client within the organization can serve a document by its content address. Fig 5 explains the steps involved in IPFS.

Algorithm 1: Leader Election Algorithm In Raft

Input : List of Orderers
Output: Elected Orderer
N ← total number of orderers in the f abric network T ← array(N)
for i ← 1 to N do
T[i] = 0 ;
end /* N must be minimum of 3 for election to happen. Each node votes to either itself or some other nodes */
for each node i in N nodes do
T[x] = T[x] + 1; // 1 ≤ x ≤ N end /* finding the maximum count of vote */
max vote = 0 ; for i ← 1 to N do
max vote = (max vote , T [i]) end;

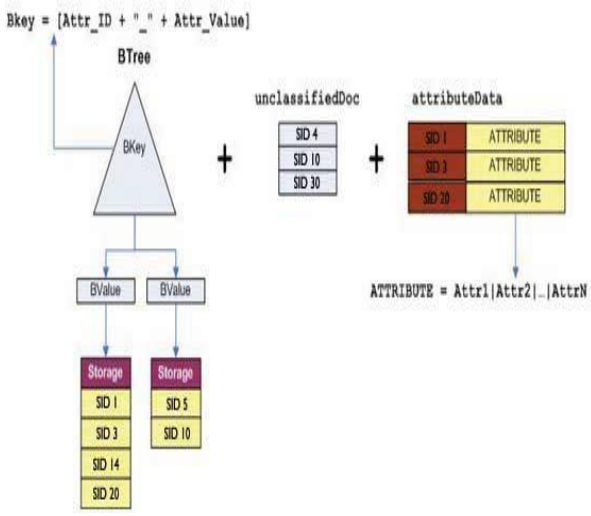

Fig. 4. Index selection from each Agent classification

Classification

It accepts a UserID and an inventory of ServiceIDs to be filtered (hereafter called INPUT-LIST) as inputs to the filtering process shown in Fig.5. supported the UserID entered, its profiles are retrieved from Profile DB, that may be a repository for all user profile information.

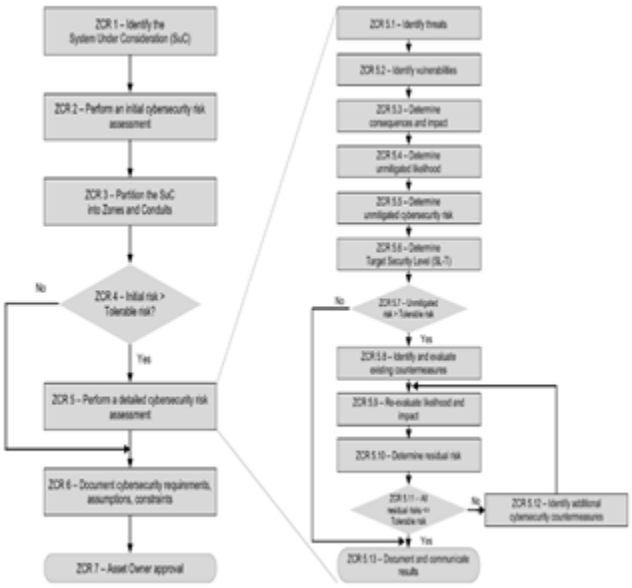

Fig. 5. Agent Key pair generation-Attribute selection

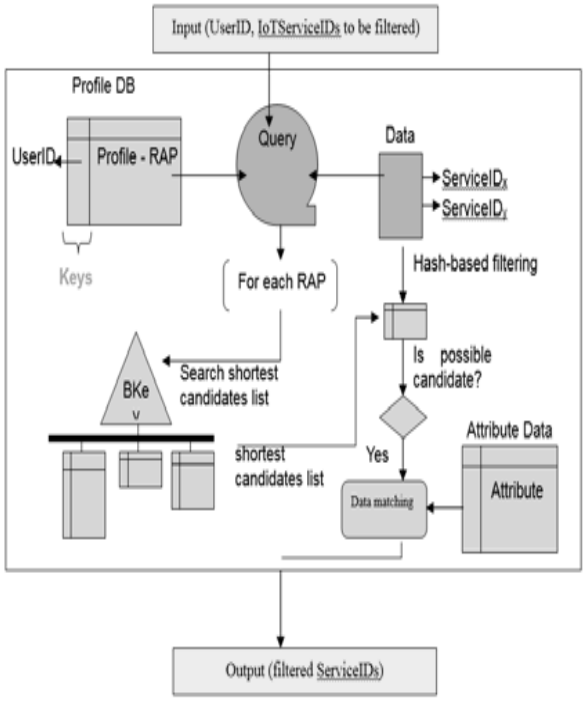

Fig. 6. ServiceID and Data Processing system of each agent data

SecIIoT performs the relational database optimization method. Because the range of records are filtered and increased. RDBMS performance is degrading significantly, whereas SecIIoT still handles the load well. The number of profiles increased, the memory-based approach performs the I/O-based approach is delayed

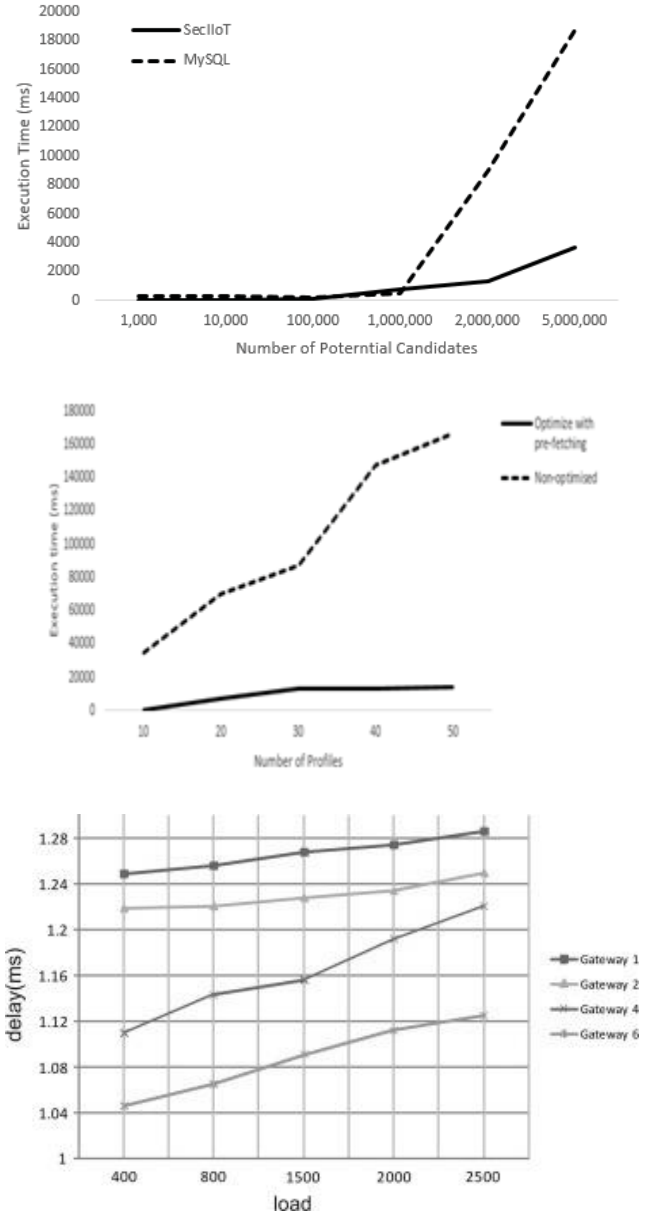

Fig. 7. Secure_IIOT results with Potential Candidates results

In Figure.6 shows that the results of various candidates mistreatment different agent illustrations. The graph shows that the multiple association representation is predicated on attribute selection and seamless knowledge transfer. Our projected approach provides an honest accuracy index supported the results.

6. Conclusion

The Industrial Internet of Things is reworking firms by

integration. The internet of Things, people, knowledge associate degreed computers with intelligent data analytics is measured in this paper. This may result in increasing operational potency and productivity of industries. IIoT access management and authorization of IIoT objects is actually changing into a significant challenge for IIoT success. During this paper, we used classification framework for safeguarding an IIoT object with connected metadata values. It permits homeowners of IIoT facilities to outline constraints corresponding to time and placement restrictions on IIoT services in an exceedingly granular and versatile. The result provides efficiency and flexibly in large-scale deployments to satisfy new IIoT security requirements.

References

[1] K. Manikanda Kumaran, M. Chinnadurai, S. Manikandan, S. PalaniMurugan, E. Elakiya, "An IoT based Green Home Architecture for Green Score Calculation towards Smart Sustainable Cities", KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS VOL. 15, NO. 7, Jul. 2021

[2] K. Shvachko, H. Kuang, S. Radia, and R. Chansler, "The Hadoop Distributed File System," Mass Storage Systems and Technologies (MSST), 2020.

[3] "Industrial Internet Reference Architecture," Industrial Internet Consortium, 2019.

[4] PalaniMurugan, P., Chinnadurai, M., Manikandan, S. (2022). "Tour Planning Design for Mobile Robots Using Pruned Adaptive Resonance Theory Networks". CMC-Computers, Materials & Continua, 70(1), 181–194, doi:10.32604/cmc.2022.016152

[5] P. Lade, R. Ghosh, and S. Srinivasan, "Manufacturing Analytics and Industrial Internet of Things", IEEE Intelligent Systems, 2019, Volume: 32, Issue: 3.

[6] S. Manikandan, P. Dhanalakshmi, K. C. Rajeswari and A. Delphin Carolina Rani, "Deep sentiment learning for measuring similarity recommendations in twitter data," Intelligent Automation & Soft Computing, vol. 34, no.1, pp. 183–192, 2022

[7] J. Mass, C. Chang, and S. N. Srirama, "WiseWare: A Device-to-Device-Based Business Process Management System for Industrial Internet of Things", IEEE International Conference on Internet of Things (iThings),2020.

[8] Z. Ding, X. Gao, L. Guo, and Q. Yang. "A hybrid search engine framework for the internet of things based on spatial-temporal, value based, and keyword-based conditions." In Green Computing and Communications (GreenCom), 2020 IEEE International Conference on, pp. 17-25. IEEE, 2020.

[9] F. Chen, P. Deng, J. Wan, D. Zhang, A.V. Vasilakos, and X. Rong."Data mining for the internet of things: literature review and challenges." International Journal of Distributed Sensor Networks (2017).

[10] E. Borgia. "The Internet of Things vision: Key features, applications and open issues." Computer Communications, 54, pp. 1-31, 2017.

[11] Manikandan. S, Dhanalakshmi. P, Priya. S, Mary OdilyaTeena. A, "Intelligent and Deep Learning Collaborative method for E-Learning Educational Platform using TensorFlow", Turkish Journal of Computer and Mathematics Education, Vol.12 No.10 (2021), E-ISSN: 1309-4653, 2669-2676

[12] R. Zhang, Y. Zhang, and K. Ren, "Distributed Privacy-Preserving Access Control in Sensor Networks," IEEE Transactionson Parallel and Distributed Systems, vol. 23, no. 8, pp. 1427–1438, 2019.

[13] S. Ludwig, G. Selander, and C. Gehrmann. "Authorization framework for the internet-of-things." In World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2019 IEEE 14th International Symposium and Workshops on a, pp. 1-6. IEEE, 2019.

[14] Manikandan, K. Raju, R. Lavanya, R.Hemavathi, "Energy Efficiency Controls on Minimizing Cost with Response Time

[16] ence of the IEEE, pp. 5293-5299. IEEE, 2019.

and Guarantee Using EGC Algorithm",International Journal of Information Technology Insights & Transformations, Vol. 3, No. 1, 2017

[15] P.P. Pereira, J. Eliasson, and J. Delsing. "An authentication and accesscontrol framework for CoAP-based Internet of Things." In Industrial Electronics Society, IECON 2017-40th Annual Confer